Certification Report

Crypto Library V3.1.x on P6022y VB

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Business Unit Security & Connectivity** **Troplowitzstrasse 20, 22529 Hamburg** **Germany**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-67206-CR3**
Report version:	**1**
Project number:	**67206**
Author(s):	**Wouter Slegers**
Date:	**29 May 2018**
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 5 (ISO/IEC 15408)
Certificate number	**CC-18-67206**

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	**Crypto Library V3.1.x on P6022y VB** Assurance Package: ▪ EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 Protection Profile Conformance: ▪ Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084
Project number	**67206**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (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 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. 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 1st issue : **28-07-2016** Date of 2nd issue : **17-11-2017** Date of 3rd issue : **31-05-2018** Certificate expiry : **28-07-2021**

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

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 Crypto Library V3.1.x on P6022y VB. The developer of the Crypto Library V3.1.x on P6022y VB 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 Target of Evaluation (TOE) consists of the Crypto Library V3.1.x and the NXP Secure Smart Card Controller P6022y VB Secure Smart Card Controller. For ease of reading the TOE is often called "Crypto Library on SmartMX2".

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 TOE provides AES, DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECDSA, ECC key generation, ECDH, ECC point addition, and 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, a secure compare routine, a secure modular multiply routine, a secure modular add and subtract routine, and includes internal security measures for residual information protection. For more details refer to the *[ST]*, chapter 1.3.2.

Note that in the *[ST]* the "Crypto Library V3.1.x" represents the Crypto Library V3.1.2.

In case of a composite evaluation the used minor version of the CL should be explicitly checked and mentioned.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 28 July 2016, and re-certified on 17 November 2017. The re-evaluation also took place by Brightsight B.V. and was completed on 16 May 2017 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

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

The major changes are the update of the underlying platform certification scope (MIFARE is now out all scopes), additional production sites and an additional variant, and subsequent recertification.

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

Note that in the second certification of this TOE, the ST has been updated to remove all claims regarding the security of ECC parameter verification. If the security of a composite or end product relies on this functionality, appropriate evaluation of the security properties of this functionality is required.

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 V3.1.x on P6022y VB, 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 V3.1.x on P6022y VB 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 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 5 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[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 Crypto Library V3.1.x on P6022y VB from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Type	Name	Release	Date	Form of delivery
Library File	phSmx2ClDes.lib	1.5	2015-09-14	Electronic file
	phSmx2ClAes.lib	1.6	2015-09-14	Electronic file
	phSmx2ClRsa.lib	1.10	2015-09-14	Electronic file
	phSmx2ClRsaKg.lib	2.7	2015-09-14	Electronic file
	phSmx2ClEccGfp.lib	2.7	2015-09-14	Electronic file
	phSmx2ClSha.lib	1.7	2015-09-14	Electronic file
	phSmx2ClSha512.lib	1.8	2015-09-14	Electronic file
	phSmx2ClRng.lib	2.8	2015-09-14	Electronic file
	phSmx2ClUtils.lib	2.2	2015-09-14	Electronic file
	phSmx2ClSymCfg.lib	1.8	2015-09-14	Electronic file
Header file	phSmx2ClDes.h	1.4	2015-03-26	Electronic file
	phSmx2ClAes.h	1.5	2015-03-26	Electronic file
	phSmx2ClRsa.h	1.9	2015-04-28	Electronic file
	phSmx2ClRsaKg.h	2.6	2015-04-28	Electronic file
	phSmx2ClEccGfp.h	2.6	2015-04-28	Electronic file
	phSmx2ClSha.h	1.6	2015-03-26	Electronic file
	phSmx2ClSha512.h	1.7	2015-03-26	Electronic file
	phSmx2ClRng.h	2.7	2015-04-28	Electronic file
	phSmx2ClUtils.h	2.0	2015-04-28	Electronic file
	phSmx2ClUtils_ImportExportFcts.h	2.0	2015-04-28	Electronic file
	phSmx2ClUtils_RngAccess.h	2.0	2015-04-28	Electronic file
	phSmx2ClTypes.h	1.1	2013-11-15	Electronic file
	phSmx2ClSymCfg.h	1.7	2015-03-26	Electronic file
	phSmx2ClSymCfg_Aes.h	1.7	2015-03-26	Electronic file
	phSmx2ClSymCfg_Des.h	1.7	2015-03-26	Electronic file
Source code	phSmx2ClUtils_ImportExportFcts.a51	2.0	2015-04-28	Electronic file
	phSmx2ClUtils_RngAccess.a51	2.0	2015-04-28	Electronic file

To ensure secure usage a set of guidance documents is provided together with the Crypto Library V3.1.x on P6022y VB. Details can be found in section 2.5 of this report.

The hardware part of the TOE is delivered by NXP as described in the hardware guidance.

The Crypto Library is delivered in Phase 1 of the TOE lifecycle (for a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.2.2.) as a software package (a set of binary files) to the developers of the Smartcard Embedded Software. The Smartcard Embedded Software may comprise in this case an operating system and/or other smart card software (applications). The Software developers can incorporate the 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 the identification of the Hardware please refer to the hardware certification.

2.2 Security Policy

The TOE provides the cryptographic algorithms AES1, DES1, Triple-DES (3DES)1, 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-Hellmann key-exchange, full point addition (ECC over GF(p)), standard security level 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, a secure compare routine, secure modular multiply routine, a secure modular add and subtract 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 chapter 4 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.

