Certification Report

NXP JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1

Sponsor and developer:	***NXP Semiconductors N.V.*** **High Tech Campus 60** **5656AG Eindhoven** **The Netherlands**
Evaluation facility:	***TÜV Informationstechnik GmbH*** **Am TÜV 1** **45307 Essen** **Germany**
Report number:	**NSCIB-CC-2200042-02-CR**
Report version:	**1**
Project number:	NSCIB-**2200042-02**
Author(s):	**Jordi Mujal**
Date:	**30 October 2024**
Number of pages:	**14**
Number of appendices:	**0**

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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.

Recognition of the Certificate

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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1. The developer of the NXP JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1 is NXP Semiconductors N.V. located in Eindhoven, The Netherlands 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 platform containing the Java Card OS embedded on the SE310 A0 Secure Element with IC Dedicated Software. The usage of the TOE is focused on security critical applications in small form factors. One main usage scenario is the use in mobile phones, which can use the TOE to enable mobile payment or mobile ticketing with the phone based on the security of the TOE.

The TOE was evaluated initially by TÜV Informationstechnik GmbH located in Essen, Germany and was certified on 28 November 2023. The re-evaluation of the TOE has also been conducted by TÜV Informationstechnik GmbH and was completed on 30 October 2024 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 second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are:

- Adding a new JCOP version

- Changes in the guidance

- Changes in the involved sites regarding life cycle

The security evaluation reused 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 JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1, 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 JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1 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 AVA_VAN.5 (Advanced methodical vulnerability analysis), ASE_TSS.2 (TOE summary specification with architectural design summary), ALC_FLR.1(Basic Flaw Remediation) and 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]* (Parts I, II and III).

TrustCB 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1 from NXP Semiconductors N.V. located in Eindhoven, The Netherlands.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP SE310 – Secure Element	SE310_SE A0.1.000 J2
Software	JCOP 8.x OS including Shared Code (with Cryptolib), FlashOS, CommOS, SystemOS, and SMK.	JCOP 8.0 R1.38.0.1 JCOP 8.1 R1.06.0.1
Byte Code Optimizer Tool	nxp-cap-optimizer	nxp-cap-optimizer-1.0.1

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1. For details, see section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.5.

2.2 Security Policy

The TOE has the following features:

- Hardware-supported features
  - hardware to perform computations on multiprecision integers, which are suitable for public-key cryptography
  - hardware to calculate the Data Encryption Standard with up to three keys
  - hardware to calculate the Advanced Encryption Standard (AES) with different key lengths
  - hardware to support Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Counter (CTR) modes of operation for symmetric-key cryptographic block ciphers
  - hardware to support Galois/Counter Mode (GCM) of operation for symmetric-key cryptographic block ciphers
  - hardware to serve with True Random Numbers
  - hardware to control access to memories and hardware components.
- Cryptographic algorithms and functionality
  - AES
  - Triple-DES (3DES)
  - RSA for encryption/decryption and signature generation and verification
  - RSA key generation
  - ECDSA signature generation and verification
  - ECDH key exchange

- ECC key generation
- ECC point operations and key validation
- Diffie Hellman key exchange on Montgomery Curves over GF(p)
- Key generation for the Diffie Hellman key exchange on Montgomery Curves over GF(p))
- EdDSA key generation and signature verification
- EdDSA signature generation (only in JCOP 8.1 R1.06.0.1 version)
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms
- HMAC algorithms
- Data Protection Module for a secure storage of the sensitive data.
- Random number generation according to class DRG.3 or DRG.4 of AIS20 and initialized (seeded) by the hardware random number generator of the TOE.

- Java Card 3.1 functionality
- GlobalPlatform 2.3.1 functionality
- NXP proprietary functionality
  - Runtime Configuration Interface: Config Applet that can be used for configuration of the TOE.
  - OS Update Component: Proprietary functionality that can update JCOP OS, Crypto Lib, Flash Services Software or Updater OS. This component allows only NXP authorised updates to the product.
  - Restricted Mode: In Restricted Mode only very limited functionality of the TOE is available such as reading logging information or resetting the Attack Counter.
  - Image4 (IM4): Software which ensures the customer authorisation of any product updates using OS update or Applet Migration features, and provides features to make the update management easier.
  - Error Detection Code (EDC) API.

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.

The following components of the platform are not part of the TOE:

• HW NFC Controller Subsystem and Power Management Unit (see *[HW-CERT]*)

• JCOP eUICC and any other secondary JCOP xxx (optional)

• CommOS

The following functionality is also present without specific security claims:

• eUICC features hosted in eUICC domain outside the boundaries of the TOE

• 5G features as per SIM Alliance 2.3

• Programmable Timeout for SMB with Limitations.

• CPLC data made available through SystemInfo.

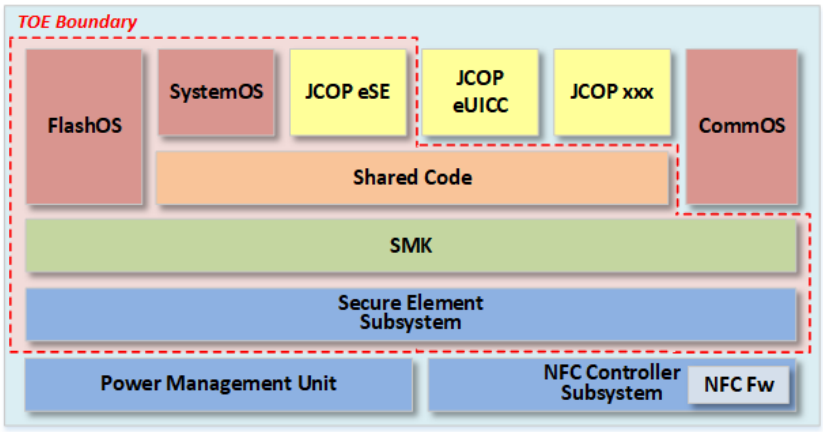
• Proprietary Bytecode Compression applied after BCV. Some standard bytecodes are replaced by optimized byte codes (one to one) with exactly the same operation.

