TÜVRheinland®
Precisely Right.

Certification Report

NXP JCOP 3 P60

Sponsor and developer: ***NXP Semiconductors GmbH***
Business Unit Security & Connectivity
Troplowitzstrasse 20
22529 Hamburg, Germany

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

Report number:	**NSCIB-CC-98209-CR4**
Report version:	**4**
Project number:	**98209**
Author(s):	**Wouter Slegers**
Date:	**14 January 2020**
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 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-20-98209**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors GmbH** **Business Unit Security & Connectivity** **Troplowitzstrasse 20, 22529 Hamburg, Germany**
Product and assurance level	**NXP JCOP 3 P60** Assurance Package: ▪ EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1 Protection Profile Conformance: ▪ ANSSI-PP-2010/03-M01: Java Card Protection Profile – Open Configuration, Version 3.0, May 2012
Project number	**98209**
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 : **02-08-2017**
Date of 2nd issue : **15-01-2018**
Date of 3rd issue : **29-11-2018**
Date of 4th issue : **14-01-2020**
Certificate expiry : **02-08-2022**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

R. De Jonge, Managing director
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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 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 JCOP 3 P60. The developer of the NXP JCOP 3 P60 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 TOE is a composite TOE, consisting of a Java Card smart card operating system, a library which provides cryptographic functions, and an underlying platform, which is a secure micro controller. The TOE provides Java Card 3.0.4 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.2.1 including SCP03. Cryptographic functionality includes AES, DES, Triple-DES (3DES), RSA, RSA-CRT, RSA key-generation, ECC over GF(p), ECC over GF(P) key generation, ECC over GF(p) secure point addition, and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms and includes MAC, CMAC and various modes of operation (e.g. ECB, CBC). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20. It includes a Configuration Service for TOE configuration and patch loading purposes. The Secure Box feature allows providing native functions to applets through a Secure Box Native Library. Finally, it provides three communication protocols, i.e. ISO/IEC 7816 T=1, T=0 and ISO/IEC 14443 T=CL (contactless) over two physical interfaces (i.e. ISO/IEC 7816 and ISO/IEC 14443).

Note that Match-on-Card (MoC) libraries are included in the TOE, but as there are no security claims on these, the biometric functionality has not been assessed, only the self-protection of the TSF.

Please note that a Secure Box Native Library is not part of the TOE, the Secure Box feature however is part of the TOE.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 02-08-2017, recertified on 15-01-2018 and maintained on 19-05-2018, recertified on 29-11-2018 and maintained on 29 July 2019. The re-evaluation also took place by Brightsight B.V. and was completed on 13-01-2020 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 fourth issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are the recertification of the hardware platform with changes to the guidance, the recertification of the cryptographic library, and an associated change to the TOE’s guidance and ST.

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 JCOP 3 P60, 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 JCOP 3 P60 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 the TOE meets the EAL5 augmented (EAL5(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (ST TOE Summary Specification), ALC_FLR.1 (Flaw remediation), ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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]*.

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

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP 3 P60 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Type	Name	Version	Date	Form of delivery
Hardware	NXP Secure Smart Card Controller P6022y VB	P6022J VB (y = J) Nameplate "9072B"	18 January 2016	Based on [HW-ST] Section 1.4.1.3: TOE Components
	Security IC Dedicated Software			
	Test ROM software	10.1D	25-04-2015	
	Boot ROM software	10.1D	25-04-2015	
	Firmware Operating System (FOS)	0C.60, 0C.70	04-2016 04-2016	
	Security IC Embedded Software			
	ROM Code (Platform ID)	JxHyyy0018D80400 *(svn6360; "OSB RC8")* JxHyyy0019790400 *(svn6521; "OSB RC9")* JxHyyy0077020400 *(svn7702; "OSC RC9")*	-	
	Patch Code (Patch ID)	JxHyyy00 18D8 0400 *(svn6360; "OSB RC8") with* 02 00 00 00 00 00 00 00 (PL2) 04 00 00 00 00 00 00 00 (PL4) JxHyyy0019790400 *(svn6521; "OSB RC9") with* 00 00 00 00 00 00 00 00 (no patch) 03 00 00 00 00 00 00 00 (PL3) 04 00 00 00 00 00 00 00 (PL4) JxHyyy0077020400 (svn7702; "OSC RC9") with 01 00 00 00 00 00 00 00 (PL1)	-	

To ensure secure usage a set of guidance documents is provided together with the NXP JCOP 3 P60. Details can be found in section ”Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.3.2.

