EUCC Certification Report

NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1

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

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

Report number: **EUCC-3110-2026-03-2500075-01 Certification Report**

Report version: **1**

Project number: **EUCC-2500075-01**

Author(s): **Jordi Mujal, TrustCB B.V.**
contact: eucc@trustcb.com

Date: **05 March 2026**

Number of pages: **21**

Number of appendices: **0**

CONTENTS

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.

Recognition of the Certificate

International recognition

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 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1.

The developer of the NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1 is NXP Semiconductors Netherlands 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 platform containing the Java Card OS embedded on the SN300 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 Secure IC requirements *[PP0084]* and JavaCard functionality as per *[PP0099]*. Further details on the TOE features are found in Section 2.2.

The TOE has been evaluated by SGS Brightsight located in Delft, The Netherlands. The evaluation was completed on 05 March 2026 with the issuance of the evaluation technical report *[ETR]* [1] . The certification procedure has been conducted 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.

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 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1, 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 JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1 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.

As per the *[ST]* conformance claim rationale, all the assumptions defined in the claimed *[PP0084]* and *[PP0099]* are taken with some exceptions. See section 2.4 for details.

The evaluation concluded that there are no special configuration requirements for the TOE besides the requirements defined in the user guidance. All users shall read these requirements and install the TOE in the operational environment accordingly.

The summary of the threats and security policies which *[ST]* defines:

- The Threats that are presented in Section 4 of *[ST]* include the threats as presented in the *[PP0084]* and *[PP0099]*, but also includes additional threats.
- The OSPs are the same as the ones defined in *[PP0084]* and *[PP0099]*, but four additional OSPs were added.

The results documented in the evaluation technical report *[ETR]* [2] 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’.

---

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

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

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).

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ICT product NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1 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	NXP SN300 Series – Secure Element	SN300_SE B1.1 J9
Software	JCOP 7.x OS including Shared Code (with Cryptolib), FlashOS, CommOS, SystemOS, and SMK.	JCOP 7.0 R1.62.0.1 JCOP 7.1 R1.04.0.1 JCOP 7.2 R1.09.0.1 JCOP 7.3 R1.07.0.1

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

The name and contact information provided for the holder of the issued Certificate associated with this Certification Report are as follows:

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/wireless-connectivity/nfc-hf/nfc-enabled-digital-wallet:NFC-ENABLED-DIGITAL-WALLET

2.2 Security Services

The following policies are referenced for this TOE:

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.
  - hardware to calculate Cyclic Redundancy Checks (CRC)
- 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 signature generation and verification
- EdDSA key generation
- 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 SMK, Crypto Lib, Flash Services Software or SystemOS. 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
  - Applet Migration: Keep User Data, Key Data or PIN Data after updating an applet.

2.3 Vulnerability handling and Assurance Continuity Policies

The following vulnerability policy has been identified as applicable to the NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1

Document reference:

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

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

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 Assumptions and Security Objectives that must be fulfilled by the TOE environment, see section 4 and 5.2 of the *[ST]*.

The user guidance as outlined in section 2.5 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.

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 *[PP0084]* and *[PP0099]* expected usage. It is important to remark that User Applets are outside the scope of this evaluation, but post-issuance 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 2.5, defines the security requirements for User Applets.

As per the *[ST]* conformance claim rationale, see section 2.3 for details, all the assumptions defined in the claimed PP *[PP0099]* and *[PP0084]* are taken with the following exceptions:

The SPD statement includes the assumptions from the *[PP0084]*. The SPD statement also includes two of the three assumptions from the *[PP0099]*. The assumption A.Deletion is excluded. The Card Manager is part of the TOE and therefore the assumption is no longer relevant.

Besides the assumptions from the *[PP0099]*, the following assumptions are added:

- A.PROCESS-SEC-IC
- A.USE_DIAG
- A.USE_KEYS
- A.APPS-PROVIDER
- A.VERIFICATION-AUTHORITY
- A.TRUSTED-GUESTOS

The assumption A.PROCESS-SEC-IC is taken from the underlying Security IC Platform PP.

The assumptions A.USE_DIAG and A.USE_KEYS are included because the Card Manager is part of the TOE and no longer part of the environment.

