EUCC Certification Report

NXP JCOP 8.9 on SN300 Secure Element, versions:
JCOP-eSE 8.9 R1.06.00.1.1 (JCOP-eUICC 8.9 R1),
JCOP-eSE 8.9 R1.06.01.1.1 (JCOP-eUICC 8.9 R1-01)
JCOP-eSE 8.9 R6.02.00.1.1 (JCOP-eSE 8.9 R6-02)

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Beiersdorfstrasse 12,** **22529 Hamburg,** **Germany**
Evaluation facility:	***TÜV Informationstechnik GmbH*** ***Am TÜV 1*** ***45307 Essen*** ***Germany***
Report number:	**EUCC-3110-2026-2500078-01 Certification Report**
Report version:	**1**
Project number:	**EUCC-2500078-01**
Author(s):	**Haico Haak, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**15 May 2026**
Number of pages:	**19**
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.

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 8.9 on SN300 Secure Element, 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 Germany GmbH located in Hamburg, Germany 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 composite platform containing the Java Card OS embedded on the SN300 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 claims conformance to the following Protection Profiles *[PP0099],[PP0104]*:

- Java Card System - Open Configuration Protection Profile, version 3.2, July 2024 registered under the reference BSI-CC-PP-0099-V3-2024
- Protection Profile “Cryptographic Service Provider (CSP)”, version 0.9.8, 19.02.2019, registered the reference BSI-CC-PP-0104-2019

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-3110-2026-2500078-01**, dated 15-05-2026 and with a 5-year validity.

The evaluation of the TOE was performed by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 06 May 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 (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis), ALC_DVS.2 (Sufficiency of security measures), ALC_FLR.2 (Flaw Reporting Procedures) and ASE_TSS.2 (TOE summary specification with architectural design summary). It also includes the assurance Composite product package as defined in *[CC]*(Part 5).

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 8.9 on SN300 Secure Element, from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP SN300 Secure Element	SN300_SE B5.1
Software	JCOP-SE 8.9 integrating JCOP-eSE 8.9 Including the Platform Core software (SMK, Shared code subsystem, System OS and Communications OS and any other Guest OS as well as preloaded Applet packages)	R1.06.00.1.1 R1.06.01.1.1 R6.02.00.1.1

Additional requirements for the operational environment of the certified ICT product are described in section 5.2 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

Organisation name:	NXP Semiconductors Germany GmbH
Address:	Beiersdorfstrasse 12, 22529 Hamburg, GERMANY
Certified product contact details	cybersecurity.certification@nxp.com

Developer of the certified ICT Product

ICT product developer	NXP Semiconductors Germany GmbH

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V. TrustCB is licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC certification activities up to and including EUCC High.

TrustCB point of contact: EUCC@trustcb.com

Identification of ITSEF

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

TÜV Informationstechnik GmbH located in Essen, Germany

2.3 Security services and policies

2.3.1 Security services

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 calculate Cyclic Redundancy Checks (CRC)
    - hardware to serve with True Random Numbers
- Cryptographic algorithms and functionality
    - AES
    - Triple-DES (3DES)
    - RSA Functions
    - ECDSA Functions
    - ECDH Functions
    - ECC Functions
    - 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 Functions
    - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms
    - HMAC algorithms
    - 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 the sensitive data.
    - Random number generation according to class DRG.3 or DRG.4 of AIS20 [5] and initialized (seeded) by the hardware random number generator of the TOE.
- Java Card 3.1 functionality
- GlobalPlatform 2.3.1 functionality
- Additional standard functionality
    - Cryptographic Service Provider feature
- NXP proprietary functionality
    - Runtime Configuration Interface: Config Applet that can be used for configuration of theTOE.
    - 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.
    - Error Detection Code (EDC) API

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the NXP JCOP 8.9 on SN300 Secure Element,

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 1.4.2.

2.3.5 Patch management process

Not applicable to this evaluation

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.

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 *[PP0099]*, but also includes additional threats. The assumed level of expertise of the attacker for all identified threats is High

The Organizational Security Polices (OSPs) are the same as in *[PP0099],* and 3 additional OSPs were added.

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

• NFC Controller Subsystem

• Power Management Unit

• JCOP eUICC

• JCOP xxx (optional)

• CommOS

• Non-Interfering Shared Code

• Non-Certified Crypto

The following functionality is also present without specific security claims:

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

• Programmable Timeout for SMB with Limitations in UGM [47] Section 6

• CPLC data made available through SystemInfo, see UGM [47] Section 1.3.3.

• NXP Proprietary Bytecode Compression – Applets installed Pre-Issuance by NXP may make use of proprietary optimised bytecodes, which group common sequences of standard bytcodes to provide exactly the same operations, whilst saving Applet code space.

