Certification Report

NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Business Unit Security & Connectivity
Troplowitzstrasse 20
Hamburg, Germany

Evaluation facility: ***Riscure***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-150453-CR2**
Report version:	**1**
Project number:	**150453**
Author(s):	**Wouter Slegers**
Date:	**29 July 2019**
Number of pages:	**15**
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

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**CC-19-150453**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors Germany GmbH** **Business Unit Security & Connectivity** **Troplowitzstrasse 20 22529 Hamburg, Germany**
Product and assurance level	**NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG** Assurance Package: ▪ EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 Protection Profile Conformance: ▪ Security IC Platform Protection Profile, Version 1.0, registered under the reference BSI-PP-0035
Project number	**150453**
Evaluation facility	**Riscure BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

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.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL 7

Validity	Date of 1st issue : **21-02-2018** Date of 2nd issue : **30-07-2019** Certificate expiry : **21-02-2023**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

CONTENTS:

Foreword **4**

Recognition of the certificate **5**

International recognition 5
European recognition 5

1 Executive Summary **6**

2 Certification Results **8**

2.1 Identification of Target of Evaluation 8
2.2 Security Policy 9
2.3 Assumptions and Clarification of Scope 10
2.4 Architectural Information 10
2.5 Documentation 10
2.6 IT Product Testing 11
2.7 Re-used evaluation results 12
2.8 Evaluated Configuration 13
2.9 Results of the Evaluation 13
2.10 Comments/Recommendations 13

3 Security Target **14**

4 Definitions **14**

5 Bibliography **15**

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 P60x080/052/040yVC(Y/Z/A)/yVG. The developer of the NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG is NXP Semiconductors Germany GmbH 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 TOE provides a hardware platform for an implementation of a smart card application with

- functionality to calculate the Data Encryption Standard (Triple-DES) with up to three keys,
- functionality to calculate the Advanced Encryption Standard (AES) with different key lengths,
- support for large integer arithmetic operations like multiplication, addition and logical operations, which are suitable for public key cryptography and elliptic curve cryptography,
- a True Random Number Generator,
- memory management control,
- cyclic redundancy check (CRC) calculation,
- ISO/IEC 7816 contact interface with UART,
- ISO/IEC 14443 A contactless interface.

Note: Large integer arithmetic operations are intended to be used for calculation of asymmetric cryptographic algorithms. Any asymmetric cryptographic algorithm utilizing the support for large integer arithmetic operations has to be implemented in the Security IC Embedded Software. Thus, the support for large integer arithmetic operations itself does not provide security functionality like cryptographic support. The Security IC Embedded Software implementing an asymmetric cryptographic algorithm is not included in this evaluation. The same scope of evaluation applies to the CRC calculation which does not in itself provide security functionality but is a supportive feature for use by the Security IC Embedded Software.

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.

The TOE has been originally evaluated by Riscure B.V. located in Delft, The Netherlands and was certified on 21 February 2018. The re-evaluation also took place by Riscure B.V. and was completed on 29 July 2019 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 change is a change in the guidance with respect to specific edge case behaviour of the MMU. Composition developers and evaluators are advised to consider the impact on their product.

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 P60x080/052/040yVC(Y/Z/A)/yVG, 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 P60x080/052/040yVC(Y/Z/A)/yVG 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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic flaw remediation) 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 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 P60x080/052/040yVC(Y/Z/A)/yVG from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

TOE components for P60x080/052/040PVC(Y):

Delivery item type	Identifier	Version
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Y)	VC(Y), 13 September 2012
Security IC Dedicated Test Software	Test-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Boot-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Firmware Operating System (FOS)	6.11, 07 May 2012

TOE components for P60x080/052/040PVC(Z/A):

Delivery item type	Identifier	Version
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Z)	VC(Z), 13 September 2012
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(A)	VC(A), 13 September 2012
Security IC Dedicated Test Software	Test-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Boot-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Firmware Operating System (FOS)	6.11/6.13, 07 May 2012

