Certification Report

NXP JCOP 4.0 on P73N2M0

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-111441-CR**

Report version: **1**

Project number: **111441**

Author(s): **Claire Loiseaux, Wouter Slegers**

Date: **14 June 2018**

Number of pages: 16

Number of appendices: **0**

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**CC-18-111441**

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 4.0 on P73N2M0** Assurance Package: ▪ EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 Protection Profile Conformance ▪ Java Card Protection Profile – Open Configuration, Version 3.0, May 2012 Published by Oracle, Inc.
Project number	**111441**
Evaluation facility	**Brightsight BV located in Delft, The Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

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

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity	Date of 1st issue : **14-06-2018** Certificate expiry : **14-06-2023**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

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

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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 4.0 on P73N2M0. The developer of the NXP JCOP 4.0 on P73N2M0 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.

This TOE is a composite TOE, consisting of a Java Card smart card operating system, an OS updater, and an underlying platform, which is composed of a library which provides cryptographic functions and a secure micro controller.

The TOE in this Certification Report 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 SCP02.
- Two communication protocols, GlobalPlatform Secure Channel Protocols 03 (Amendment D) and 11 (Amendment F).
- OS Update functionality to update the JCOP OS and/or the Updater OS.
- Config Applet: Software that handles personalization and configuration.
- A Secure Box to run third-party native code
- Factory Reset: to create a Clear List to enable deletion of applets, packages and SDs
- Restricted Mode: A Limited functionality mode allowing reset of the Attack Counter and reading logging information.

Cryptographic functionality includes Triple-DES (3DES), AES, AES-CMAC, RSA-CRT and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms, HMAC and ECC over GF(p). Furthermore, the TOE provides random number generation according to class DRG.4 of AIS 20.

The TOE allows post-issuance downloading of Java Card applications (applets), provided these applets have been verified by an off-card trusted component. A Java Card application developer may develop applications (applets) that are loaded post-issuance to execute on the Java Card JCOP operating system. The Java Card applications are stored in persistent memory of the NXP hardware and are not part of the TOE.

The TOE also includes an OS update component. The UpdaterOS is a standalone operating system that can only be active when JCOP4 OS is not active. Besides the capability to update JCOP4 OS, UpdaterOS is also capable to update itself.

The evaluation of the TOE was conducted as a composite evaluation and uses the results of the CC evaluation of the NXP Secure Smart Card Controller P73N2M0B0.200, certified under the French CC scheme on 16 February 2018 *[HW-CERT]* and the Crypto Library P73N2M0B0.2C0 / 2P0, certified under French CC Scheme on 13 April 2018 *[CL-CERT]*.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 12/06/2018 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 NXP JCOP 4.0 on P73N2M0, 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 4.0 on P73N2M0 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

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

security functionality. This assurance level is augmented with ASE_TSS.2 “TOE summary specification with architectural design summary”, and ALC_FLR.1 “Basic flaw remediation”.

All components required for EAL6 are already met by the augmentations on the underlying hardware apart from SPM. As the SPM for this TOE is independent of the Hardware, the requirements for EAL6 composition are met.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP 4.0 on P73N2M0 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP Secure Smart Card Controller P73N2M0B0.200	P73N2M0B0.200
Firmware	Micro Controller Firmware “MC FW” for booting and low-level functionality of the secure microcontroller.	Firmware v1.5.4
Software	“Security Software” for providing Flash Services and Crypto Library functionality.	Service Software v1.9.0 and Crypto Library v1.0.8
Software	JCOP4 OS including the “OS Update Component”, “Native Applications” and “Config Applet” identified by the Platform Identifier.	J5O1M60121980100

To ensure secure usage a set of guidance documents is provided together with the NXP JCOP 4.0 on P73N2M0. Details can be found in section 2.5 of this report.

The TOE is delivered following the procedures of the hardware part of the TOE, i.e. as a wafer in phase 3 or in packaged form in phase 4 of the smart card life cycle.

Applets can be loaded in phases 3 to 7.

Applets and Native applications are outside the scope of the TOE.

OS update can be triggered in phase 7.