2.4 Architectural Information

This chapter provides a high-level description of the IT product and its major components based on the evaluation evidence described in the Common Criteria assurance family entitled “TOE design (ADV_TDS)”. The intent of this chapter is to characterise the degree of architectural separation of the major components and to show dependencies between the TOE and products using the TOE in a composition (e.g. dependencies between HW and SW).

The TOE contains a Crypto Library, which provides a set of cryptographic functionalities 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)) signature generation and verification, ECDSA (ECC over GF(p)) key generation, ECDH (ECC Diffie-Helmann) key-exchange, 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.

Finally, the TOE provides a secure copy routine, a secure compare routine, a secure modular multiply routine, a secure modular add and subtract 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
Documents	User Guidance Manual	1.6	2018-02-28	Electronic document
	User Guidance: DES	1.0	2015-11-23	Electronic document
	User Guidance: AES	1.0	2015-11-23	Electronic document
	User Guidance: RSA	1.0	2015-11-23	Electronic document
	User Guidance: RSA Key Generation	1.0	2015-11-23	Electronic document
	User Guidance: ECC over GF(p)	1.0	2015-11-23	Electronic document
	User Guidance: SHA	1.0	2015-11-23	Electronic document
	User Guidance: SHA512	1.0	2015-11-23	Electronic document
	User Guidance: RNG	1.0	2015-11-23	Electronic document
	User Guidance: Utils	1.0	2015-11-23	Electronic document
	User Guidance: SymCfg	1.1	2016-03-16	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 FSP, 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 a test-OS that allows access to the functionalities. 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 conducted according to the following testing approach:

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 NXP Crypto Library. In addition, both external ([BSI-RSA], [BSI-ECC]) and internal attack lists are used to augment the JIL attack list.
2. *Validation of security functionalities*

This step identifies the implemented security functionalities and performs tests to verify implementation and to validate proper functioning. (ATE)

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. (AVA)
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. (AVA)
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. (AVA)
6. *Penetration testing*
   This step performs the penetration tests identified in step 4 and step 5. (AVA)
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 NXP Crypto Library against attackers possessing a high attack potential.

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 following items were used to provide support during the tests:

- A set of card samples (the TOE) containing the following:
  - Hardware sample: P6022P VB in contact mode.
  - Crypto library loaded into the hardware sample.
  - CryptOS loaded into the hardware sample.
- A toolset provided by the developer in order to facilitate recreation of the Cryptographic library, and loading the library and the CryptOS into samples.
- CryptOS documentation

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. These activities revealed that for some cryptographic functionality the security level could be reduced. As the remaining security level still exceeds 80 bits, this is considered sufficient. So no exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Re-used evaluation results

This is 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.

Note that this is a re-certification with major change. Since the previous certification of this TOE, the scope of the underlying platform certification has been updated: MIFARE is now out all scopes, production sites are added and an additional variant is included.

Note: since the first certification of this TOE, the ST has been updated to remove all claims regarding the security of ECC parameter verification. If the security of a composite or end product relies on this functionality, appropriate evaluation of the security properties of this functionality is required.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE (NXP Semiconductors Hamburg, NXP Semiconductors Austria GmbH Styria, NXP Semiconductors Leuven) by the use of site certificates and site re-use report approaches. Sites involved in the development and production of the hardware platform were re-used by composition.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Crypto Library V3.1.x on P6022y VB.

The TOE consists of a hardware part and a software part. This certification covers the configurations of the TOE identified as follows:

- The authenticity of the hardware part of the TOE is checked following the guidance and certification report of the hardware.
- The reference of the software part of the TOE is checked by calculating the SHA-256 hash value of the delivered files and comparing them to reference values provided in the user guidance.

2.9 Results of the Evaluation

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

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Crypto Library V3.1.x on P6022y VB, 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 *[BSI-PP-0084]*.

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

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the implemented cryptographic algorithms 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: MIFARE (out of scope).

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).

3 Security Target

The Crypto Library V3.1.x on P6022y VB Security Target, Rev. 2.0, 22 March 2018 *[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
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
IC	Integrated Circuit
MAC	Message Authentication Code
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
RNG	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:

[BSI-ECC] Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations Version 2.0 (DRAFT2).

[BSI-PP-0084] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014.

[BSI-RSA] Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations Version 1.0.

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

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

[ETR] Evaluation Technical Report Crypto Library V3.1.x on P6022y VB EAL6+, 18-RPT-115, Version 2.0, 09 May 2018.

[ETRfC] ETR for Composite Evaluation Crypto Library V3.1.x on P6022y VB EAL6+, 18-RPT-116, version 2.0, 09 May 2018.

[HW-CERT] Certification report BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software, version 1.0, 18 May 2018.

[HW-ETRfC] Evaluation Technical Report for Composite Evaluation (ETR COMP) for the P6022y VB, version 3, 2018-05-03, TÜV Informationstechnik GmbH (confidential document).

[JIL] Attack methods for Smart cards and similar devices, JIL, version 2.2, January 2013 (restricted distribution).

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.

[ST] Crypto Library V3.1.x on P6022y VB Security Target, Rev. 2.0, 22 March 2018.

[ST-HW] Security Target BSI-DSZ-CC-1059-2018, NXP Secure Smart Card Controller P6022y VB – Security Target, Rev. 2.1, 6 April 2018.

(This is the end of this report).