TOE components for P60x080/052/040PVG:

Delivery item type	Identifier	Version
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVG	VG, 26 November 2013
Security IC Dedicated Test Software	Test-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Boot-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Firmware Operating System (FOS)	6.11/6.13, 07 May 2012

TOE components for P60D080/052/040MVC(Z/A)/MVG:

Delivery item type	Identifier	Version
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Z)	VC(Z), 13 September 2012
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(A)	VC(A), 13 September 2012
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVG	VG, 26 November 2013
Security IC Dedicated Test Software	Test-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Boot-ROM Software	0A.05, 07 May 2012
Security IC Dedicated support Software	Firmware Operating System (FOS)	6.12/6.13, 07 May 2012

TOE components for P60D080/052/040DVC(Z/A)/DVG and P60D080/052/040JVC(Z/A)/JVG:

Delivery item type	Identifier	Version
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Z)	VC(Z), 13 September 2012
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(A)	VC(A), 13 September 2012
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVG	VG, 26 November 2013
Security IC Dedicated Test Software	Test-ROM Software	0A.09, 17 December 2012
Security IC Dedicated support Software	Boot-ROM Software	0A.09, 17 December 2012
Security IC Dedicated support Software	Firmware Operating System (FOS)	08.00, 17 December 2012

To ensure secure usage a set of guidance documents is provided together with the NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG. Details can be found in section ”Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, sections 1.4.4 and 1.4.5.

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.

The TOE provides a hardware platform for an implementation of a smart card application with

- functionality to calculate the Data Encryption Standard (Triple-DES) with up to three keys,
- functionality to calculate the Advanced Encryption Standard (AES) with different key lengths,
- support for large integer arithmetic operations like multiplication, addition and logical operations, which are suitable for public key cryptography and elliptic curve cryptography,
- a True Random Number Generator,
- memory management control,
- cyclic redundancy check (CRC) calculation,
- ISO/IEC 7816 contact interface with UART,
- ISO/IEC 14443 A contactless interface.

Note: Large integer arithmetic operations are intended to be used for calculation of asymmetric cryptographic algorithms. Any asymmetric cryptographic algorithm utilizing the support for large integer arithmetic operations has to be implemented in the Security IC Embedded Software. Thus, the support for large integer arithmetic operations itself does not provide security functionality like cryptographic support. The Security IC Embedded Software implementing an asymmetric cryptographic algorithm is not included in this evaluation. The same scope of evaluation applies to the CRC calculation which does not in itself provide security functionality but is a supportive feature for use by the Security IC 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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 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 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:

Identifier	Version
Product Data Sheet, SmartMX2 family P60x040/052/080 VC/VG Secure high-performance smart card controller, NXP Semiconductors, Business	5.2, 27 June 2014

Unit Identification, Revision 5.2, Document Number 203652, 27 June 2014	
Instruction Set for the SmartMX2 family, Secure smart card controller, NXP Semiconductors, Business Unit Identification, Revision 3.1, Document Number 147831, 02 February 2012	3.1, 02 February 2012
Information on Guidance and Operation, NXP Secure Smart Card Controller P60x040/052/080 VC/VG, NXP Semiconductors, Business Unit Identification, Revision 1.5, Document Number 239316, 21 January 2019	1.6, 21 January 2019
Product data sheet addendum: SmartMX2 family P60x040/052/080 VC/VG Wafer and delivery specification, NXP Semiconductors, Revision 3.4, Document Number 237234, 18 July 2018	3.4, 18 July 2014
Product data sheet addendum: SmartMX2 family, Post Delivery Configuration (PDC), NXP Semiconductors, Business Unit Identification, Revision 3.2, Document Number 225032,, 04 February 2013	3.2, 04 February 2013
Product data sheet addendum: SmartMX2 family, Chip Health Mode (CHM), NXP Semiconductors, Business Unit Identification, Revision 3.1, Document Number 224431, 01 October 2014	3.1, 01 October 2014
Product data sheet addendum: SmartMX2 family, Firmware Interface Specification (FIS), NXP Semiconductors, Business Unit Identification, Revision 4.2, Document Number 233342, 24 June 2015	4.2, 24 June 2015
Product data sheet addendum: Product Errata Sheet, SmartMX2 family P60x040/052/080 VC/VG Secure high-performance smart card controller, NXP Semiconductors, Business Unit Identification, Revision 1.0, Document Number 453710, 11 December 2017	1.0, 11 December 2017

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.