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

2.2 Security Policy

The TOE in this Certification Report 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 SCP02.
- Two communication protocols, GlobalPlatform Secure Channel Protocols 03 (Amendment D) and 11 (Amendment F).
- OS Update functionality to update the JCOP OS and/or the Updater OS.
- Config Applet: Software that handles personalization and configuration.
- A Secure Box to run third-party native code
- Factory Reset: to create a Clear List to enable deletion of applets, packages and SDs
- Restricted Mode: A Limited functionality mode allowing reset of the Attack Counter and reading logging information.

Cryptographic functionality includes Triple-DES (3DES), AES, AES-CMAC, RSA-CRT and SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms, HMAC and ECC over GF(p). Furthermore, the TOE provides random number generation according to class DRG.4 of AIS 20.

The TOE allows post-issuance downloading of Java Card applications (applets), provided these applets have been verified by an off-card trusted component. A Java Card application developer may develop applications (applets) that are loaded post-issuance to execute on the Java Card JCOP operating system. The Java Card applications are stored in persistent memory of the NXP hardware and are not part of the TOE.

The TOE also includes an OS update component. The UpdaterOS is a standalone operating system that can only be active when JCOP4 OS is not active. Besides the capability to update JCOP4 OS, UpdaterOS is also capable to update itself.

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 5.2 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.

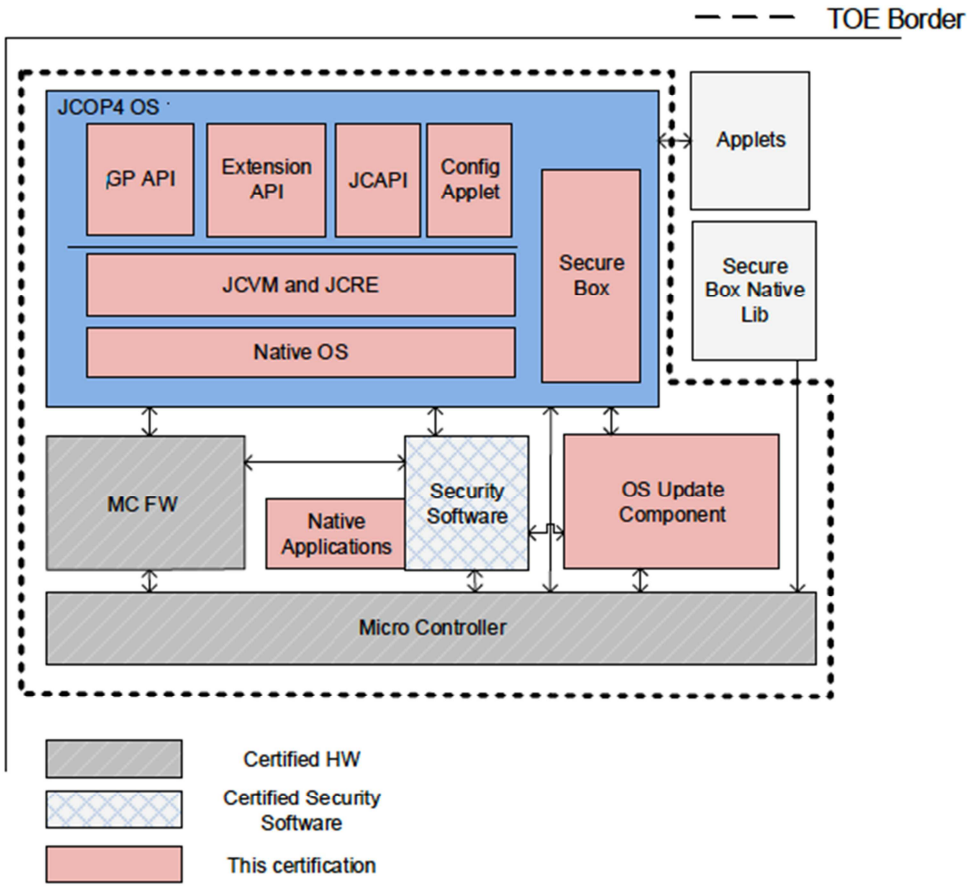
Note that that the Secure Box mechanism has been evaluated, not any specific Secure Box Native Library.