2.2 Security Policy

The TOE is a composite TOE, consisting of a Java Card smart card operating system, a library which provides cryptographic functions, and an underlying platform, which is a secure micro controller. The TOE provides Java Card 3.0.4 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.2.1 including SCP03. Cryptographic functionality includes AES, DES, Triple-DES (3DES), RSA, RSA-CRT, RSA key-generation, ECC over GF(p), ECC over GF(P) key generation, ECC over GF(p) secure point addition, and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms and includes MAC, CMAC and various modes of operation (e.g. ECB, CBC). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20. Finally, it provides three communication protocols, i.e. ISO/IEC 7816 T=1, T=0 and ISO/IEC 14443 T=CL (contactless) over two physical interfaces (i.e. ISO/IEC 7816 and ISO/IEC 14443).

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 4.8 of the *[ST]*.

2.3.2 Clarification of scope

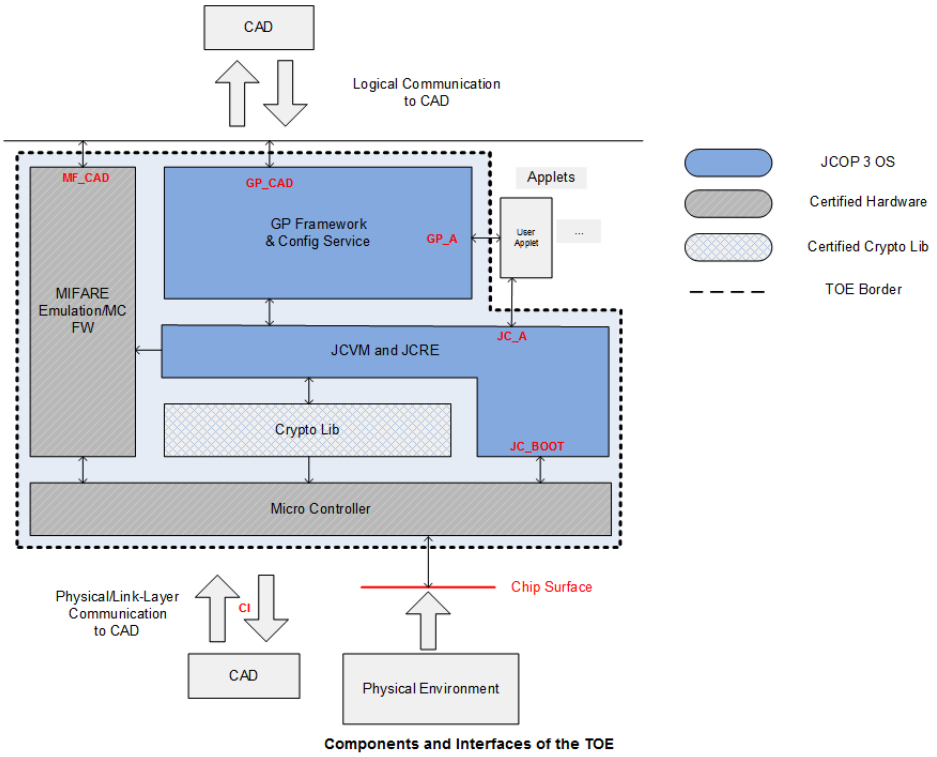
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that the MoC libraries are included in the TOE, but as there are no security claims on these, the biometric functionality has not been assessed, only the self-protection of the TSF.

Note also that the Secure Box mechanism has been evaluated, not any specific Secure Box Native Library.