The assumptions A.APPS-PROVIDER and A.VERIFICATION-AUTHORITY are added because Security Domains from the GlobalPlatform Specification are introduced. All the applets and packages are signed by the APSD and the correctness is verified on the TOE by VASD before the package or applet is installed or loaded. A.APPSPROVIDER and A.VERIFICATION-AUTHORITY are additions to PP for card content management environment.

The assumptions A.TRUSTED-GUESTOS is included because the Guest Operating Systems that are hosted in external contexts are provided by a trusted actor.

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

- HW NFC Controller Subsystem and Power Management Unit
- JCOP 7.x with eUICC extension and any other secondary JCOP (optional)
- CommOS

There is no security claim on the ECDAA signature generation, Galois Message Authentication code (GMAC) for symmetric-key crypto, SHA-3, Korean SEED, MIFARE and FeliCa APIs provided by JCOP 7.x.

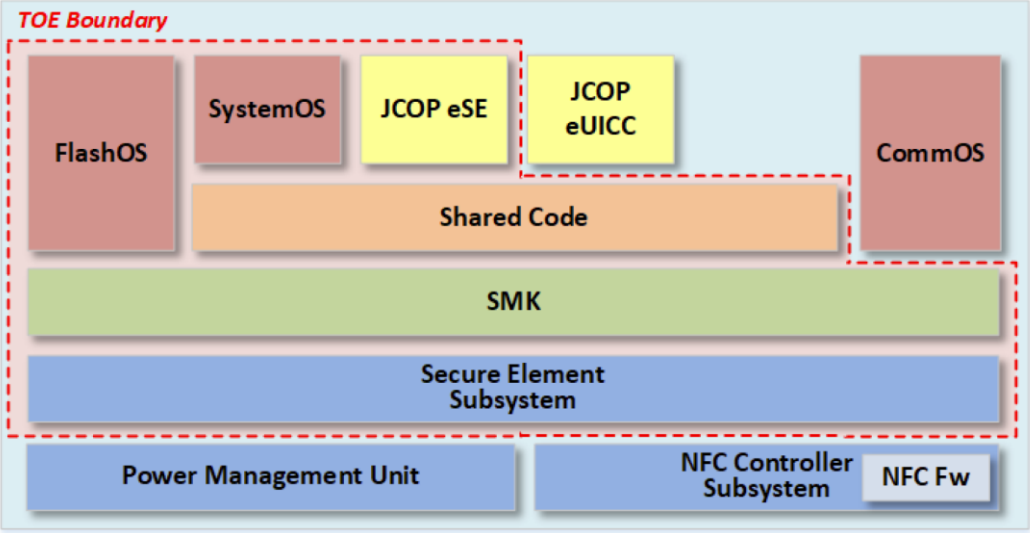
The following functionality is also present without specific security claims:

- 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

2.5 Architectural Information

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



TOE identification provided in the ST identifies the JCOP eSE OS functionalities and including Shared Code (with Cryptolib), FlashOS, SystemOS, and SMK. There are no known JavaCard applications loaded pre-issuance or post-issuance for this evaluation.

2.6 Supplementary Cybersecurity Information

The contact information of the NXP Semiconductors Netherlands N.V. and accepted methods for receiving vulnerability information from end users and security researchers for the NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1 is as provided in section 2.1.

The stated period during which security support will be offered to end users for the NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1, in particular as regards the availability of cybersecurity related updates, is 5 years:

Further information, including guidance and online repositories listing publicly disclosed vulnerabilities related to the NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1 and to any relevant cybersecurity advisories are detailed from this link:

https://www.nxp.com/products/wireless-connectivity/nfc-hf/nfc-enabled-digital-wallet:NFC-ENABLED-DIGITAL-WALLET

The following documentation is provided with the product by the developer to the customer for the JCOP 7.0 R1.62.0.1:

Identifier	Revision
NXP. JCOP 7.0 User Guidance Manual	1.24.7
NXP. JCOP 7.0 User Guidance Manual Addendum	1.24.1
NXP. JCOP 7.0 Anomaly Sheet	1.24.1
NXP. JCOP 7.0 R1.62.0.1 (JCOP 7.0 17.4-1.62) User Guidance Manual for JCOP eSE	1.20.7

