Certification Report

Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG

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

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

Report number: **NSCIB-CC-15-84058-CR**

Report version: **1**

Project number: **NSCIB-CC-15-84058**

Authors(s): **Wouter Slegers**

Date: **11 January 2017**

Number of pages: **16**

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 with the Amsterdam 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-15-84058**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors Germany GmbH, Business Line Security and Connectivity** **Stresemannallee 101, D-22529 Hamburg, Germany**
Product and assurance level	**Crypto Library V1.0 on 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, 15.06.2007; published under the reference BSI-PP-0035
Project number	**NSCIB-CC-15-84058**
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)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of issue : **12-01-2017** Certificate expiry : **12-01-2022**

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 intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

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

Recognition of the certificate

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

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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 Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG. The developer of the Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG is NXP Semiconductors 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 Target of Evaluation – TOE (i.e., the Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG) consists of the Crypto Library V1.0 and the NXP P60x080/052/040yVC(Y/Z/A)/yVG with IC Dedicated Software. For ease of reading the TOE is often called “Crypto Library on SmartMX2”.

The evaluation of the TOE was conducted as a composite evaluation and uses the results of the CC evaluation of the underlying NXP SmartMX2 P60x080/052/040yVC(Y/Z/A)/yVG Secure Smart Card Controller (re)certified under the German CC Scheme on 5 August 2016 (*[HW CERT]*).

The Crypto Library on SmartMX2 is a cryptographic library, which provides a set of cryptographic functions that can be used by the Smartcard Embedded Software. The cryptographic library consists 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 arbitrary memory. The NXP SmartMX2 smart card processor provides the computing platform and cryptographic support by means of co-processors for the Crypto Library on SmartMX2.

The Crypto Library on SmartMX2 provides AES, DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECDSA (ECC over GF(p)) signature generation and verification, ECDSA (ECC over GF(p)) key generation, ECDH (ECC Diffie-Helmann) keyexchange, full point addition (ECC over GF(p), 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.

Finally, the TOE provides a secure copy routine and a secure compare routine and includes internal security measures for residual information protection. For more details refer to the *[ST]*, chapter 1.3.2.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 30 November 2016 with the approval 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 Crypto Library V1.0 on 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 Crypto Library V1.0 on 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 provide sufficient evidence that it meets the EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE summary specification with architectural design summary) and ALC_FLR.1 (Flaw Remediation).

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 Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified

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

Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

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

Type	Name	Release	Date	Form of delivery
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Y)	VC(Y)	13 September 2012	Wafer, module, inlay, package (dice have nameplate 9049A)
IC Dedicated Test Software	Test-ROM Software	0A.05	07 May 2012	Test-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex
Security IC Dedicated Support Software	Boot-ROM Software	0A.05	07 May 2012	Boot-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex
	Firmware Operating System (FOS)	6.11	07 May 2012	Firmware Operating System on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex

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

Type	Name	Release	Date	Form of delivery
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Z)	VC(Z)	13 September 2012	Wafer, module, inlay, package (dice have nameplate 9049A)
	NXP Secure Smart Card Controller P60x080/052/040PVC(A)	VC(A)		
IC Dedicated Test Software	Test-ROM Software	0A.05	07 May 2012	Test-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex
Security IC Dedicated Support Software	Boot-ROM Software	0A.05	07 May 2012	Boot-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex
	Firmware Operating System (FOS)	6.11 6.13	07 May 2012	Firmware Operating System on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex

Specific TOE components for P60x080/052/040PVG:

Type	Name	Release	Date	Form of delivery
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVG	VG	26 November 2013	Wafer, module, inlay, package (dice have nameplate 9049B)
IC Dedicated Test Software	Test-ROM Software	0A.05	07 May 2012	Test-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex
Security IC Dedicated Support	Boot-ROM Software	0A.05	07 May 2012	Boot-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex

