Version 2022-01

Certification Report

NXP JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element

Sponsor and developer: ***NXP Semiconductors NV***
High Tech Campus 60
5656 AG
Eindhoven
The Netherlands

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-156530-CR4**

Report version: **1**

Project number: **156530_4**

Author(s): **Andy Brown**

Date: **02 December 2022**

Number of pages: **14**

Number of appendices: **0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Head Office:
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 Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 licence 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, 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 authorised only if the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element. The developer of the NXP JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element is NXP Semiconductors NV located in Eindhoven, The Netherlands and they also act as the sponsor of the evaluation. 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 Java Card with GP functionality. It can be used to load, install, instantiate and execute off-card verified Java Card applets.

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 and preparation for Java Card 3.0.5 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 was evaluated initially by SGS Brightsight B.V located in Delft, The Netherlands and was certified on 01 April 2019. A re-evaluation also took place by SGS Brightsight B.V. and was completed on 27 January 2020 with the approval of the ETR. A second re-evaluation also took place by SGS Brightsight B.V. and was completed on 24-09-2020 with the approval of the ETR. This third re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 02 December 2022 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]*.

The second issue of the Certification Report was a result of a “recertification with major changes”. The major changes were the addition of two variants, JCOP 4.5 and JCOP 4.6, with a renaming of the TOE to “JCOP 4.x on P73N2M0B0.2C2/2C6 Series” and recertification of the underlying hardware.

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

The third issue of the Certification Report was a result of a “recertification with major changes”.

The major changes were the addition of variant JCOP 4.8 and a renaming of the TOE to “JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element".

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

This fourth issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are the claim of conformance to Java Card Protection Profile – Open Configuration Protection Profile version 3.1, *[JC PP]* and addition of variant JCOP 4.10 with associated guidance.

Additionally, some development activities have been relocated from one site to a different, already-evaluated site.

The security evaluation reused the evaluation results of previously performed evaluations. This included the use of a site reuse report to cover some development activities that have been relocated from a site that was used during the previous certification activities.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 4.x on P73N2M0B0.2C2/2C6 Secure Element, 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.x on P73N2M0B0.2C2/2C6 Secure Element 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 Include the following, if applicable: 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 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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. Note that the certification results apply only 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 available for public review.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element from NXP Semiconductors NV located in Eindhoven, The Netherlands.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware (Part of P73 certificates)	NXP High-Performance secure controller "P73N2M0B0.202"	B.02
Software / Firmware (Part of SN73 certificates)	Factory OS	1.4.4
	Boot OS	1.2.3 PL2 v8
	Flash Driver Support	1.5.2
	"P73N2M0B0.2C2" Service Software	1.9.14
	"P73N2M0B0.2C2" Crypto Library	1.0.8
	"P732N2M0B0.2C6" Service Software	1.9.18
	"P732N2M0B0.2C6" Crypto Library	1.0.8
Software	"JCOP 4.2 R1.10.0" OS, Native applications and OS Update Component	JCOP 4.2 R1.10.0
	"JCOP 4.5 R1.07.0" OS, Native applications and OS Update	JCOP 4.5 R1.07.0
	Configuration "JCOP 4.6 R1.04.0" OS, Native applications and OS Update	JCOP 4.6 R1.04.0
	Configuration "JCOP 4.8 R1.01.0" OS, Native applications and OS Update	JCOP 4.8 R1.01.0
	Configuration "JCOP 4.10 R1.05.0" OS, Native applications and OS Update	JCOP 4.10 R1.05.0

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element. For details, see section 2.5 "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

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: JCOP OS includes a Config Applet that can be used for configuration of the TOE.
- OS Update Component: Proprietary functionality that can update JCOP OS or UpdaterOS.
- Applet Migration: Keep User Data, Key Data or PIN Data after updating an applet.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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