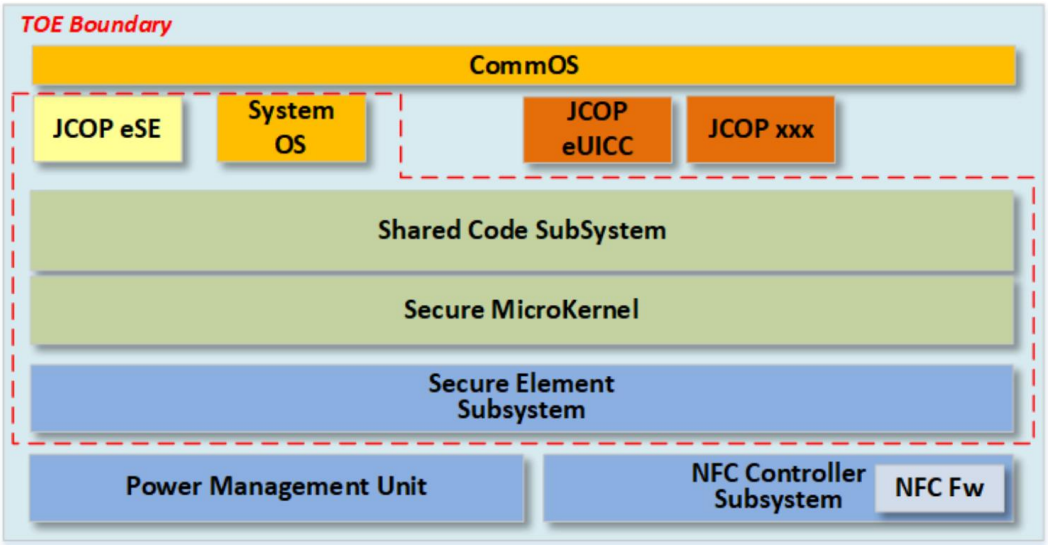
• Compliance to Secure Element configuration, Common Implementation Configuration, UICC Configuration, and UICC Configuration Contactless Extension.

• MIFARE is subject of separate MIFARE certification scheme

• Felica Lib is subject of separate Felica certification scheme

2.5 Architectural Information

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



2.6 Supplementary Cybersecurity Information

The following website link was provided for the NXP JCOP 8.9 on SN300 Secure Element, 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

This link provides further details and links on:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the NXP JCOP 8.9 on SN300 Secure Element,.
- The period during which the NXP JCOP 8.9 on SN300 Secure Element, security support will be offered to end users, 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 8.9 on SN300 Secure Element,.
- the online repository listing publicly disclosed vulnerabilities related to the NXP JCOP 8.9 on SN300 Secure Element, and to any relevant cybersecurity advisories .

Note: 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 8.9 on SN300 Secure Element,:

Guidance and recommendations specific to JCOP eSE R1	
Identifier	**Version**
JCOP8.9 User Guidance manual (UGM)	Rev 1.7.0
JCOP 8.9 R1 System Identification Manual	Rev 1.1.0
JCOP-eSE 8.9 R1 – User Guidance Manual for JCOP eSE	Rev 1.7.0
JCOP-eSE 8.9 R1 – User Guidance Manual Addendum for JCOP eSE	Rev 1.7.0
JCOP 8.9 R1 UGM Addendum for System Management	Rev 1.7.0
JCOP 8.9 R1 User Manual Addendum for CSP	Rev 1.7.0
JCOP 8.9 R1 User Manual Addendum - Amd I SEMS Application	Rev 1.7.0

JCOP 8.9 R1 Anomaly Sheet	Rev 1.7.0

Guidance and recommendations specific to JCOP eSE R6	
Identifier	**Version**
JCOP8.9 R6.02 (SN300) I3C User Guidance Manual (UGM)	Rev. 1.0.1
JCOP-eSE 8.9 R6.02 (SN300) I3C User Guidance Manual for JCOP eSE	Rev. 1.0.1
JCOP-eSE 8.9 R6.02 (SN300) I3C User Guidance Manual Addendum for JCOP eSE	Rev. 1.0.0
JCOP8.9 R6.02 (SN300) I3C User Guidance Manual Addendum for System Management	Rev. 1.0.0
JCOP8.9 R6.02 (SN300) I3C CSP User Manual Addendum	Rev. 1.0.0
JCOP8.9 R6.02 (SN300) I3C Amd I SEMS Application User Manual Addendum	Rev. 1.0.0
JCOP8.9 R6.02 (SN300) I3C Errata Sheet	Rev. 1.0.0

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2** and
- **Composition evaluation package (COMP)**,

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

Protection Profile “Cryptographic Service Provider (CSP)”, version 0.9.8, 19.02.2019, registered the reference BSI-CC-PP-0104-2019

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 and crypto-library 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

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 was 10,5 weeks. During that test campaign 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 20% perturbation attacks, 30% retrieving keys with FA, 40% side-channel attacks, 0% exploitation of test features, 0% attacks on RNG, 10% software attacks, and 0% application isolation penetration tests

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 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.

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.

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.