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

2.6.2 Independent Penetration Testing

The evaluator independent penetration tests were conducted according to the following testing approach:

- During evaluation of the ADV, ATE and ALC classes the evaluators hypothesized possible vulnerabilities. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained in particular from the source code analysis in IMP. This resulted in a shortlist of potential vulnerabilities to be tested.
- Next the evaluators analysed the TOE design and implementation for resistance against the JIL attacks. This resulted in further potential vulnerabilities to be tested.
- The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ARC has assessed all information.

- The evaluators concluded that a number of areas could be potentially vulnerable for attackers possessing a high attack potential. Consequently practical penetration testing was performed for absolute assurance.

In total 18 fault injection, 9 side channel and 4 logical penetration tests were performed in the original evaluation. For the recertification 2 fault injection, 1 side channel and 1 logical penetration tests were performed, confirming the original test results.

2.6.3 Test Configuration

Testing was performed on the P60D080PVC(A), P60D080JVC(A), and P60D080JVG variants. The difference between the variants has been analysed and has no impact on the test results, hence the test results apply to all variants of the TOE.

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 TOE supports a wide range of key sizes (see *[ST]*), including those with a sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

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

2.7 Re-used evaluation results

This is 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 site certificates and Site Technical Audit Re-use report approaches.

- NXP Semiconductors Hamburg Business Unit Identification (BU ID),
- NXP Semiconductors Eindhoven,
- NXP Semiconductors Nijmegen,
- NXP Gratkorn Austria,
- NXP Eindhoven Secure Room,
- NXP Bangalore,
- TSMC Fab 2/5,
- TSMC Fab 8 (replaces Fab 7),
- TSMC Fab 14A,
- Chipbond Technology Corporation,
- NXP Semiconductors Test Center Europe – Hamburg (TCE-H),
- Assembly and Test Bangkok (ATBK),
- Assembly and Test Kaohsiung (ATKH),
- HID Global Ireland Teoranta,,
- Linxens (formerly SMARTTRAC Technology Ltd)

- Colt Hamburg
- Akquinet Hamburg
- HCL Gothenburg

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 P60x080/052/040yVC(Y/Z/A)/yVG. See *[ST]* for the all covered configurations.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] and 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 P60x080/052/040yVC(Y/Z/A)/yVG, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ASE_TSS.2 and ALC_FLR.1**. 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.

The major change is a change in the guidance with respect to specific edge case behaviour of the MMU. Composition developers and evaluators are advised to consider the impact on their product.

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 P60x080/052/040yVC(Y/Z/A)/yVG Security Target, NXP Semiconductors, Business Unit Identification, Rev. 2.6, 23 January 2019 *[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
DES	Data Encryption Standard
DFA	Differential Fault Analysis
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

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]	Evaluation Technical Report P60x080/052/040yVC(Y/Z/A)/yVG version 2.2, dated 12 July 2019. ST-LITE EVALUATION FOR P60X080/052/040YVC(Y/Z/A)/YVG, NSCIB-CC-19-150453
[ETRfC]	ETR for Composite Evaluation P60x080/052/040yVC(Y/Z/A)/yVG, version 2.2, 17 July 2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, March 28 2019.
[PP]	Security IC Platform Protection Profile, Version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035
[ST]	NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG Security Target, NXP Semiconductors, Business Unit Identification, Rev. 2.6, 23 January 2019.
[ST-lite]	NXP Secure Smart Card Controller Security Target Lite, Rev 2.6, 23 January 2019.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).