EUCC Certification Report

NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1

Sponsor and Developer:	***NXP Semiconductors Netherlands N.V.*** **High Tech Campus 60** **5656AG Eindhoven** **The Netherlands**
Evaluation facility:	***Keysight Technologies Netherlands Riscure B.V.*** **Delftechpark 49,** **2628 XJ Delft,** **The Netherlands**
Report number:	**EUCC-3110-2026-2500172-01 Certification Report**
Report version:	**1.0**
Project number:	**EUCC-2500172-01**
Author(s):	**Jordi Mujal, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**23 October 2026**
Number of pages:	**21**
Number of appendices:	**0**

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

® TrustCB is a registered trademark. Any use or application requires prior approval by TrustCB.

CONTENTS

Foreword 3

International recognition of the certificate 4

1 Executive Summary 5

2 ICT Product details 6

2.1 Identification of the ICT Product 6
2.2 Contact information related to the evaluation of the ICT Product 6
2.3 Security services and policies 7
2.3.1 Security services 7
2.3.2 Vulnerability management 8
2.3.3 Assurance Continuity policies 9
2.3.4 Lifecycle management processes and production facilities 9
2.3.5 Patch management process 9
2.4 Assumptions and Clarification of Scope 9
2.4.1 Assumptions 9
2.4.2 Clarification of scope 9
2.5 Architectural Information 9
2.6 Supplementary Cybersecurity Information 10

3 Evaluation summary 12

3.1 Identification of used assurance components 12
3.2 EUCC State of the Art documents and Protection Profiles 12
3.3 ICT Product testing 12
3.3.1 Testing approach and depth 12
3.3.2 Independent penetration testing 12
3.3.3 Test configuration 12
3.3.4 Test results 12
3.4 ICT Product evaluation 13
3.4.1 Reused evaluation results 13
3.4.2 Evaluated configuration 13
3.4.3 Assessment against each assurance requirement 13
3.5 Results of the evaluation 15
3.6 Certificate information and scheme label 15
3.7 Comments and Recommendations 15

4 Security Target 17

5 Glossary 17

6 Bibliography 19

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated 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 security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

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

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is NXP Semiconductors Netherlands N.V. located in Eindhoven**,** The Netherlands and they also act as the sponsor of the evaluation and certification. This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The TOE is a platform containing the Java Card OS embedded on the NSN4XX2M0 B1 Secure Element with IC Dedicated Software. The TOE functionality of the product is defined by the requirements in the *[ST]* and it is mainly covering the JavaCard functionality as per *[PP]*. Further details on the TOE features are found in Section 2.3.

The TOE claims conformance to the following Protection Profiles *[PP]*:

- Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024, registered under the reference BSI-CC-PP-0099-V3-2024

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500172-01**, dated **23 October 2026** and with a 5-year validity.

The evaluation of the TOE was performed by Keysight Technologies Netherlands Riscure B.V. located in Delft, The Netherlands . The evaluation was completed on 16-10-2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) ALC_FLR.2 (Flaw Reporting Procedures), AVA_VAN.5 (Advanced methodical vulnerability analysis) and ASE_TSS.2 (TOE summary specification with architectural design summary). This assurance level is recognised by article 52 of *[CSA]* as ‘high’.

Consumers of this ICT Product 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.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

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 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1 from NXP Semiconductors Netherlands N.V. located in Eindhoven, The Netherlands.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NSN4XX2M0_SE	NSN4XX2M0_SE B1.1.000 J6 (for JCOP 10.0 R1.09.0.1) NSN4XX2M0_SE B1.1.000 T0 (for JCOP 10.0 R1.10.0.1)
Software	JCOP 10.0 eSE including Shared Code (with Crypto Library), NVM-OS, CommOS, SystemOS, and SMK.	1.09.0.1, 1.10.0.1
Byte Code Optimizer Tool	nxp-cap-optimizer	nxp-cap-optimizer- 1.0.2

Additional requirements for the operational environment of the certified ICT product are described in section 1.3.3 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate and Developer of the certified ICT Product

Organisation name:	NXP Semiconductors Netherlands N.V.
Address:	High Tech Campus 60, 5656AG Eindhoven, The Netherlands
Certified product contact	cybersecurity.certification@nxp.com
Website link for supplementary cybersecurity information associated with the TOE, in accordance with Article 55 of [EU-EUCC]	https://www.nxp.com/products/nxp-product-information/eucc-certified-products:EUCC-CERTIFIED

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V located in Hoofddorp, The Netherlands.

