TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Certification Report

NXP JCOP 4.2 on P73N2M0B0.2C2

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-156530-CR**

Report version: **1**

Project number: **156530**

Author(s): **Claire Loiseaux**

Date: **1 April 2019**

Number of pages: **13**

Number of appendices: **0**

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

Certificate

Standard

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number   **CC-19-156530**

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

<u>NXP JCOP 4.2 on P73N2M0B0.2C2</u>

Assurance Package:
- EAL5 augmented with AVA_VAN.5, ASE_TSS.2, ALC_DVS.2 and ALC_FLR.1

Protection Profile Conformance:
- Java Card Protection Profile – Open Configuration, Version 3.0, Certified by ANSSI, the French Certification Body, May 2012

Project number   **156530**

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)

Common Criteria Recognition
Arrangement for components
up to EAL2

SOGIS Mutual Recognition
Agreement for components up
to EAL 7

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

Validity

Date of 1ˢᵗ issue   : **04-04-2019**
Certificate expiry : **04-04-2024**

PRODUCTS
RvA C078
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.

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

TÜVRheinland®
Precisely Right.

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 4.2 on P73N2M0B0.2C2. The developer of the NXP JCOP 4.2 on P73N2M0B0.2C2 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 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.

It includes also NXP Proprietary Functionality: Config Applet, OS Update Component, Applet Migration, Restricted Mode and Error Detection Code (EDC) API.

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

Note that proprietary applications have been included in the TOE, but as there are no security claims on these applications in this certificate, these applications have not been assessed, only the self-protection of the TSF.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 1 April 2019 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 4.2 on P73N2M0B0.2C2, 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 4.2 on P73N2M0B0.2C2 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 EAL5 augmented (EAL5(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), ASE_TSS.2 ("TOE summary specification with architectural design summary"), ALC_FLR.1 (Basic flaw remediation) 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 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

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

---

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

2   Certification Results

2.1   Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP 4.2 on P73N2M0B0.2C2 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Type	Name	Version	
Hardware	NXP Secure Smart Card Controller P73N2M0B0.202	P73N2M0B0.202	P73N2M0B0.2C2
Software	Micro Controller Firmware "MC FW" for booting and low-level functionality of the secure microcontroller.	Firmware v1.5.4 which includes: - Boot_OS v1.2.3, with patch PL2 V8 - Factory_OS v1.4.4 - Service_ROM v1.5.2	
	"Security Software" for providing Flash Services and Crypto Library functionality.	Service Software v1.9.14 Crypto Library v1.0.8	
Software	JCOP4 OS including the "OS Update Component", "Native Applications" and "Config Applet" identified by the Platform Identifier.	Platform Identifier J5Q2M00148750000 (SVN = "84085")	

To ensure secure usage a set of guidance documents is provided together with the NXP JCOP 4.2 on P73N2M0B0.2C2. Details can be found in section 2.5 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

This TOE is a composite TOE, consisting of a Java Card smart card operating system, an OS updater, an applet migration feature, a restricted mode and an underlying platform, which is composed of a library which provides cryptographic functions and 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. It includes also NXP proprietary functionalities:

- Config Applet: JCOP4.2 OS includes a Config Applet that can be used for configuration of the TOE.
- OS Update Component: Proprietary functionality that can update JCOP4.2 OS or UpdaterOS.
- Applet Migration: Keep User Data, Key Data or PIN Data after updating an applet.
- Restricted Mode: In Restricted Mode only very limited functionality of the TOE is available such as, e.g.: reading logging information or resetting the Attack Counter.
- Error Detection Code (EDC) API.

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

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 4.4 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.

Note that proprietary applications have been included in the TOE, but as there are no security claims on these applications in this certificate, these applications have not been assessed, only the self-protection of the TSF.

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST], of the TOE can be depicted as follows:
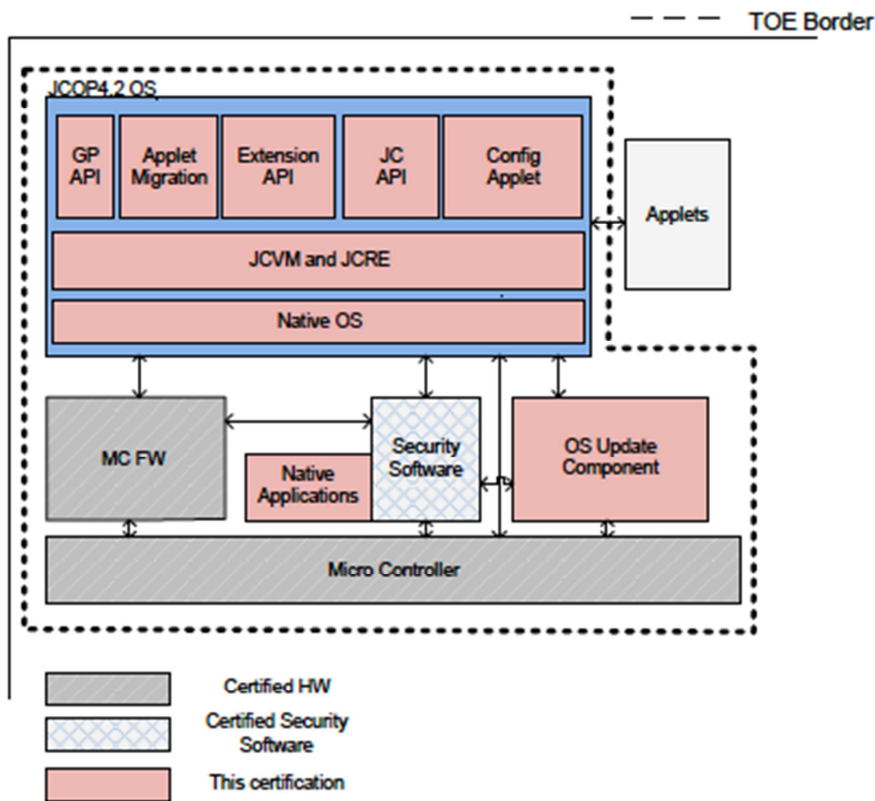