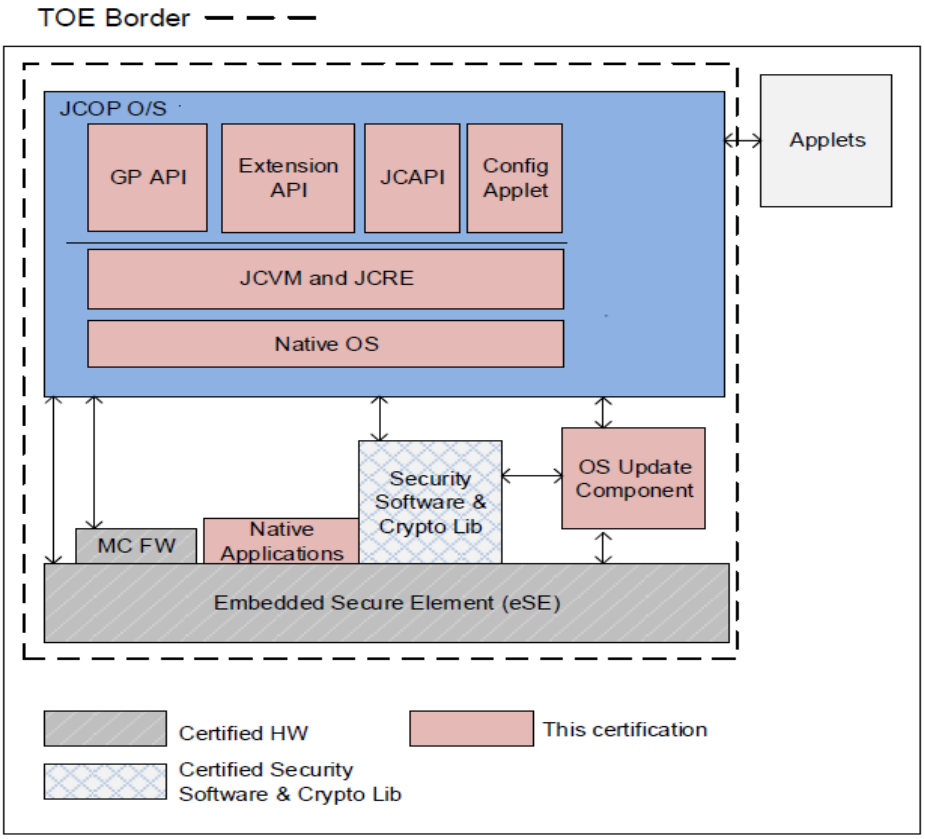
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the *[ST]*.

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.

2.4 Architectural Information

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



Logical architecture of the TOE

The TOE has the following features:

- Cryptographic algorithms and functionality:
  - 3DES for en-/decryption (CBC and ECB) and MAC generation and verification (2-key 3DES, 3-key 3DES, Retail-MAC, CMAC and CBC-MAC).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

- AES (Advanced Encryption Standard) for en-/decryption (GCM, CCM, CBC and ECB) and MAC generation and verification (CMAC, CBC-MAC).
- RSA and RSA CRT for en-/decryption and signature generation and verification.
- RSA and RSA CRT key generation.
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithm.
- Secure SHA-1, Secure SHA-224, Secure SHA-256, Secure SHA-384, Secure SHA-512 hash algorithm.
- HMAC
- ECC over GF(p) for signature generation and verification (ECDSA).
- ECC over GF(p) key generation for key agreement.
- Random number generation according to class DRG.3 of AIS 20

- Java Card 3.0.4 and preparation for Java Card 3.0.5 functionality.
- GlobalPlatform 2.2.1 functionality.
- NXP Proprietary Functionality:
  - Config Applet: JCOP OS includes a Config Applet used for configuration of the TOE.
  - OS Update Component: Proprietary functionality that can update JCOP 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.

2.5 Documentation

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

Identifier	**Version**
JCOP 4 PN8xy Common Criteria Requirements for NXP PN8xy Products	Rev 1.1
JCOP 4.2 R1.10.0 specific documents	
JCOP 4.2 R1.10.0 (JCOP 4.2 7.2.10) User Guidance Manual	Rev 1.34
JCOP 4.2 R1.10.0 (JCOP 4.2 7.2.10) User Guidance Manual Addendum	Rev 1.23
JCOP 4..2 R1.10.0 (JCOP 4.2 7.2.10) Anomaly Sheet	Rev 1.8
JCOP 4.5 R1.07.0 specific documents	
JCOP 4.5 R1.07.0 (JCOP 4.5 9.2.07) User Guidance Manual	Rev 3.13
JCOP 4.5 R1.07.0 (JCOP 4.5 9.2.07) User Guidance Addendum	Rev 3.8
JCOP 4.5 R1.10.0 (JCOP 4.5 9.2.07) Anomaly Sheet	Rev 3.10
JCOP 4.6 R1.04.0 specific documents	
JCOP 4.6 R1.04.0 (JCOP 4.6 11.2.04) User Guidance Manual	Rev 5.9
JCOP 4.6 R1.04.0 (JCOP 4.6 11.2.04) User Guidance Manual Addendum	Rev 5.5
JCOP 4.6 R1.04.0 (JCOP 4.6 11.2.04) Anomaly Sheet	Rev 5.6
JCOP 4.8 R1.01.0 specific documents	
JCOP 4.8 R1.01.0 (JCOP 4.8 13.2.01) User Guidance Manual	Rev 7.4