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

Keysight Technologies Netherlands Riscure B.V. located in Delft, The Netherlands

Responsible national cybersecurity certification authority

Dutch Authority for Digital Infrastructure (RDI)

2.3 Security services and policies

2.3.1 Security services

As per *[ST]* section 1.3, the TOE offers the following security features:

Secure Element Hardware:

- The security features of the certified underlying Secure Element Hardware are described in the [HW_CERT].

Cryptographic algorithms and functionality:

- AES
- Triple-DES (3DES)
- RSA for en-/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 signature generation and verification
- EdDSA key generation
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 algorithms
- HMAC algorithms
- ML-DSA (Module-Lattice-Based Digital Signature Standard) key generation, signature generation and verification
- ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism Standard) key generation, encapsulation, and decapsulation
- Multi-precision arithmetic operations including exact division, modular addition, modular subtraction, modular multiplication, modular inversion, arithmetic comparison and exact addition and subtraction
- Data Protection Module for a secure storage of the sensitive data
- Random number generation according to class DRG.3 or DRG.4 of *[AIS31]* and initialized (seeded) by the hardware random number generator of the TOE

Java Card 3.2 functionality:

- Executing Java Card bytecodes
- Managing memory allocation of code and data of applets
- Enforcing access rules between applets and the JCRE
- Mapping of Java method calls to native implementations of e.g., cryptographic operation
- Garbage Collection fully implemented with complete memory reclamation including compactification
- Support for Extended Length APDUs

- Support for Extended CAP file format
- Persistent Memory Management and Transaction Mechanism
- A call to not supported or deprecated methods will throw an exception of type ISO7816.SW_FUNC_NOT_SUPPORTED

GlobalPlatform 2.3.1 functionality:

- Loading of Java Card packages
- Instantiating applet instances
- Java package deletion
- Java applet instance deletion
- Creating Supplementary Security Domains
- Associating applets to Security Domains
- Installation of keys
- Verification of signatures of signed applets
- CVM Management (Global PIN) fully implemented
- Secure Channel Protocol is supported (SCP03, SCP04)
- Delegated Management, DAP
- Supported Amendments A, C, D, K, and J

NXP Proprietary Functionality

- Runtime Configuration Interface: Config Applet that can be used for configuration of the TOE
- OS update: Proprietary functionality that can update JCOP eSE, Shared code (including Crypto Lib), NVM- OS, SystemOS, CommOS, SMK. This component allows only NXP authorised and customer authorized updates to the product
- 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 reading logging information or resetting the Attack Counter
- Error Detection Code (EDC) API

Functionality in scope with general security claims

- NXP Proprietary Bytecode Compression – Applets installed Pre-Issuance by NXP and post-issuance may make use of proprietary optimised bytecodes.
- Firmware Measurement Mode (FWMM) is a NXP proprietary feature that supports the JCOP integrity check at host side

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1

Document reference: *[PSIRT]* PSIRT, Product Security Incident Response Process, NXPOMS-1719007347-4179, version 1.3, 14 March 2024

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

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

User Applet development is outside the scope of this evaluation. The life cycle allows pre-issuance and post-issuance loading of applets after TOE delivery as it is described in *[SotA_COSP]*.

2.3.5 Patch management process

Not applicable.

2.4 Assumptions and Clarification of Scope

2.4.1 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]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST].

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.