Fig. 1.1: Components of the TOE

2.5 Documentation

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

Reference	Name	Version	Date
[UGM]	JCOP 4.2 R1.10.0 (JCOP 4.2 7.2.10) User Guidance Manual	v1.28	22-01-2019

Reference	Name	Version	Date
[UGM_ADD]	JCOP 4.2 R1.10.0 (JCOP 4.2 7.2.10) User guidance Manual Addendum	v1.23	02-02-2018
[UGM_Anomaly]	JCOP 4.2 R1.10.0 (JCOP 4.2 7.2.10 User Anomaly Sheet	v1.8	20-03-2017
[AGD_PRE]	Common Criteria Requirements for PN8xy products	v1.1	14-09-2017

2.6 IT Product Testing

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

2.6.1 Testing approach and depth

The developer used a set of test suites (industry standard and proprietary ones) and tools to test the TOE 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.

Code coverage analysis is used by NXP to verify overall test completeness. 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 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.

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.

- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis, the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed taking into account the attack methods in *[JIL-AM]* and attack potential in *[JIL-AP]*. An important source for assurance in this step are the technical reports *[HW-ETRfC]* and *[CL-ETRfC]* of the underlying platform.

- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable by using *[JIL-AP]*. For most of the potential vulnerabilities a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

According to *[NSI_08]* a testing re-use rationale was provided. Four complementary tests were performed against a test effort of 6 weeks. See details in *[ETR]*.

2.6.3 Test Configuration

The TOE was tested (Unit Tests, System Tests and Acceptance Tests) in the following configurations:

- FPGA Emulator and PC Platform
- TOE (SO28 package and PN80T package)
- Using DWP 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 wide range of key sizes (see *[ST]*), including those with a sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. 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 2 site certificates

- NXP Semiconductors in Hamburg,
- NXP Semiconductors India Private limited,

and 2 site re-use report approach.

- NXP Semiconductors Taiwan Ltd. (APK) Assembly Plant Kaohsiung
- NXP Semiconductors Austria GmbH Styria Gratkorn.

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 NXP JCOP 4.2 on P73N2M0B0.2C2.

The TOE can only be in a single evaluated configuration. Changes that can be made using the Config Applet are within this configuration.

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 4.2 on P73N2M0B0.2C2, to be CC Part 2 extended, CC Part 3 conformant and to meet the requirements of EAL 5 augmented with AVA_VAN.5, ASE_TSS.2, ALC_DVS.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 *[JC 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 implemented cryptographic algorithms and protocols was not rated in the course of this evaluation.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". In order to be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

---

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

TÜVRheinland®
Precisely Right.

3   Security Target

The NXP JCOP4.2 on P73N2M0B0.2C2 Security Target, Version 1.3, 2019-02-21. *[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:

ACL	Access Control List`
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
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

TÜVRheinland®
Precisely Right.

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]	Rapport de certification ANSSI-CC-2018/55, P73N2M0B0.2C2, dated 2018-12-14.
[CL-ETRfC]	Evaluation Technical Report Lite, P73B project, P73N2M0B0.2C2, P73B_ETR-Lite_V1.1/1.1.
[CL-ST]	NXP P73N2M0B.2C2 Security Target Lite, Version 2.5, 13 November 2018.
[ETR]	Evaluation Technical Report NXP JCOP 4.2 on P73N2M0B0.2C2, 19-RPT-105 Evaluation Technical Report, Version 4.0, 2019-03-15.
[ETRfC]	ETR for Composite Evaluation NXP JCOP 4.2 on P73N2M0B0.2C2, 19-RPT-104 Evaluation Technical Report for Composition JCOP4.2 on P73, Version 5.0, 2019-03-15.
[HW-CERT]	Rapport de certification ANSSI-CC-2018/52, P73N2M0B0.202, dated 2018-11-16.
[HW-ETRfC]	Evaluation Technical Report Lite, P73A project, P73N2M0B0.202, P73A_ETR-Lite_V1.1/1.1.
[HW-ST]	NXP P73N2M0B.202 Security Target Lite, Version 2.4, 2 November 2018.
[JC PP]	Java Card Protection Profile – Open Configuration, Version 3.0, Certified by ANSSI, May 2012.
[JIL-AP]	JIL, (Mandatory) Application of Attack Potential to Smartcards, Version 2.9, January 2013.
[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, 27 Sept 2017.
[NSI_08]	NSI_08_Performing_Testing_v2.4, 2018-06-01.
[ST]	NXP JCOP4.2 on P73N2M0B0.2C2 Security Target, Version 1.3, 2019-02-21.
[ST-lite]	NXP JCOP4.2 on P73N2M0B0.2C2 Security Target Lite, Version 1.2, 2019-02-21.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).