Type	Name	Release	Date	Form of delivery
Software	Firmware Operating System (FOS)	6.11 6.13	07 May 2012	Firmware Operating System on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex

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

Type	Name	Release	Date	Form of delivery
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Z)	VC(Z)	13 September 2012	Wafer, module, inlay, package (dice have nameplate 9049A)
	NXP Secure Smart Card Controller P60x080/052/040PVC(A)	VC(A)		
	NXP Secure Smart Card Controller P60x080/052/040PVG	VG	26 November 2013	Wafer, module, inlay, package (dice have nameplate 9049B)
IC Dedicated Test Software	Test-ROM Software	0A.05	07 May 2012	Test-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex
Security IC Dedicated Support Software	Boot-ROM Software	0A.05	07 May 2012	Boot-ROM on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex
	Firmware Operating System (FOS)	6.12 6.13	07 May 2012	Firmware Operating System on the chip acc. to 9049A_LA001_TESTROM_v1_btos_0Av05_fos_6v10.hex

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

Type	Name	Release	Date	Form of delivery
IC Hardware	NXP Secure Smart Card Controller P60x080/052/040PVC(Z)	VC(Z)	13 September 2012	Wafer, module, inlay, package (dice have nameplate 9049A)
	NXP Secure Smart Card Controller P60x080/052/040PVC(A)	VC(A)		
	NXP Secure Smart Card Controller P60x080/052/040PVG	VG	26 November 2013	Wafer, module, inlay, package (dice have nameplate 9049B)
IC Dedicated Test Software	Test-ROM Software	0A.09	17 December 2012	Test-ROM on the chip acc. to 9049A_LF097_TESTROM_v1_btos_0Av09_fos_8v00.hex
Security IC Dedicated Support Software	Boot-ROM Software	0A.09	17 December 2012	Boot-ROM on the chip acc. to 9049A_LF097_TESTROM_v1_btos_0Av09_fos_8v00.hex
	Firmware Operating System (FOS)	8.0	17 December 2012	Firmware Operating System on the chip acc. to 9049A_LF097_TESTROM_v1_btos_0Av09_fos_8v00.hex

TOE components shared for all TOE variants:

Type	Name	Release	Date	Form of delivery
Library file	phSmx2ClAes.lib	1.0	2012-12-05	Electronic file
	phSmx2ClDes.lib	1.0	2012-12-05	Electronic file

Type	Name	Release	Date	Form of delivery
	phSmx2ClRsa.lib	1.0	2012-12-05	Electronic file
	phSmx2ClRsaKg.lib	1.0	2012-12-05	Electronic file
	phSmx2ClEccGfp.lib	1.0	2012-12-05	Electronic file
	phSmx2ClSha.lib	1.0	2012-12-05	Electronic file
	phSmx2ClSha512.lib	1.0	2012-12-05	Electronic file
	phSmx2ClRng.lib	1.0	2012-12-05	Electronic file
	phSmx2ClUtils.lib	1.0	2012-12-05	Electronic file
Header file	phSmx2ClAes.h	1.0	2012-12-05	Electronic file
	phSmx2ClDes.h	1.0	2012-12-05	Electronic file
	phSmx2ClRsa.h	1.0	2012-12-05	Electronic file
	phSmx2ClRsaKg.h	1.0	2012-12-05	Electronic file
	phSmx2ClEccGfp.h	1.0	2012-12-05	Electronic file
	phSmx2ClSha.h	1.0	2012-12-05	Electronic file
	phSmx2ClSha512.h	1.0	2012-12-05	Electronic file
	phSmx2ClRng.h	1.0	2012-12-05	Electronic file
	phSmx2ClUtils.h	1.0	2012-12-05	Electronic file
	phSmx2ClUtils_ImportExportFcts.h	1.0	2012-12-05	Electronic file
	phSmx2ClUtils_RngAccess.h	1.0	2012-12-05	Electronic file
	phSmx2ClTypes.h	1.0	2012-12-05	Electronic file
Source code	phSmx2ClUtils_ ImportExportFcts.a51	1.0	2012-12-05	Electronic file
	phSmx2ClUtils_ RngAccess.a51	1.0	2012-12-05	Electronic file

To ensure secure usage a set of guidance documents is provided together with the Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG. Details can be found in section 2.5 of this report.

