Brightsight B.V.

Brassersplein 2
2612 CT Delft
The Netherlands

t (+31) 15 269 2500
brs.info@sgs.com

www.brightsightcb.com

coc 30105045

EUCC-3100-2026-0002

Certification Report

NXP JCOP 7.x on SN300 Secure Element

26-CB-092

Version and Approval

Version	Date	Author	Version information	Reviewed
1.0	2026-10-09	Miquel Hernandez	First release	Jason Chen Thomas Ribbrock
2.0	2026-10-20	Miquel Hernandez	Addressing feedback on CSC-387	

Approved by:	Rob Kemper

brightsight

By SGS

Table Of Contents

Contents

1 Executive Summary 4
1.1 Required information: 4
1.1.1 Assurance continuity and certificate review 4
1.2 Brief description of the certification report results 4
1.3 International recognition of the certificate 5
1.4 Disclaimer(s) 6

2 Identification of the ICT product 7
2.1 Unique identification 7
2.2 Product components 7
2.3 Additional requirements for the operating environment of the ICT product 10

3 Contact information related to the evaluation of the ICT product 13

4 Security Policies 14
4.1 Security services 14
4.2 Vulnerability handling policy 15
4.2.1 Reference 15
4.2.2 Description 15
4.3 Assurance continuity policy 15
4.4 Patch management procedure 15

5 Assumptions and clarification of scope 16
5.1 Assumptions on the ICT's product usage and deployment 16
5.2 Assumptions for the environment for compliant operation 16
5.3 Threats to the ICT product not countered by its security functions 18

6 Architectural information 19

7 Supplementary cybersecurity information 22

8 ICT product evaluation summary and evaluated configuration 23
8.1 Required information 23
8.2 Product settings and configuration 23

9 Results of the evaluation and information regarding the certificate 25
9.1 Required information 25
9.2 Assurance requirements 25
9.3 Testing approach and results 25
9.3.1 Testing approach and depth 25
9.3.2 Penetration testing 25

9.3.3 Test results 25

10 Security target 26

11 Mark or label associated to the scheme 27

12 Glossary 28

13 Bibliography 29
13.1.1 Evaluation criteria 29
13.1.2 Evaluation technical report 29
13.1.3 Technical reference documentation 30
13.1.4 Developer documentation 30
13.1.5 ITSEF documentation 31

A Mapping of evaluator actions and verdicts 34
A.1 ASE 34
A.2 ADV 36
A.3 AGD 37
A.4 ALC 38
A.5 ATE 39
A.6 AVA 40

brightsight

By SGS

1 Executive Summary

1.1 Required information:

Name of the evaluated ICT product	NXP JCOP 7.x on SN300
Name of the ITSEF which performed the evaluation	SGS Brightsight B.V. (referred to as Brightsight ITSEF)
Completion date of evaluation	2026-09-29
Date of issuance of the certificate	2026-10-20
Date of issuance of the initial certificate	N/A
Validity period	5 years
Certificate ID	EUCC-3100-2026-0002
Website ID	EUCC-3100-2026-000002-I-00
CC Version	ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation (CC), CC:2022 Revision 1
CC assurance package and security assurance components	EAL5, augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2
Assurance level as per Regulation (EU) 2019/881	High, at AVA_VAN.5
Protection Profile(s)	BSI-CC-PP-0084-V2-2026 BSI-CC-PP-0099-V3-2024
Security Policy of the evaluated ICT product	Refer to chapter 4 of this report

1.1.1 Assurance continuity and certificate review

Not Applicable.

1.2 Brief description of the certification report results

This Certification Report presents the results of the Common Criteria security evaluation of NXP NXP JCOP 7.x on SN300. The TOE was developed by NXP Semiconductors B.V., who also sponsored the evaluation and certification.

The purpose is also to inform potential buyers about the conditions required for the product's proper use, so they can ensure it complies with the requirements under which it was evaluated and certified. Therefore, users should review the certification report alongside the relevant usage and administration guides, as well as the security target [ST], which outlines assumed threats, environmental factors, and usage conditions. This helps users decide if the product aligns with their security goals.