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

This is a new certification under EUCC.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number NXP JCOP 8.9 on SN300 Secure Element, versions**:**
JCOP-eSE 8.9 R1.06.00.1.1 (JCOP-eSE 8.9 R1)
JCOP-eSE 8.9 R1.06.01.1.1 (JCOP-eSE 8.9 R1-01)
JCOP-eSE 8.9 R6.02.00.1.1 (JCOP-eSE 8.9 R6-02).

3.4.3 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
Consistency of Composite product ST	ASE.COMP.1

The *[ST]* contains all relevant information for this class and the according families ac-cording to EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and the COMP package.

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

Developer Evidence, i.e. implementation representation was provided that enabled the evaluator to ensure that all relevant aspects for this class and the according families according to EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and the COMP package are met by the TOE.

AGD

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

The guidance documentation for the TOE, as outlined in the *[ST]* is provided that contains all relevant information for this class and the according families according to EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and the COMP package

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
Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1

The TOE Life Cycle is covered by audited sites and Developer Documentation has been provided that contains all relevant information for this class and the according families according to EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and the COMP package.

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 developer provided Test documentation, a test witnessing session was performed and independent testing was performed. The provided information enabled the evaluator to positively assess that the TOE

meets this class and the according families according to EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and the COMP package.

AVA

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

A vulnerability analysis was performed and penetration tests based on the analysis were conducted. No deviation from the expected result was detected. Therefore, the TOE meets this class and the according families according to EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and the COMP package.

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 8.9 on SN300 Secure Element, 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 AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

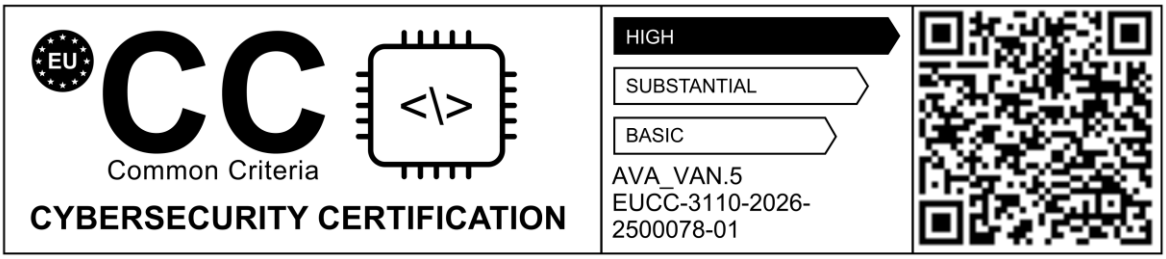
The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP0099]* and claims 'strict' conformance to the Protection Profile *[PP0104]*.

3.6 Certificate information and scheme label

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

Unique identifier: EUCC-3110-2026-2500078-01

Date of issuance: 15-05-2026 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: 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).

4 Security Target

The certification references the following security target:

NXP JCOP 8.9 on SN300 Secure Element Security Target, Rev. 2.6 — 1 May 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
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
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EdDSA	Elliptic Curve Edwards-curve Digital Signature Algorithm
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
eUICC	embedded Universal Integrated Circuit Card
GCM	Galois/Counter Mode
GF	Galois Field
GP	Global Platform
GSMA	Groupe Speciale Mobile Association
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
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation

6 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 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2025-001]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 2025-10-15, CCMB-2025-001
[DEV_DOCS]	For developer documentation used in the evaluation effort, see [ETRfc] and [ETR]
[ETR]	EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), Version 4, Project / Certification ID: 8123731517 / EUCC-2500078-01, 2026-05-06
[ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), Version 4, Project / Certification ID: 8123731517 / EUCC-2500078-01, 2026-05-06
[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]	Certification Report NXP SN300 B5 Series - Secure Element version SN300_SE B5.1.002 JD, NSCIB-CC-2300083-02-CR, Version 1, 10 February 2025
[HW-ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), Version 2, 10 February 2025
[HW-ST]	NXP SN300 B5 Series - Secure Element Security Target version 0.5, 22 August 2023
[PP0099]	Java Card System - Open Configuration Protection Profile, version 3.2, July 2024 registered under the reference BSI-CC-PP-0099-V3-2024
[PP0104]	Protection Profile “Cryptographic Service Provider (CSP)”, version 0.9.8, 19.02.2019, registered the reference BSI-CC-PP-0104-2019
[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 Potential to Smartcards and Similar Devices, Version 2, 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_COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation and certification for CC: 2022 Version 1, 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
[SotA_CRYPTO]	EUCC SCHEME, GUIDELINES ON CRYPTOGRAPHY, Agreed Cryptographic Mechanisms, Version 2, May 2025
[ST]	NXP JCOP 8.9 on SN300 Secure Element Security Target, Rev. 2.6 — 1 May 2026
[ST-lite]	NXP JCOP 8.9 on SN300 Secure Element Security Target Lite, Rev. 2.2 — 1 May 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.)