The hardware part of the TOE is delivered by NXP either as wafer, module, inlay, or packaged form together with the IC Dedicated Support Software. The Crypto Library is delivered in Phase 1 of the TOE lifecycle 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 Crypto Library 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 a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.2.2.

2.2 Security Policy

The TOE provides the cryptographic algorithms AES, DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECDSA (ECC over GF(p)) signature generation and verification, ECDSA (ECC over GF(p)) key generation, ECDH (ECC Diffie-Helmann) keyexchange, full point addition (ECC over GF(p), SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms 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. SHA is only resistant against Side Channel Attacks and timing attacks. Details on the resistance claims are provided in the Security Target *[ST],* relevant details are provided in the user guidance documents.

The TOE implements a software (pseudo) random number generator, which is initialised (seeded) by the hardware random number generator of the SmartMX2.

The TOE also a secure copy routine and a secure compare routine and includes internal security measures for residual information protection.

Note 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. 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.

Major configurations P60x080/052/040M, P60x080/052/040D, and P60x080/052/040J include emulation MIFARE Plus MF1PLUSx0 or MIFARE DESFire EV1 or both MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1. Note that these emulations are not part of the TOE.

2.4 Architectural Information

The TOE contains a Crypto Library, which provides a set of cryptographic functionalities that can be used by the Smartcard Embedded Software. The Crypto Library consists 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 arbitrary memory. 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 provided. The whole TOE provides AES, DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECDSA (ECC over GF(p)) signature generation and verification, ECDSA (ECC over GF(p)) key generation, ECDH (ECC Diffie-Helmann) keyexchange, full point addition (ECC over GF(p), SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms in addition to the functionality described in the Hardware Security Target *[ST-HW]* for the hardware platform. In addition, 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 contains a secure copy routine and a secure compare routine and includes internal security measures for residual information protection.

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	Product Data Sheet SmartMX2 family P60D040/052/080 VC, Secure high-performance smart card controller	5.2	27 June 2014	Electronic document
	Instruction Set for the SmartMX2 family, Secure smart card controller	3.1	2 February 2012	Electronic document

Type	Name	Release	Date	Form of delivery
	NXP Secure Smart Card Controller P60x040/052/080VC Guidance and Operation Manual	1.3	10 May 2016	Electronic document
	SmartMX2 family P60x040/052/080 VC Wafer and delivery specification	3.4	18 July 2014	Electronic document
	Product data sheet addendum: SmartMX2 family Post Delivery Configuration (PDC)	3.2	4 February 2013	Electronic document
	Product data sheet addendum: SmartMX2 family Chip Health Mode (CHM)	3.1	1 October 2013	Electronic document
	Product data sheet addendum: SmartMX2 family, Firmware Interface Specification (FIS)	4.1	25 June 2014	Electronic document
Software	Crypto Library on SmartMX2 Preparative procedures and operational user guidance	1.6	14 October 2016	Electronic document
	SmartMX2 Crypto Library: User Manual – Random Number Generator	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – AES	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – DES	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – SHA	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – SHA-512	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – RSA	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – RSA Key Generation	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – ECC over GF(p)	1.0	5 December 2012	Electronic document
	SmartMX2 Crypto Library: User Manual – Utils	1.1	7 September 2016	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

For the Crypto Library, the developer has performed extensive testing on functional specifications, subsystem and module level.

All possible parameter choices and boundary cases have been addressed by a highly automated test environment. Test scripts are employed to verify that the test results are as expected.