2.4.2 Clarification of scope

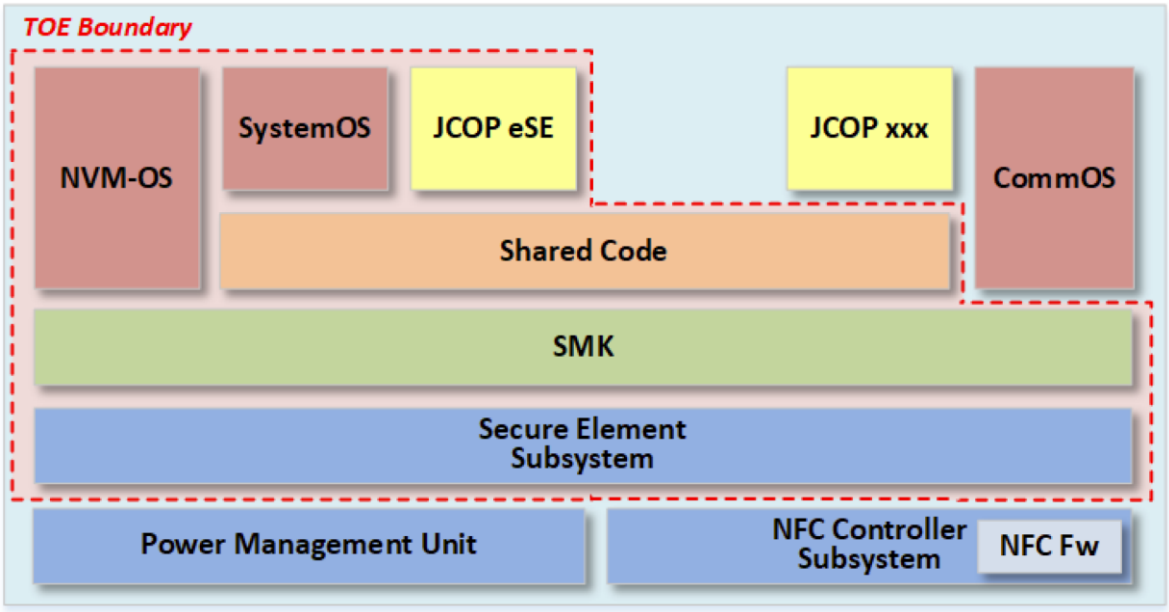
Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The circumstances and objectives related to the intended use of the product, are the ones related to the TOE type and its requirements defined in the *[ST],* and according to the claimed PP *[PP]* expected usage. It is important to remark that User Applets are outside the scope of this evaluation, but loading of applets is allowed as defined in *[SotA_COSP]*. Any application loaded post-issuance must adhere to the guidance restrictions in order to fulfil the Objectives for the Environment defined in the *[ST]*. On this aspect, the product guidance described in section 2.6, defines the security requirements for User Applets.

Threats addressed by the TOE and the IT environment are presented in Section 4.1.2 of *[ST]* and include the threats as presented in the *[PP]*, but also includes additional threats due to added functionality. The Organizational Security Polices (OSPs) are the same as in *[PP]* but also 2 additional OSPs were added. The *[ST]* contains all assumptions from the *[PP]* with the exception of one (as the card manager is part of the TOE), and six additional assumptions were added.

2.5 Architectural Information

The top-level block diagram of the TOE as it is depicted in the *[ST]*:



There are no known JavaCard applications loaded pre-issuance or post-issuance for this evaluation.

2.6 Supplementary Cybersecurity Information

The following website link was provided for the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.nxp.com/products/nxp-product-information/eucc-certified-products:EUCC-CERTIFIED

This link provides further details and links on:

- Guidance and recommendations to assist end users of the TOE with the secure configuration, installation, deployment, operation and maintenance of the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1.
- The period during which the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1 security support will be offered to end users of the TOE, in particular as regards the availability of cybersecurity related updates, is stated as 5 years, aligned with the validity of the issued EUCC certificate.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1.
- the online repository listing publicly disclosed vulnerabilities related to the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1 and to any relevant cybersecurity advisories.

