TÜV Rheinland Nederland B.V.

Certification Report

NXP Secure Smart Card Controller P40C012/040/072 VD

Sponsor and developer:	***NXP Semiconductors Germany GmbH,*** **Business Unit Identification** **Stresemannallee 101** **D-22529 Hamburg** **Germany**
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-13-37658-CR**
Report version:	**1**
Project number:	**NSCIB-CC-13-37658**
Author(s):	**Wouter Slegers**
Date:	**October 7th, 2014**
Number of pages:	**13**
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 **C13-37658**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

NXP Semiconductors Germany GmbH, Business Unit Identification

Stresemannallee 101, D-22529 Hamburg, Germany

Product and assurance level

NXP Secure Smart Card Controller 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, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, Rev 1.0, 15 June 2007.

Project number **NSCIB-CC-13-37658-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.

SOGIS

Validity

Date of issue : **07-10-2014**

Certificate expiry : **07-10-2019**

Registration number

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

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

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

Currently the Common Criteria Recognition Arrangement (CCRA) and SOGIS-Mutual Recognition Agreement (SOGIS-MRA) do not cover the recognition of Site Certificates. However, the evaluation process followed all the rules of these agreements and used the agreed supporting document for Site certification *[CCDB]*. Therefore, the results of this evaluation and certification procedure can be re-used by any scheme in a subsequent product evaluation and certification procedure that makes use of certified site.

The 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 evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

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 P40C012/040/072 VD. The developer is NXP Semiconductors Germany GmbH, Business Unit Identification located in Hamburg, Germany and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Target of Evaluation (TOE) is a hardware secure smart card controller IC with IC Dedicated software. A Smartcard Embedded Software developer may create Security IC Embedded Software to execute on the NXP P40C012/040/072 VD hardware. This software is stored in arbitrary memory of the NXP P40C012/040/072 VD hardware and is not part of the TOE.

The TOE provides a hardware co-processor for Triple-DES (3DES) and AES, 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 evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on October 1st, 2014 with the acceptance 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 TOE, 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 TOE 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), 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 NXP Secure Smart Card Controller 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.

[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 P40C012/040/072 VD from NXP Semiconductors Germany GmbH, Business Unit Identification located in Hamburg, Germany.

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

Type	Name	Release	Date	Form of delivery
IC Hardware	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

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

The TOE is delivered following the procedures of the hardware part of the TOE, i.e. 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 *[BSI-PP-0035]*. 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 the 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.

NXP Secure Smart Card Controller P40C012/040/072 VD 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,
- hardware to calculate Advanced Encryption Standard (AES) with different key lengths,
- 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 for 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. The following objectives for the environment are of relevance:

- OE.Plat-Appl: Usage of Hardware Platform
- OE.Resp-Appl: Treatment of User Data
- OE.Process-Sec-IC: Protection during Packaging, Finishing and Personalisation
- 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.

Please note that although the TOE contains accelerators for 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

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 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 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

Type	Name	Release	Date	Form of delivery
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

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 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: 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]*. 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*

   This step uses the JIL attack list *[JIL-AM]* as a reference for completeness and studies the ST claims to decide which attacks in the JIL attack list apply for the TOE.

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.

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. This step has been performed as part of AVA evaluation.

4. *Analysis of input from other evaluation activities*

   This step first analyses the input from other CC-evaluation classes expressed as possible vulnerabilities. Secondly, the evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance. This step has been performed as part of AVA evaluation.

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 4 and step 5. This step has been performed as part of AVA evaluation.

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.

In total 40 weeks of testing effort was spent on 6 light manipulation, 2 voltage manipulation and 11 side channel analysis attack scenarios.

2.6.3 Test Configuration

The developer provided the evaluator with the TOE including a proprietary test operating system called IC Dedicated Test Software. 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

This security evaluation is a new, full evaluation under NSCIB. No evaluation results on the TOE have been re-used.

There has been extensive re-use of the ALC aspects for the sites, by use of two site certificates and eight times re-use following the *[AIS38]* methodology. No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE was tested in the major configuration with an EEPROM of 72 kBytes (P40C072 VD).

All major configurations as well as all minor configuration options that can be selected are described in chapter 1.4.2.2 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 P40C012 VD, P40C040 VD, and P40C072 VD as well as for all minor configurations described in the *[ST]*.

2.9 Results of the Evaluation

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

The verdict of all claimed assurance requirements is: **Pass**.

Based on the above evaluation results the evaluation lab concluded the NXP Secure Smart Card Controller 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 the Security Target *[ST]*.

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 of this report) 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.

Please note that although the TOE contains accelerators for 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.

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).

[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 Security Target *[ST]* is included here by reference. A sanitized public version *[ST-lite]* is available*.*

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:

[AIS31] AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der Informationstechnik. Version 2.0, September 18, 2011.

[AIS38] AIS 38: Reuse of evaluation results, Bundesamt für Sicherheit in der Informationstechnik. Version 2.9, June 8th 2011.

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

[CC] Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 4.

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

[ETR] Brightsight, Evaluation Technical Report NXP Secure Smart Card Controller P40C012/040/072 VD EAL5+, 14-RPT-252, version 2.0, dated 1 October 2014.

[ETRfC] Brightsight, Evaluation Technical Report for Composition NXP Secure Smart Card Controller P40C012/040/072 VD EAL5+, 14-RPT-253, version 2.0 dated 1 October 2014.

[JIL-AM] Attack methods for Smart cards and similar devices, JIL, version 2.2, January 2013.

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

[ST] NXP Secure Smart Card Controllers P40C012/040/072 VD Security Target, Rev. 1.4, 2014-09-25.

[ST-lite] NXP Secure Smart Card Controllers P40C012/040/072 VD Security Target Lite, Rev. 1.1, 2014-09-25.

(This is the end of this report).