Since the hardware is operated according to its guidance and the composite evaluation requirements are met, the hardware test results are extendible to composite evaluations on the hardware part of this TOE.

The developer has provided the testing environment to the evaluators. The evaluators have reproduced a large set of developer tests by taking advantage of the highly automated test scripts, as well as they have designed few number of tests.

2.6.2 Independent Penetration Testing

The evaluator used the following approach in penetration testing

The evaluation considers the all security features and security services that are in the scope of the evaluation as defined in the security target by the developer. An overview of this is established in the security requirements analysis phase.

The subsequent system analysis phase then assesses how the functional design refines the security features and services in the system design.

Based on this assessment of the security design and implementation of the system the evaluation mounts a methodical vulnerability analysis to identify flaws in the system. The starting point is the continuously maintained and improved knowledge in the various general knowledge domains as well as the market specific attack knowledge. For smartcards and similar devices the JIL attack methods define the state of the art attack methods, which are applicable to products which are exposed in a hostile environment and aim at reaching resistance against an attacker with a high attack potential. These attack methods completely cover the various types of attacks like physical attacks, side channel analysis, fault injection etc. but do not detail aspects like applying these methods in a specific application context like breaking an RSA implementation using the attacks techniques presented e.g. by Bellcore or Schindler and Itoh. For maintaining the state-of-the-art knowledge about such attack techniques, Riscure actively participates in international working groups like JHAS, monitors relevant sources like publications of certification bodies or in conferences, and conducts internal research and development.

Based on this solid attack knowledge, the vulnerability analysis is conducted for the specific product while taking the results of the system analysis into account. Furthermore, the product knowledge gained while performing the evaluation activities required by other evaluation classes are taken into consideration. As a result, product specific attack variants can be identified or potential attacks can be ruled out based on experience on the effectiveness of specific security measures in the implementation. The results of the vulnerability analysis is a test plan.

According to the test plan the penetration testing is performed. The results of the penetration testing together with the assurance gained during the rest of the evaluation activities are rated using the JIL rating. Based on the ratings and gained assurance the evaluators come to a conclusion about the resistance of the TOE against attackers possessing high attack potential.

In total 7 side channel analysis attacks and 2 perturbation attacks were performed. For detailed information, see the *[ETR].*

2.6.3 Test Configuration

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

The TOE was tested on P60D080JV0G095 using the built-in Test OS. The results of the tests are deemed applicable to the Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG, based on the similarity of results obtained in the base evaluations of the TOE on the respective platforms, and the fact that the hardware architecture of the platforms only differ in the memory size and availability of Mifare (out of scope of this evaluation).

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 strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. No exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references several Intermediate Reports. 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 Crypto Library V1.0 on 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 technical requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile Security IC Platform Protection Profile, Version 1.0, 15.06.2007; published under the reference BSI-PP-0035.

2.9 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).

[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 Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG, Rev. 1.11 - 14 October 2016 *[ST]* is included here by reference.

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
ECC	Elliptic Curve Cryptography
ECB	Electronic Code Book (a block cipher mode of operation)
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
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]	Riscure, ETR Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG, version 1.3, dated 16 November 2016.
[ETRfC]	Riscure, ETR for Composite Evaluation Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG, version 1.1, dated 16 November 2016.
[HW-CERT]	Certification Report for NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG with IC Dedicated Software, BSI-DSZ-CC-0837-V3-2016, 5 August 2016.
[HW-ETRfC]	TÜV Informationstechnik GmbH - Evaluation Technical Report for Composite Evaluation P60x080/052/040yVC(Y/Z/A)/yVG, Version 2, 2016-07-04.
[HW-ST]	NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG Security Target, Rev 2.3..
[JIL]	Attack methods for Smart cards and similar devices, JIL, version 2.2, January 2013.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.
[ST]	Security Target Crypto Library V1.0 on P60x080/052/040yVC(Y/Z/A)/yVG, Rev. 1.11 - 14 October 2016.

(This is the end of this report).