2.4 Architectural Information

The architecture of the TOE is as follows:



Components and Interfaces of the TOE

The TOE is a composite TOE, consisting of:

- **Hardware** "NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software" used as evaluated platform *[HW-CERT]*, where only the P6022J VB* (y=J) configuration is allowed for this TOE;
- **Cryptographic Library** "Crypto Library V3.1.x on P6022y VB" built upon this hardware platform *[CL-CERT],* where only the V3.1.2 (x=2) version is allowed for this TOE.
- **Operating System** "JCOP OS" built upon this hardware platform and using the Crypto Library as follows:
  - "svn6360", or
  - "svn6521", or
  - "svn7702"
- **Patch Code**, as follows:
  - For "svn6360": "02 00 00 00 00 00 00 00" or "04 00 00 00 00 00 00 00"
  - For "svn6521": "03 00 00 00 00 00 00 00" or "04 00 00 00 00 00 00 00" or "00 00 00 00 00 00 00 00" (no patches)
  - For "svn7702": "01 00 00 00 00 00 00 00"

The TOE is a Java Card (version 3.0.4) smart card allowing post-issuance loading of applications using the Global Platform (version 2.2.1) framework. It includes a Configuration Service for TOE configuration and patch loading purposes. The Secure Box feature allows providing native functions to applets through a Secure Box Native Library. Please note that a Secure Box Native Library is not part of the TOE, the Secure Box feature however is part of the TOE. The MIFARE and FIDO U2F related functionality is not part of the evaluation.

2.5 Documentation

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

Type	Name	Version	Date	Form of delivery
Document	User Guidance and Administrator Manual	3.2 for EMV and Secure ID Use Cases ("OSB" configurations)	4-9-2019	Electronic document
		1.6 for Fingerprint and Token Use Cases ("OSC" configurations)	4-9-2019	Electronic document
Document	ES_JCOP 3 SECID P60 CS (OSB) Errata Sheet	2.3	07-06-2017	Electronic document
Document	ES_JCOP 3 SECID P60 CS (OSB) Errata Sheet for Morpho,	2.2	07-06-2017	Electronic document
Document	Product Data Sheet SmartMX2 family P6022y VB Secure high-performance smart card controller	3.6	22-08-2019	Electronic document
Document	HW Wafer and delivery specification	3.3	12-07-2019	Electronic document

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has performed extensive testing on functional specification, subsystem and module level. All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, as the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

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 penetration tests are devised after performing the Evaluator Vulnerability Analysis. The reference for attack techniques against smart card-based devices such as the TOE must be protected against is the document named "Attack methods for smart cards" and referenced as *[JIL-AM]*. The susceptibility of the TOE to these attacks has been analysed in a white box investigation conforming to AVA_VAN.5. This analysis has followed the following steps:

1. *Inventory of required resistance*
   This step uses the JIL attack list as described in *[JIL-AM]* as a reference for completeness and studies the ST claims to decide which attacks in the JIL attack list apply for the TOE.
2. *Validation of security functionalities*
   This step identifies the implemented security functionalities and performs tests to verify implementation and to validate proper functioning (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 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 the TOE against attackers possessing a high attack potential.

A number of penetration tests were performed on an earlier TOE version. For this evaluation an analysis was performed that allowed full use of the penetration test results. Also, one configuration of the TOE was used and results reassessed for the other three configurations.

In total 6 side channel attacks and 10 perturbation attacks were performed, some on an earlier version of the TOE but still applicable to this TOE.

2.6.3 Test Configuration

Testing was performed on the following TOE test configurations:

Component	Versions
Hardware IC	P6022y VB where y = J (P6022J VB) in DIL24 and CLCC68 packaging
Crypto Library	“Crypto Library V3.1.x on P6022y VB” with minor version (x = 2) resulting in V3.1.2
JCOP OS	“JxHyyy0018D80400” (SVN 6360)
Patch code	“E2 00 00 00 00 00 00 00” (Patch 02 + attack counter patch)

Table 1. Test configuration (OSB.2).