• Compliance to Secure Element configuration, Common Implementation Configuration, UICC Configuration, and UICC Configuration Contactless Extension

• For JCOP 8.0 R1.38.0.1 EdDSA signature generation

2.4 Architectural Information

The top-level block diagram of the TOE is depicted in the following figure.



2.5 Documentation

For JCOP 8.0 R1.38.0.1, the following documentation is provided with the product by the developer to the customer:

Identifier	Version
JCOP 8.0 User Guidance Manual	Rev. 2.7.5
JCOP 8.0 User Guidance Manual Addendum	Rev. 2.6.1
JCOP 8.0 Anomaly Sheet	Rev. 2.6.4
JCOP 8.0 R1.38.0.1 (JCOP 8.0 19.5-1.38) User Guidance Manual for JCOP eSE	Rev. 2.7.8
JCOP 8.0 User Guidance Manual Addendum for JCOP eSE	Rev. 2.6.2
JCOP 8.0 User Guidance Manual Addendum System Management	Rev. 2.6.3
JCOP 8.0 UGM Addendum for Non-standard Optimized Byte Codes	Rev. 2.6.1
NXP Cap Optimizer User Manual	Rev. 1.0.1

For JCOP 8.1 R1.06.0.1, the following documentation is provided with the product by the developer to the customer:

Identifier	Version
JCOP 8.1 User Guidance Manual	Rev. 3.5.2
JCOP 8.1 User Guidance Manual Addendum	Rev. 3.5.0
JCOP 8.1 Anomaly Sheet	Rev. 3.5.2

JCOP 8.1 R1.06.0.1 (JCOP 8.1 20.5-1.06) User Guidance Manual for JCOP eSE	Rev. 3.5.2
JCOP 8.1 User Guidance Manual Addendum for JCOP eSE	Rev. 3.5.0
JCOP 8.1 User Guidance Manual Addendum System Management	Rev. 3.5.0
JCOP 8.1 UGM Addendum for Non-standard Optimized Byte Codes	Rev. 3.5.0
NXP Cap Optimizer User Manual	Rev. 1.0.1

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

The underlying hardware test results are extendable to composite evaluations, because 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 provided samples and a test environment. 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

Based on a list of potential vulnerabilities applicable to the TOE in its operational environment created during vulnerability analysis the evaluators devised the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could be exploited in the TOE's operational environment. While doing this, also the aspects of the security architecture were considered for penetration testing.

Source code reviews of the provided implementation representation accompanied the development of test cases and were used to find input for testing. The code inspection also supported the testing activities because they enabled the evaluator to verify implementation aspects that could hardly be covered by test cases.

The total test effort expended by the evaluators during this re-evaluation was 99 days. During that test campaign, 43% of the total time was spent on Perturbation attacks, 45% on side-channel testing, and 12% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

Penetration testing was also performed on derivative revisions of the TOE. The assurance gained from testing on these derivative revisions has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". 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).

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

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of multiple site certificates and 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 JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. 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 JCOP8.x on SE310 A0 Secure Element, versions JCOP 8.0 R1.38.0.1, JCOP 8.1 R1.06.0.1, to be **CC Part 2 extended, CC Part 3 conformant**, (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_FLR.1 and ALC_DVS.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP0099]*.

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 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: EdDSA signature generation (for JCOP 8.0 R1.38.0.1), MIFARE and FeliCa, which are out of scope as there are no security claims relating to these.
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).

3 Security Target

The NXP JCOP8.x on SE310 A0 Secure Element", Security Target, Revision 0.2.6, 7 May 2024 *[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:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CFB	Cipher Feedback
CTR	Counter
DES	Data Encryption Standard
CPLC	Card Production Life Cycle
CRT	Chinese Remainder Theorem
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DRG	Deterministic Random Generator
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDAA	Elliptic Curve Direct Anonymous Attestation
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
EDC	Error Detection Code
EdDSA	Elliptic Curve Edwards-curve Digital Signature Algorithm
eUICC	embedded Universal Integrated Circuit Card
GCM	Galois/Counter Mode
GF	Galois Field
GP	Global Platform
GCM	Galois/Counter Mode
GSMA	Groupe Speciale Mobile Association
IM4	Image4
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MNO	Mobile Network Operators
NFC	Near-Field Communication
NSCIB	Netherlands Scheme for Certification in the area of IT security

PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SMB	Secure Mailbox
TOE	Target of Evaluation

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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), NSCIB-2200042-02, version 4, 28 October 2024
[ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), NSCIB-2200042-02, version 4, 28 October 2024
[HW-CERT]	NXP SE310 Series – Secure Element version SE310_SE A0.1.000_J2, NSCIB-2200031-01-CR, version 2, 28 November 2023.
[HW-ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION, 2200031-01_ETR-COMP_230525_v3, 3.0, 25-May-2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	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 2.6, 02 August 2022
[PP0099]	Java Card System - Open Configuration Protection Profile, version 3.1, April 2020, registered under the reference BSI-CC-PP-0099-V2-2020
[ST]	NXP JCOP8.x on SE310 A0 Secure Element", Security Target, Revision 0.2.6, 7 May 2024
[ST-lite]	NXP JCOP8.x on SE310 A0 Secure Element", Security Target Lite, Revision 0.2.6, 9 August 2024.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)