2.4 Architectural Information

The TOE consists of the Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. The software stack can be further split into the following components:

- MC FW: Firmware for booting and low level functionality of the Micro Controller,
- Security Software: Software for implementing cryptographic operations on the Micro Controller
- OS Update Component Software to update JCOP4 OS or UpdaterOS, called OS Update Component.
- JCOP4 OS Software for implementing
    - Native OS low level functionality,
    - JCVM and JCRE: Software for implementing the Java Card Virtual Machine and a Java Card Runtime Environment
    - JCAPI Software for implementing Java Card Application Programming Interface [
    - GP API Software for implementing content management according to GlobalPlatform
    - Extension API Software that implements a proprietary programming interface,
    - Config Applet: Software that handles personalization and configuration,
    - Secure Box: Software to run third party native code (Secure Box Native Lib).
    - Native Applications Software for implementing third party functionality.

The TOE does not include any software on the application layer (Java Card applets). See *[ST]* section 1.2 and 1.3 for details.



2.5 Documentation

In addition to the documentation of the Hardware, the following documentation is provided with the product by the developer to the customer:

Identifier	Version	Date
JCOP 4.0 R1.00.1, User Guidance Manual	Rev. 1.4	2017-08-24
Common Criteria Requirements for NXP PN8xy Products	Rev. 1.1	2017-09-14

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 SFR-enforcing 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.

The tests cover all security functions and aspects of the TSF. The developer used a set of test suites (industry standard and proprietary ones) and tools to test the TOE (SO28 and PN80T package) as well as an emulator, PC Platform and FPGA tool as some tests could only be performed in such environment. The identification was checked based on the SVN number. The developer uses a distributed test environment to allow usage of a vast amount of simultaneously driven testing equipment. The developer has performed extensive testing on FSP, subsystem, module and module interface level. The tests are performed by NXP through execution of the test scripts using an automated and distributed system. Test tools and scripts are extensively used to verify that the tests return expected values.

The ordering dependencies were analysed. The developer performed random order testing to identify any ordering dependencies. This was done for Unit Tests, System Tests and Acceptance Tests. For most (commercial) test suites there are no claims on ordering dependencies. For these situations tests were executed both in random order as in alphabetical order and the results were compared.

Code coverage analysis is used by NXP to verify overall test completeness. Test benches for the various TOE parts are executed using code coverage measurement and analysis tools to determine the code coverage (i.e. lines, branches and/or instructions, depending on tool) of each test bench. Cases with incomplete coverage are analysed. For each tool, the developer has investigated and documented inherent limitations that can lead to coverage being reported as less than 100%. In such cases the developer provided a “gap” analysis with rationales (e.g. attack counter not hit due to redundancy checks).

The evaluator used an agreed approach for evaluating ATE based on code coverage analysis. The evaluator also used an acceptable alternative approach (as described in the application notes, Section 14.2.2 in *[CEM]*) and used analysis of the implementation representation (i.e. inspection of source code) to validate the rationales provided by the developer.

The cryptographic algorithms have been validated as part of the Crypto Library evaluation.

The protection against side channel analysis and perturbation attacks has been verified by the evaluator by performing code inspection of the countermeasures in the implementation representation of the JCOP4 OS, on key handling by the operating system and finally operations not provided by the hardware or Crypto Library. Also, logical attacks were considered.

2.6.2 Independent Penetration Testing

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. The penetration tests are devised after performing the Evaluator Vulnerability Analysis. This approach has followed the following steps:

1. *Inventory of required resistance*
   As part of this step, the attack list as described in *[JIL-AM]* is used as a reference for completeness. The ST claims are studied to decide which attacks in the list apply for the TOE.

2. *Validation of security functionalities*
   As part of this step, the implemented security functionality is identified and tests are performed to verify implementation and validate proper functioning (ATE).

3. *Vulnerability analysis*
   As part of this step, an overview is made showing which attacks the implemented security functionality is meant to provide protection against. Secondly, the design of the implemented security functionality is studied. Thirdly, an analysis is performed to determine whether the design contains possible (potential) vulnerabilities against the attacks listed as part of step 1 (AVA).

4. *Analysis of input from other evaluation activities*
   As part of this step, an analysis is made of input originating from other CC evaluation classes. This input consists of possible (potential) vulnerabilities. Secondly, an analysis is made of the TOE in

its indented environment to check if the developer vulnerability analysis provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance (AVA).