The JCOP 7.x on SN300 Secure Element combines a Java Card Operating System on an Embedded Secure Element with an NFC Controller on a single die. It also provides a Power Management Unit and IC specific software services.

- The Main Operating System (SMK - Secure Micro Kernel) creates separate and independently updatable secondary Operating Systems (Guest OS) providing a converged product consisting of • A Java Card Secure Element (eSE) Operating System
- A Java Card eUICC Operating System with UICC functionality in accordance with the GSMA Specification and external ISO-7816 connectivity

All Secondary OSs at the platform level are underpinned by the same Java Card and Global Platform technology, but are dedicated to their own application.
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 component of the SN300 on which the TOE executes is the embedded Secure Element, abbreviated to SN300_SE. TOE functionality is defined by the requirements in the [ST]. Additional information on TOE features is provided in chapter 4.

Brightsight ITSEF performed the evaluation. The evaluation was completed on September 29, 2026, resulting in the evaluation technical report [ETR]. The certification procedure was conducted in accordance with the EUCC, as set out in Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, and its amendments.

The scope of the evaluation is defined in the [ST]. The [ST] sets out the evaluation assumptions, the intended operating environment for the TOE, the security requirements, and evaluation assurance level at which the product is intended to meet those requirements. The TOE claims conformance to [PP].

Consumers are advised to confirm that their own environment is consistent with the [ST] and to take into account the comments, observations, and recommendations in this Certification Report.

The evaluation concluded that the TOE has no special configuration requirements beyond those specified in the user guidance. Users shall review these requirements and install the TOE in the operational environment accordingly.

The results documented in the evaluation technical report [ETR] provide sufficient evidence that the TOE meets the EAL5 augmented assurance requirements for the evaluated security functionality. The assurance level is augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and is recognised according to Article 52 of [CSA] as “High”.

The evaluation was performed using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 [CEM] and assessed conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 [CC] (Parts 1–5).

This certificate applies only to the specific version and release of the product in its evaluated configuration.

1.3 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.

1.4 Disclaimer(s)

The certification does not guarantee a product is completely free of exploitable vulnerabilities.

2 Identification of the ICT product

2.1 Unique identification

This certification considers the following product:

TOE name	NXP JCOP 7.x on SN300 Secure Element
TOE version(s)	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 JCOP 7.4 R1.07.0.1

2.2 Product components

The TOE comprises the following items:

- IC Hardware: NXP SN300 Series - Secure Element, identified as SN300_SE B1.1 J9.
- Embedded Software: JCOP 7.x OS including
  - Shared Code (with Cryptolib)
  - FlashOS;
  - CommOS;
  - SystemOS;
  - and SMK.
- For each version of the embedded software, the corresponding guidance documents are supplied, as listed below.

More specifically, for each version of the embedded software, the following elements are delivered. Please note that JCOP eUICC and CommOS are both delivered in embedded software but not part of the TOE.

- Delivery items for JCOP 7.0 R1.62.0.1, whose Embedded Software is identified as 1.62.0.1.

Type	Name	Delivery form
IC Hardware	NXP SN300 Series - Secure Element	Package WLCSP
Embedded Software	JCOP 7.0 R1.62.0.1 OS including Shared Code (with Cryptolib), FlashOS, CommOS, SystemOS, and SMK.[1]	On-chip software stored into the FLASH area of the TOE.
Document	JCOP 7.0 R1.62.0.1 User Guidance Manual (UGM)	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.0 R1.62.0.1 UGM Addendum	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.0 R1.62.0.1 UGM Anomaly	Electronic Document (PDF via NXP Docstore)

Type	Name	Delivery form
Document	JCOP 7.0 R1.62.0.1 (JCOP 7.0 17.4-1.62) UGM for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.0 R1.62.0.1 UGM Addendum for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.0 R1.62.0.1 UGM Addendum System Management	Electronic Document (PDF via NXP Docstore)

- Delivery items for JCOP 7.1 R1.04.0.1, whose Embedded Software is identified as 1.04.0.1.