The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0:

Identifier	Version
JCOP 10.0 User Guidance Manual	Rev. 1.9.3
JCOP 10.0 User Guidance Manual Addendum	Rev. 1.9.0
JCOP 10.0 Errata Sheet	Rev. 1.9.0
JCOP 10.0 R1.09.0.1 (JCOP 10.0 22.7-1.13) User Guidance Manual for	Rev. 1.9.4

JCOP eSE,	
JCOP 10.0 User Guidance Manual Addendum for JCOP eSE,	Rev. 1.9.0
JCOP 10.0 UGM Addendum for Non-standard Optimized Byte Codes,	Rev. 1.9.0
JCOP 10.0 User Guidance Manual Addendum System Management	Rev. 1.9.2
Cap Optimizer User Manual	Rev. 1.0.2
NSN4XX2M0 Integration manual	v1.3

The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.10.0.1.

Identifier	**Version**
JCOP 10.0 User Guidance Manual	Rev. 1.10.0
JCOP 10.0 User Guidance Manual Addendum	Rev. 1.10.0
JCOP 10.0 Errata Sheet	Rev. 1.10.0
JCOP 10.0 R1.10.0.1 (JCOP 10.0 22.7-1.14) User Guidance Manual for JCOP eSE	Rev. 1.10.1
JCOP 10.0 UGM Addendum for Non-standard Optimized Byte Codes	Rev. 1.10.0
JCOP 10.0 User Guidance Manual Addendum for JCOP eSE	Rev. 1.10.0
JCOP 10.0 User Guidance Manual Addendum System Management	Rev. 1.10.1
Cap Optimizer User Manual	Rev. 1.0.2
NSN4XX2M0 Integration manual	v1.3

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 5 augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5 and ASE_TSS.2**

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

The following Protection Profiles were applied:

Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024, registered under the reference BSI-CC-PP-0099-V3-2024

3.3 ICT 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.

3.3.1 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.

3.3.2 Independent penetration testing

The independent vulnerability analysis performed was conducted along the steps described in section 3.4.3, AVA part.

3.3.3 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 an earlier revision of the TOE. The assurance gained from testing on an earlier revision 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.

The ITSEF assessed the differences between these versions and concluded the test results obtained on the different versions are fully applicable to the version of the TOE stated in the *[ST]*

3.3.4 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 *[ACM]*.

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

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

3.4 ICT Product evaluation

The evaluation was performed referencing ISO/IEC 18045, Common Evaluation Methodology, and the EUCC State of the Art documents listed in section 6 of this report as *SotA* Documents.

No further security evaluation criteria (for example domain-specific technical guidelines, national interpretations) were applied in this evaluation.

3.4.1 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.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1.

The TOE of the evaluated product is an open and isolating platform according to [EUCC_OPEN]. The platform provides isolating mechanisms that follows the Java Card specification and was evaluated according to *[SotA-COSP]*.

3.4.3 Assessment against each assurance requirement

As it is presented in the *[ETR]*, here the summary for each class:

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE_REQ.2
TOE summary specification	ASE_TSS.2
Consistency of Composite product ST	ASE_COMP.1

In detail, the security target (ASE) highlights important aspects for understanding the precise evaluation and certification scope. The security target provides a good overview of the security services offered by the product and the intended usage.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.5

Implementation representation	ADV_IMP.1
Well-structured internals	ADV_INT.2
TOE design	ADV_TDS.4
Composite design compliance	ADV_COMP.1

The evaluation of the assurance class development (ADV), based on the ADV approach as defined in *[NI002]*, demonstrated a structured approach to the specifications, architecture and design of the product, which is reflected in the quality of the materials provided and the fact that there were no observations for requirements in the ADV assurance classes.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The evaluation of the user guidance (AGD) showed that the provided user guidance gives clear instructions on how to set up and use the TOE such that its security claims are maintained. Overall, the evaluator concludes that the requirements of the assurance class AGD are met by the TOE.

ALC

ALC	
CM capabilities	ALC_CMC.4
CM Scope	ALC_CMS.5
Delivery	ALC_DEL.1
Development security	ALC_DVS.2
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2
Tools and techniques	ALC_TAT.1
Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1

The evaluation of the life-cycle related aspects (ALC) successfully verified the TOE development and production lifecycle. The verification of proper application of the procedures involved spot-checks conducted by the evaluator, but also relied on the re-use of other evidence such as site certifications and site technical audit reports. The assessment of the ALC_DVS requirements completely relied on these existing evidences so that no site audits needed to be conducted. Overall, the evaluator concludes that the requirements of the assurance class ALC are met by the TOE.