Identifier	Revision
NXP. JCOP 7.0 User Guidance Manual Addendum for JCOP eSE	1.24.1
NXP JCOP 7.0 UGM Addendum System Management	1.24.2
ES_JCOP7.x Documentation Errata	1.3
SN300 family; SN300V, SN300R and SN300W Single Chip Secured (NFC) controller, Objective data sheet	3.1

The following documentation is provided with the product by the developer to the customer for the JCOP 7.1 R1.04.0.1:

Identifier	Revision
NXP. JCOP 7.1 User Guidance Manual	3.05.4
NXP. JCOP 7.1 User Guidance Manual Addendum	3.04.1
NXP. JCOP 7.1 Anomaly Sheet	3.04.1
NXP. JCOP 7.1 19.4-1.04 User Guidance Manual for JCOP eSE	3.06.4
NXP. JCOP 7.1 User Guidance Manual Addendum for JCOP eSE	3.05.1
NXP JCOP 7.1 UGM Addendum System Management	3.04.2
ES_JCOP7.x Documentation Errata	1.3
SN300 family; SN300V, SN300R and SN300W Single Chip Secured (NFC) controller, Objective data sheet	3.1

The following documentation is provided with the product by the developer to the customer for the JCOP 7.2 R1.09.0.1:

Identifier	Revision
NXP. JCOP 7.2 User Guidance Manual	4.05.3
NXP. JCOP 7.2 User Guidance Manual Addendum	4.05.0
NXP. JCOP 7.2 Anomaly Sheet	4.05.0
NXP. JCOP 7.2 JCOP 7.2 20.4-1.06 User Guidance Manual for JCOP eSE,	4.05.3
NXP. JCOP 7.2 User Guidance Manual Addendum for JCOP eSE	4.05.0
NXP JCOP 7.2 UGM Addendum System Management	4.05.0
ES_JCOP7.x Documentation Errata	1.3
SN300 family; SN300V, SN300R and SN300W Single Chip Secured (NFC) controller, Objective data sheet	3.1

The following documentation is provided with the product by the developer to the customer for the JCOP 7.3 R1.07.0.1:

Identifier	Revision

Identifier	Revision
NXP. JCOP 7.3 User Guidance Manual	5.6.2
NXP. JCOP 7.3 User Guidance Manual Addendum	5.6.0
NXP. JCOP 7.3 Anomaly Sheet	5.6.1
NXP. JCOP 7.3 JCOP 7.3 21.4-1.07 User Guidance Manual for JCOP eSE	5.6.2
NXP. JCOP 7.3 User Guidance Manual Addendum for JCOP eSE	5.6.0
NXP JCOP 7.3 UGM Addendum System Management	5.6.0
ES_JCOP7.x Documentation Errata	1.3
SN300 family; SN300V, SN300R and SN300W Single Chip Secured (NFC) controller, Objective data sheet	3.1

2.7 Lifecycle Management processes and production facilities

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 5.2.

User Applet development is outside the scope of this evaluation. Applet loading into Flash memory can be done in phases 3, 4, 5, and 6. Applet loading in phase 7 is also allowed. This means post-issuance loading of applets is allowed,

2.8 ICT Product Testing

2.8.1 Identification of CAB and ITSEF

TrustCB is the Certification Assessment Body, licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities.

TrustCB point of contact: EUCC@trustcb.com

Testing was performed by following ITSEF: SGS Brightsight B.V.

2.8.2 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, ASE_TSS.2**

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

2.8.3 EUCC State of the Art documents and Protect Profiles

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

The following Protection Profile was applied:

Java Card System – Open Configuration Protection Profile, as certified under the reference BSI-CC-PP-0099-V3-2024 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI) following evaluation by ITSEF TÜV Informationstechnik GmbH. The author of this Protection Profile is Oracle Corporation. The assurance package required for a product conforming to this protection profile is EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2.

Contact details for CB of PP: Zertifizierung@bsi.bund.de

Contact details of ITSEF for PP: M.LeGuin@tuvit.de

Security IC Platform Protection Profile with Augmentation Packages, as certified under the reference BSI-CC-PP-0084-2014 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI) following evaluation by ITSEF Brightsight. The author of this Protection Profile is Inside Secure, Infineon

Technologies AG, NXP Semiconductors Germany GmbH and STMicroelectronics. The assurance package required for a product conforming to this protection profile is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

Contact details for CB of PP: Zertifizierung@bsi.bund.de

Contact details of ITSEF for PP: brs.sales@sgs.com

2.8.4 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and SFR-enforcing module level. The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

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.