Type	Name	Delivery form
IC Hardware	NXP SN300 Series - Secure Element	Package WLCSP
Embedded Software	JCOP 7.1 R1.04.0.1 OS including Shared Code (with Cryptolib), FlashOS, CommOS, SystemOS, and SMK.[1]	On-chip software stored into the FLASH area of the TOE.
Document	JCOP 7.1 R1.04.0.1 User Guidance Manual (UGM)	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.1 R1.04.0.1 UGM Addendum	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.1 R1.04.0.1 UGM Anomaly	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.1 R1.04.0.1 (JCOP 7.1 19.4-1.04) UGM for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.1 R1.04.0.1 UGM Addendum for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.1 R1.04.0.1 UGM Addendum System Management	Electronic Document (PDF via NXP Docstore)

- Delivery items for JCOP 7.2 R1.09.0.1, whose Embedded Software is identified as 1.09.0.1.

Type	Name	Delivery form
IC Hardware	NXP SN300 Series - Secure Element	Package WLCSP
Embedded Software	JCOP 7.2 R1.09.0.1 OS including Shared Code (with Cryptolib), FlashOS, CommOS, SystemOS, and SMK.[1]	On-chip software stored into the FLASH area of the TOE.

Type	Name	Delivery form
Document	JCOP 7.2 R1.09.0.1 User Guidance Manual (UGM)	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.2 R1.09.0.1 UGM Addendum	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.2 R1.09.0.1 UGM Anomaly	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.2 R1.09.0.1 (JCOP 7.2 20.4-1.06) UGM for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.2 R1.09.0.1 UGM Addendum for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.2 R1.09.0.1 UGM Addendum System Management	Electronic Document (PDF via NXP Docstore)

- Delivery items for JCOP 7.3 R1.07.0.1, whose Embedded Software is identified as 1.07.0.1.

Type	Name	Delivery form
IC Hardware	NXP SN300 Series - Secure Element	Package WLCSP
Embedded Software	JCOP 7.3 R1.07.0.1 OS including Shared Code (with Cryptolib), FlashOS, CommOS, SystemOS, and SMK.[1]	On-chip software stored into the FLASH area of the TOE.
Document	JCOP 7.3 R1.07.0.1 User Guidance Manual (UGM)	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.3 R1.07.0.1 UGM Addendum	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.3 R1.07.0.1 UGM Anomaly	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.3 R1.07.0.1 (JCOP 7.3 21.4-1.07) UGM for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.3 R1.07.0.1 UGM Addendum for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.3 R1.07.0.1 UGM Addendum System Management	Electronic Document (PDF via NXP Docstore)

- Delivery items for JCOP 7.4 R1.07.0.1, whose Embedded Software is identified as 1.07.0.1.

Type	Name	Delivery form
IC Hardware	NXP SN300 Series - Secure Element	Package WLCSP
Embedded Software	JCOP 7.4 R1.07.0.1 OS including Shared Code (with Cryptolib), FlashOS, CommOS, SystemOS, and SMK.[1]	On-chip software stored into the FLASH area of the TOE.
Document	JCOP 7.4 R1.07.0.1 User Guidance Manual (UGM)	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.4 R1.07.0.1 UGM Addendum	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.4 R1.07.0.1 UGM Anomaly	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.4 R1.07.0.1 (JCOP 7.4 22.4-1.07) UGM for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.4 R1.07.0.1 UGM Addendum for JCOP eSE	Electronic Document (PDF via NXP Docstore)
Document	JCOP 7.4 R1.07.0.1 UGM Addendum System Management	Electronic Document (PDF via NXP Docstore)

2.3 Additional requirements for the operating environment of the ICT product

As described in the [ST] section 5.2 in order to ensure compliant operation, the product's environment must ensure the following objective for the environment is met.