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

JCOP 4.8 R1.01.0 (JCOP 4.8 13.2.01) User Guidance Manual Addendum	Rev 7.2
JCOP 4.8 R1.01.0 (JCOP 4.8 13.2.01) Anomaly Sheet	Rev 7.2
JCOP 4.10 R1.05.0 specific documents	
JCOP 4.10 R1.05.0 (JCOP 4.10 17.2.05) User Guidance Manual	Rev 10.6
JCOP 4.10 R1.05.0 (JCOP 4.10 17.2.05) User Guidance Manual Addendum	Rev 10.5
JCOP 4.10 R1.05.0 (JCOP 4.10 17.2.05) Anomaly Sheet	Rev 10.5

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. In the baseline evaluation, the evaluators 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 is the technical report *[HW-ETRfC]* of the underlying platform.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

- 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.

In the initial re-certification, 4 complementary tests were performed against a test effort of 6 weeks. In the second re-certification 4 perturbation tests, 1 side channel test and 1 logical test were performed with a test effort of 8 weeks. In this third re-certification the total test effort expended by the evaluators was 10 weeks. During that test campaign, 43% of the total time was spent on Perturbation attacks and 57% on logical tests.

See details in *[ETRfC]*.

2.6.3 Test configuration

During this re-certification with major change, samples were used that provided assurance for all four configurations, i.e. “JCOP 4.2 R1.10.0”, “JCOP 4.5 R1.07.0”, “JCOP 4.6 R1.04.0” and “JCOP 4.8 R1.01.0”, “JCOP 4.10 R1.05.0. Please note that for some tests, intermediate and earlier versions were used. The used intermediate and earlier versions provide assurance for the TOE configurations as the code base and security concepts are shared. The following intermediate versions were used: “JCOP 4.2 R2.11.0”, “JCOP 4.9 R2.03.0”, “JCOP 4.6 R2.02.0” and “JCOP 4.5 R1.05.0”.

2.6.4 Test 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 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

Sites involved in the development and production of the hardware platform were reused by composition.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the software component of the TOE, by use of 7 Site Technical Audit Reports.

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.x on P73N2M0B0.2C2/2C6 Secure Element.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

The TOE can be identified using the Platform Identifier, tag DF20, as explained in Section 1.2 of the respective “User Guidance Manual” listed in section 2.5 of this Certification Report.

The term “Platform” is being used for the entire TOE. This means that the DF20 tag as returned shall have the following value in ASCII format:

JCOP 4.x revision	Identifier
JCOP 4.2 R1.10.0	J5Q2M00148750000
JCOP 4.5 R1.07.0	J5Q2M001C1A10000
JCOP 4.6 R1.04.0	J5Q2M002242B0000
JCOP 4.8 R1.01.0	J5Q2M0027B840000
JCOP 4.10 R1.05.0	J5Q2M00386040000

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2]. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must 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.x on P73N2M0B0.2C2/2C6 Secure Element, 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 *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” 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 concerning 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 must 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. For the evolution of attack methods and techniques to be covered, the customer 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: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. 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 Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The NXP JCOP4.x on P73N2M0B0.2C2/2C6 Secure Element Security Target, Rev. 4.2, 28 September 2022 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions 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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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
[ETR]	Evaluation Technical Report “NXP JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element” – EAL5+, 22-RPT-1301, Version 2.0, 29 November 2022
[ETRfC]	Evaluation Technical Report for Composition “JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element” – EAL5+, 22-RPT-1300, Version 2.0, 29 November 2022
[HW-CERT]	Certificate for P73N2M0B0.202, ANSSI-CC-2018/52-S03, 14 January 2022
[HW-FIRM]	Certificate for P73N2M0B0.2C2, ANSSI-CC-2019/62-S02, 14 January 2022
[HW-ETRfC]	Surveillance Technical report Lite for composition P73_P73-CL_P73A_P73B_P73C6_STR_LITE_V2.0, 7 December 2021, version 2.0
[HW-STLITE]	Security Target Lite, P73N2M0B0.2C2/2C6, rev 3.3, 22 August 2019
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JC PP]	Java Card System – Open Configuration Protection Profile Version 3.1, April 2020, registered under the reference BSI-CC-PP-0099-V2-2020, 06 May 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	NXP JCOP4.x on P73N2M0B0.2C2/2C6 Secure Element Security Target, Rev. 4.2, 28 September 2022
[ST-lite]	NXP JCOP4.x on P73N2M0B0.2C2/2C6 Secure Element Security Target Lite, Rev 4.2, 28 September 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.