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.

2.8.5 Independent penetration testing

The independent vulnerability analysis performed was conducted along the steps described in section 2.9.1, AVA part.

2.8.6 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.
Some of the independent and penetration testing was performed on a different version of the software and underlying platform (JCOP 7.0 R1.54.0.2, JCOP 7.0 R2.01.0.1, JCOP 7.0 R1.66.0.1) or on JCOP 7.x eUICC OS instance (JCOP 7.0 R1.54.0.2). The ITSEF assessed the differences between these versions and concluded that do not negatively impact security, the test results obtained on the different versions are fully applicable to the TOE versions in the *[ST]*.

2.8.7 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.

2.8.8 Reused Evaluation Results

This was a new certification under EUCC however documentary evaluation results of an earlier version of the TOE certified under the SOG-IS Netherlands Scheme for Certification in the area of IT

security (NSCIB) have been partially reused. Vulnerability analysis and penetration testing has been renewed.

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.

2.8.9 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1.

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]*.

2.9 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**".

2.9.1 Assessment against each assurance requirement

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

The TOE introduction, conformance claim, security problems, security objectives, extended components, security requirements and TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2. No issues or deviations were identified.

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

The evaluation has demonstrated that the developer's evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. The subsystem/module level model is sensible, useful, and shows TSFIs and subsystem/module decomposition. The security architecture is thoroughly explained, design compliance rationale is complete and coherent, and necessary evidence is extracted per alternative approach. The evaluator confirmed why the TSF is well-structured. SFRs were inspected, with findings mapped to the implementation representation in both evaluation meetings. Accordingly, the ADV activities meet the assurance requirements for EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2, with no issues or deviations identified.

AGD

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

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements for EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2, with no issues or deviations identified.

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.2

The evaluation has demonstrated that the developer's evidence meets ALC specified. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in accordance with the CM plan to maintain all configuration items by automated means. Delivery procedures were well-documented, ensuring security during TOE distribution. Security measures for protecting the confidentiality and integrity of the TOE in physical, procedural, personnel, logical and other areas were justified as sufficient. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. The development life-cycle model provided necessary control; tools were well-defined with clear documentation and implementation standards have been applied by the developer. Accordingly, the ALC activities satisfy the assurance requirements for EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2, with no issues or deviations identified.

ATE

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.3

Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2

The evaluation has demonstrated that the developer's evidence for ATE requirements meets all specified requirements. The testing approach used by the developer effectively covered the TSFIs and modules. The developer's rationale for testing all TSFIs and modules was presented and verified. The developer test results show that for all tests either the result was pass or a proper rationale was given why the test failed. For the evaluator's independent testing, the overall approach for test selection, goals for the witnessing session, and independent test plan were clearly outlined. The evaluator's testing results showed that all sampled tests were passed. Accordingly, the ATE activities satisfy the assurance requirements for EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2, with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.5

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis it was performed according to the *[SotA_AAPS]*.
- The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE under consideration of the components identified in the list of third-party components, and specific IT products in the environment that the TOE depends on, e.g., bytecode verifier. No potential vulnerabilities were identified.
- All potential vulnerabilities are 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. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

Consequently, the AVA activities were performed in full compliance with the assurance requirements EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2, providing a high level of confidence in the TOE's resistance to exploitation.

2.9.2 Overall result of evaluation

Based on the above evaluation results the evaluation lab concluded the NXP JCOP 7.x on SN300 Secure Element, versions JCOP 7.0 R1.62.0.1, JCOP 7.1 R1.04.0.1, JCOP 7.2 R1.09.0.1, JCOP 7.3 R1.07.0.1, to be **CC:2022 revision 1 Part 2 extended, CC:2022 revision 1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as 'high', and to meet the assurance 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]*.