5. *Design assurance evaluation*
   As part of this step, the list defined in step 1 is used for design analysis from an attack perspective. Based on this design analysis it is determined if the design provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance (AVA).
6. *Penetration testing*
   As part of this step, penetration tests are defined based on results obtained as part of step 4 and 5 (AVA) followed by actually performing penetration testing.
7. *Conclusions on resistance*
   As part of this final step, a rating is computed compliant to *[JIL-AM]* on the obtained results during penetration testing in relation to the assurance already gained during the design analysis. Based on the computed ratings conclusions are drawn on the resistance of the TOE against attackers possessing a high attack potential.

Penetration testing of this TOE was divided into a number of campaigns, i.e.:

- Penetration testing performed as part of an EMVCo evaluation of the TOE.
- Common Criteria (actual) penetration testing
- Common Criteria (refreshment #1) penetration testing
- Common Criteria (refreshment #2) penetration testing

In agreement with the certifier, re-use of the penetration test results was done along with repetition of a number of penetration tests.

Test Configuration

Testing was performed on the following TOE test configuration:

Component	Version
Hardware IC	P73N2M0B0.2C0
Security Software	Service Software v1.9.0 Crypto Library v1.0.8
JCOP OS	J5O1M60121980100 (svn = “74136”)

Testing was performed by employing test applets using TSFIs: JC_A and GP_CAD over the SWP interface.

It is noted that the TOE was provided in a physical packaging (CLCC68) enabling easy access to the physical surface of the chip necessary to perform perturbation attacks using light and perform EMFI attacks.

2.6.3 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 algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

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

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 Austria - Gratkorn,
- REC sp. z o.o. Poland - Wroclaw,
- NXP India – Bangalore,
- NXP Semiconductors Taiwan - Kaohsiung

and 1 site re-use report approaches:

- NXP Semiconductors Germany - Hamburg.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP JCOP 4.0 on P73N2M0.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references a 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 4.0 on P73N2M0, to be **CC Part 2 extended, CC Part 3 conformant**, (check ST compliance claim) 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 'demonstrable' conformance to the Protection Profile Java Card Protection Profile – Open Configuration, Version 3.0, May 2012 *[JCPP]*.

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.

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

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).

The TOE uses the RSA key generation of the underlying hardware and crypto library directly. Note that the certification of the underlying hardware *[HW-CERT]* and crypto library *[CL-CERT]* has _not_ considered the ROCA attack, however there is no reason to consider this attack applicable to the TOE.

3 Security Target

The NXP JCOP 4 on P73N2M0 Secure Smart Card Controller Security Target, Rev. 1.3 – 2018-06-01 *[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 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
[CL-CERT]	Certificate ANSSI-CC-2018/19, P73N2M0B0.2C0/2P0, 2018-04-13.
[CL-ETRfC]	Evaluation Technical Report Lite, P73-CL Project, v2.1, 2018-03-26.
[CL-ST]	NXP P73N2M0B0.2C0/2P0, Crypto Library Services Software, Security Target, Rev. 1.2, 2018-03-19.
[ETR]	Evaluation Technical Report NXP JCOP 4.0 on P73N2M0, 17-RPT-643 ETR JCOP 4 P73, v5.0, 2018-06-01.
[ETRfC]	ETR for Composite Evaluation NXP JCOP 4.0 on P73N2M0, 18-RPT-272 ETR JCOP 4 P73, v2.0, 2018-06-01.
[HW-CERT]	Certificate ANSSI-CC-2018/08, P73N2M0B0.200, 2018-02-16.
[HW-ETRfC]	Evaluation Technical Report Lite, P73 Project, v2.0, 2018-02-09.
[HW-ST]	P73N2M9B0.200, Security Target, Rev. 1.1, 2017-12-20.
[JCPP]	Java Card Protection Profile – Open Configuration, Version 3.0, May 2012 Published by Oracle, Inc. registered under the reference ANSSI-PP-2010/03-M01
[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 2.4, 2017-09-27.
[ST]	NXP JCOP 4 on P73N2M0 Secure Smart Card Controller Security Target, Rev. 1.3 – 2018-06-01.
[ST-lite]	NXP JCOP 4 on P73N2M0 Secure Smart Card Controller Security Target Lite, Rev. 1.3 – 2018-06-01.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).