Component	Versions
Hardware IC	P6022y VB where y = J (P6022J VB) in DIL24 and CLCC68 packaging
Crypto Library	“Crypto Library V3.1.x on P6022y VB” with minor version (x = 2) resulting in V3.1.2
JCOP OS	“JxHyyy0019790400” (SVN 6521)
Patch code	“E3 00 00 00 00 00 00 00” (Patch 03 + attack counter patch)

Table 2. Test configuration (“OSB RC9 PL3”).

Component	Versions

Component	Versions
Hardware IC	P6022y VB where y = J (P6022J VB) in DIL24 and CLCC68 packaging
Crypto Library	“Crypto Library V3.1.x on P6022y VB” with minor version (x = 2) resulting in V3.1.2
JCOP OS	“JxHyyy0077020400” (SVN 7702)
Patch code	“E1 00 00 00 00 00 00 00” (Patch 01 + attack counter patch)

Table 3. Test configuration (“OSC RC9 PL1”).

As part of the re-certification, test configuration “OSB.2 (svn 636)” was used.

Testing was performed by employing test applets using TSFIs: JC_A and GP_CAD over the IEO/IEC 7816 T=0 interface.

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 wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5). Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”.

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80 bits, this is considered sufficient. So no exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Re-used evaluation results

This is 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. Perturbation retesting in test configuration OSB RC8 (svn 6360) was performed and considered to cover all variants.

Sites involved in the development and production of the hardware platform and crypto library were re-used by composition.

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 4 site certificates:

- NXP Semiconductors Hamburg
- NXP Semiconductors Austria GmbH Syria
- NXP Semiconductors Livingston
- NXP HTC60

Three site audits associated to the Match on Card functionality have been re-used. No Site Reuse reports have been made.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP JCOP 3 P60 as described in the identification part of this report.

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 NXP JCOP 3 P60, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with AVA_VAN.5, ALC_DVS.2, 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.

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:

- MIFARE and FIDO U2F support (as there are no security claims).

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", sufficiently large cryptographic key sizes shall 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 JCOP 3 P60 Security Target, Rev 4.0, dated 2019-08-23 *[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
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
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands scheme for certification in the area of IT security
PKI	Public Key Infrastructure
PP	Protection Profile
TOE	Target of Evaluation
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
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 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
[CL-CERT]	Certification Report Crypto Library V3.1.x on P6022y VB, NSCIB-CC-67206-CR4, 07 January 2020.
[CL-ETRfC]	ETR for Composite Evaluation Crypto Library V3.1.x on P6022y VB EAL6+, 18-RPT-116, v6.0, 28 November 2019.
[CL-ST]	Crypto Library V3.1.x on P6022y VB Security Target, v2.0, 22 March 2018.
[ETR]	Evaluation Report on the IAR NXP JCOP 3 P60 - Recertification, 19-RPT-812, version 5.0, 13 January 2020.
[ETRfC]	Evaluation Technical Report for Composition NXP JCOP 3 P60 – EAL5+, 17-RPT-308, version 13.0, dated 13 January 2020.
[HW-CERT]	Certification report BSI-DSZ-CC-1059-V2-2019 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software, 24 June 2019.
[HW-ETRfC]	Evaluation Technical Report for Composite Evaluation (ETR COMP), P6022y VB, BSI-DSZ-CC-1059-V3, Version 3, 2019-09-19.
[HW-ST]	NXP Secure Smart Card Controller P6022y VB, Security Target, Rev. 2.6, 2019-08-23.
[JIL-AM]	JIL, Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.2, January 2013.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Java Card Protection Profile - Open Configuration, Version 3.0, Certified by ANSSI, the French Certification Body May, 2012. This TOE does not support the optional Java Card RMI.
[ST]	JCOP 3 P60 Security Target, Rev 4.0, dated 2019-08-23.
[ST-lite]	JCOP 3 P60, Security Target Lite, Rev. 4.0, 2019-08-23
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).