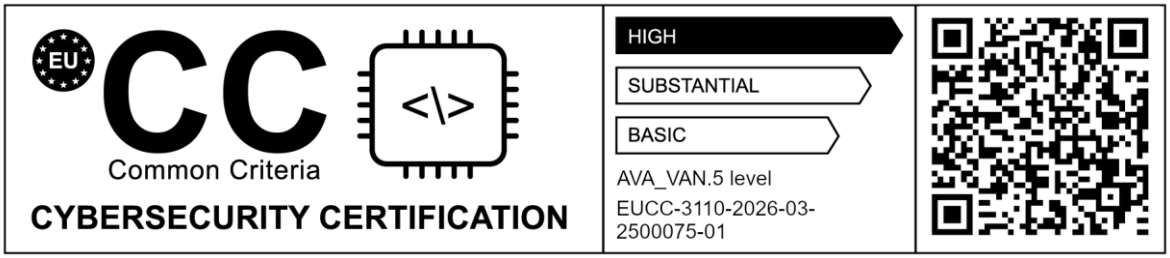
The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP0099]* and strict compliance to *[PP0084]*.

2.10 Certificate information and scheme label

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

Unique identifier: EUCC-3110-2026-03-2500075-01

Date of issuance: 05-03-2026 and with a validity period of **5 years**.



2.11 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: 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).

3 Security Target

The "NXP JCOP 7.x on SN300 Secure Element", Security Target, Revision 3.1, 24 November 2025 *[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]*.

This *[ST]* is summarised in the *[ETR]* as follows:

The TOE is the Java Card eSE OS embedded on the SN300 Secure Element with IC Dedicated Software. It excludes the NFC Controller, the Power Management Unit and Java Card eUICC OS. The security functionality of the evaluated ICT product is represented by the implementation of the selected components of *[CC]* Part2 with extended components defined in *[PP0084]* and are listed in section 7 Security Functional Requirements (ASE_REQ) of the *[ST]*. Regarding the secure element, the Security Functional Requirements Statement copies the SFRs from the Security IC Platform Protection Profile *[PP0084]*. Where applicable, security functional components are replaced with their counterparts from *[CC]* Part2 to ensure conformity with CC:2022. Further, additional SFRs have been included. Please refer to *[ST]* Section 2.3.2.3 for a summary of all sets.

Regarding the JCOP 7.x Java Card OS, the Security Functional Requirements Statement copies most SFRs as defined in the Java Card Protection Profile - Open Configuration *[PP0099]*, with the exception of a number of options. For the copied set of SFRs the ST is considered equivalent to the statement of SFRs in the PP. Moreover, as requested by the PP, the ST adds additional threats, objectives and SFRs to fully cover and describe additional security functionality implemented in the TOE.

4 Definitions

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
eUICC	embedded Universal Integrated Circuit Card
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

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, CC:2022 Parts 1, 2, 3, 4 and 4, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[DEV_DOCS]	For developer documentation used in the evaluation effort, see [ETRfc] and [ETR]
[ETR]	Evaluation Technical Report “NXP JCOP7.x on SN300 B1.1 J9 Secure Element (versions: JCOP 7.0 R1.62.0.1 - JCOP 7.1 R1.04.0.1 - JCOP 7.2 R1.09.0.1 - JCOP 7.3 R1.07.0.1)” – EAL5+, 25-RPT-848, version 5.0, 05 March 2026
[ETRfC]	Evaluation Technical Report for Composition “NXP JCOP7.x on SN300 B1.1 Secure Element (versions: JCOP 7.0 R1.62.0.1 - JCOP 7.1 R1.04.0.1 - JCOP 7.2 R1.09.0.1 - JCOP 7.3 R1.07.0.1)” – EAL5 augmented with ASE_TSS.2, AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2, 25-RPT-849, version 3.0, 25 February 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
[PP0099]	Java Card System – Open Configuration Protection Profile, Version 3.2, July 2024, registered under the reference BSI-CC-PP-0099-V3-2024
[PP0084]	Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 January 2014, registered under the reference BSI-CC-PP-0084-2014
[PSIRT]	PSIRT, Product Security Incident Response Process, NXPOMS-1719007347-4179, version 1.3, 14 March 2024
[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potentical to Smarcards and Similar Devices, Version 2, February 2025
[SotA_COSP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT CERTIFICATION OF “OPEN” SMART CARD PRODUCTS VERSION 1.1, October 2023
[SotA_MSSR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Minimum Site Security Requirements, Version 2, February 2025
[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 7.x on SN300 Secure Element", Security Target, Revision 3.1, 24 November 2025
[ST-lite]	"NXP JCOP 7.x on SN300 Secure Element", Security Target Lite, Revision 3.1, 24 November 2025.
[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.)