ATE

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.3
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2
Composite functional testing	ATE_COMP.1

The evaluation of the developer test campaign (ATE) demonstrated that nearly all modules and TSFIs are covered by the developer testing campaign. The verification of the completeness of the testing effort consisted of independent tests by the evaluator and sampling of the developer test campaign. The

developer test campaign is found to be structured and complete. The independent evaluator tests demonstrated that the test campaign of the developer is complete and accurate. Overall, the evaluator concludes that all requirements of the assurance class ATE are met.

AVA

AVA	
Vulnerability analysis	AVA_VAN.5
Composite vulnerability assessment	AVA_COMP.1

The vulnerability analysis (AVA) and review of the implementation representation resulted in a number of penetration tests to be performed. These tests were aimed at perturbation, side channel analysis and logical attacks. Both the vulnerability analysis and penetration testing campaign confirmed to the evaluator that the TOE is resistant to attacks with a high attack potential *[SotA_AAPS]*. Overall, the product and all related evidence are very mature and consistent with only limited room for further improvements.

3.5 Results of the evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents and developer documentation *[DEV_DOCS]*.

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 evaluation results the evaluation lab concluded the NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element, version JCOP 10.0 R1.09.0.1 and JCOP 10.0 R1.10.0.1, to be **CC:2022 R1 1 Part 2 extended, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as '**High**', with **AVA_VAN 5** and to meet the requirements of **EAL 5 augmented with ALC_FLR.2, ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

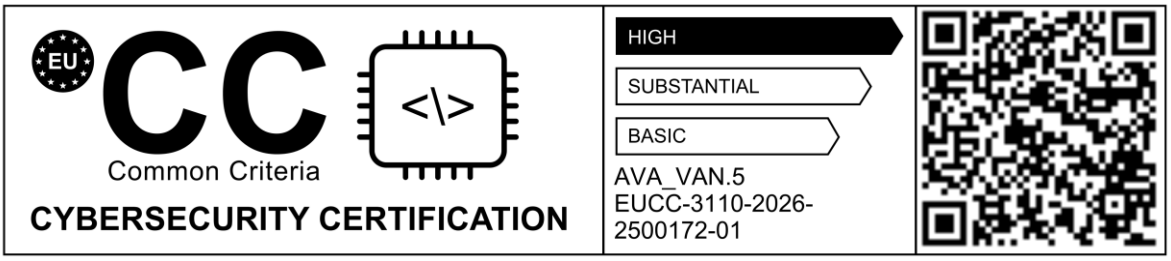
The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP]* with "Sensitive Result" augmentation package.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500172-01

Date of issuance: 23 October 2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 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).

4 Security Target

The certification references the following security target:

"NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element", Security Target, Revision 1.8, 14 October 2026 *[ST]*.

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

5 Glossary

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
APSD	Application Provider Security Domain
CAB	Conformity Assessment Body
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CFB	Cipher Feedback
CPLC	Card Production Life Cycle
CRT	Chinese Remainder Theorem
CSP	Cryptographic Service Provider
CTR	Counter
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
GCM	Galois/Counter Mode
GF	Galois Field
GP	Global Platform
GCM	Galois/Counter Mode
IM4	Image4
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NFC	Near-Field Communication
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm

SHA	Secure Hash Algorithm
SMB	Secure Mailbox
SPD	Security Problem Definition
SotA	State of the Art document for EUCC
TOE	Target of Evaluation

6 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[ACM]	EUCC Scheme Guidelines on cryptography Agreed Cryptographic Mechanisms, version 2.0, April 2025, published by ENISA.
[AIS31]	A Proposal for: Functionality Classes for Random Number Generators, version 3.0, 10 September 2024.
[CC]	Common Criteria for Information Technology Security Evaluation, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2

[DEV_DOCS]	NXP Semiconductors, CIList SN450 SE Star JCOP10.0 R1.09.0 split off at JCOP10.0 R1.09.0-RC1, rev.421538, 22 June 2026. NXP Semiconductors, CIList SN450 SE Star SN450 SE Star JCOP10.0 R1.10.0, rev.442265, 27 July 2026. NXP Semiconductors, CIList SN450 SE JCOP10.0 R1.10.0, rev.442480_Certification, 27 July 2026. CM Scope for the Evaluation of NXP JCOP, version 0.1, 05 April 2026 Cap Optimizer User Manual, Rev. 1.0.2, 28 August 2024 NSN4XX2M0 Integration manual , UM10955, version 1.3, 28 May 2026 For JCOP 10.0 R1.09.0.1: JCOP 10.0 User Guidance Manual, Rev. 1.9.3, 23 June 2026 JCOP 10.0 User Guidance Manual Addendum, Rev. 1.9.0, 11 March 2026 JCOP 10.0 Errata Sheet, Rev. 1.9.0, date 11 March 2026 JCOP 10.0 R1.09.0.1 (JCOP 10.0 22.7-1.13) User Guidance Manual for JCOP eSE, Rev. 1.9.4, 13 October 2026. JCOP 10.0 User Guidance Manual Addendum for JCOP eSE, Rev. 1.9.0, 11 March 2026 JCOP 10.0 UGM Addendum for Non-standard Optimized Byte Codes, Rev. 1.9.0, 11 March 2026 JCOP 10.0 User Guidance Manual Addendum System Management, Rev. 1.9.2, 13 October 2026. For JCOP 10.0 R1.10.0.1 JCOP 10.0 User Guidance Manual, Rev. 1.10.0, 30 September 2026 JCOP 10.0 User Guidance Manual Addendum, Rev. 1.10.0, 30 September 2026 JCOP 10.0 Errata Sheet, Rev. 1.10.0, 30 September 2026 JCOP 10.0 R1.10.0.1 (JCOP 10.0 22.7-1.14) User Guidance Manual for JCOP eSE, Rev. 1.10.1, 13 October 2026 JCOP 10.0 UGM Addendum for Non-standard Optimized Byte Codes, Rev. 1.10.0, 30 September 2026 JCOP 10.0 User Guidance Manual Addendum for JCOP eSE, Rev. 1.10.0, 30 September 2026 JCOP 10.0 User Guidance Manual Addendum System Management, Rev. 1.10.1, 13 October 2026
[ETR]	JCOP 10.x on NSN4XX2M0 B1 Secure Element - Evaluation Technical Report, version 1.1, 16 October 2026
[ETRfC]	JCOP 10.x on NSN4XX2M0 B1 Secure Element - ETR for Composite Evaluation, 1.1, 16 October 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[HW-CERT]	EUCC-3110-2026-2500173-01 Certification Report, version 1.0, 12 August 2026
	EUCC Assurance Continuity: Maintenance Report NXP NSN4XX2M0 Series - Secure Element, versions NSN4XX2M0_SE B1.1.000 J6, NSN4XX2M0_SE B1.1.000 T0, NSN4XX2M0_SE B2.1.000 T0, version 2.0, 18 September 2026
[HW-ETRfC]	ETR for Composite Evaluation for NSN4XX2M0 Series Secure Element, v1.4, 11 August 2026
[HW-ST]	"NXP NSN4XX2M0 Series - Secure Element", Security Target Lite, Revision 2.4, 7 September 2026.
[NI002]	NI002 - Content and presentation of evaluation review meetings, version 1.0, 08 July 2024
[PP]	Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024, registered under the reference BSI-CC-PP-0099-V3-2024
[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA_COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation and certification for CC: 2022 Version 1, February 2025
[SotA_CC_IC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Common Criteria to integrated circuits Version 2.0, December 2024
[SotA_COSP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT CERTIFICATION OF “OPEN” SMART CARD PRODUCTS VERSION 1.1, October 2023
[SotA_SARC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, version 1.1, October 2023
[SotA_STAR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT, STAR methodology, version 1, February 2025
[ST]	"NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element", Security Target, Revision 1.8, 14 October 2026
[ST-lite]	"NXP JCOP 10.x on NSN4XX2M0 B1 Secure Element", Security Target Lite, Revision 1.8, 14 October 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2
	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)