Name	Title
OE.Process-Sec-IC	Protection during composite product manufacturing[1]

[1] The title includes the term "composite" which is not appropriate for the current product but the OE is still valid as it applies to phases after TOE delivery.

With regards to OE.Resp-Appl, since the TOE implements the IC Embedded Software, this objective is met in by the ICT product and does not need to mandate the environment to meet certain conditions.

OE.CAP_FILE	**Applet** No CAP file loaded post-issuance shall contain native methods.
OE.VERIFICATION	**Bytecode Verification** All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. The latest available version of the verifier should be used. See SA.VERIFICATION for details. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform. Application Note: Constraints to maintain the isolation property of the platform are provided by the platform developer in application development guidance. The constraints apply to all application code loaded in the platform.
OE.CODE-EVIDENCE	**Code Evidence** For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION. For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification. For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required in OE.VERIFICATION are performed. On-card bytecode verifier is out of the scope of this Protection Profile. Application Note: For application code loaded post-issuance and verified off-card, the integrity and authenticity evidence can be achieved by electronic signature of the application code, after code verification, by the actor who performed verification.
OE.APPS-PROVIDER	**Application Provider** The AP shall be a trusted actor that provides applications. The AP is responsible for its security domain keys.
OE.TRUSTED-GUEST OS	**Trusted Guest OS** The external Guest OS provider is a trusted actor that is reponsible for the security and trust of his OS.
OE.VERIFICATION-AUTHORITY	**Verification Authority** The VA should be a trusted actor who is able to verify bytecode of an application loaded on the card, guarantee and generate the digital signature attached to an application and ensure that its public key for verifying the application signature is on the TOE.
OE.KEY-CHANGE	**Security Domain Key Change** The AP must change its security domain initial keys before any operation on it.

OE.KEY-CHANGE	**Security Domain Key Change** The AP must change its security domain initial keys before any operation on it.
OE.SECURITY-DOMAINS	**Security Domains** Security domains can be dynamically created, deleted and blocked during usage phase in post-issuance mode.
OE.USE_DIAG	**Secure TOE communication protocols** Secure TOE communication protocols shall be supported and used by the environment.
OE.USE_KEYS	**Protection of OPE keys** During the TOE usage, the terminal or system in interaction with the TOE, shall ensure the protection (integrity and confidentiality) of their own keys by operational means and/or procedures.
OE.PROCESS_SEC_IC	**Protection during composite product manufacturing** Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.
OE.CONFID-UPDATE-IMAGE.CREATE	**Confidentiality of Update Image - CREATE** The off-card Update Image Creator ensures that the image is signed and transferred encrypted to the device and is not disclosed during the creation and transfer. The keys used for signing and encrypting the image are kept confidential.

brightsight

By SGS

3 Contact information related to the evaluation of the ICT product

Developer Name	NXP Semiconductors Netherlands N.V.
EUCC certificate holder name and contact information	NXP Semiconductors Netherlands N.V. High Tech Campus 60, 5656AG Eindhoven, The Netherlands Contact: Cristina Surdu www.nxp.com cristina.surdu@nxp.com +31 (0) 642665695
Certification Body	SGS Brightsight B.V. (referred to as Brightsight CB) Brassersplein 2 2612 CT Delft The Netherlands Contact: Rob Kemper www.brightsightcb.com rob.kemper@sgs.com +31 15 269 25 44
National Cybersecurity Certification Authority	Dutch Authority for Digital Infrastructure – Ministry of Economic Affairs Contact: eucc@dutchncca.nl
ITSEF	SGS Brightsight B.V. (referred to as Brightsight ITSEF) Brassersplein 2 2612 CT Delft The Netherlands Contact: Juan Pablo Rodriguez www.brightsight.com Juan-Pablo.Rodriguez@sgs.com +31 15 269 25 00
Subcontractors	N/A

4 Security Policies

4.1 Security services

The hardware part of the ICT product has the following features:

- Security Services

Security Services	Name
SS.RNG	Random Number Generator
SS.TDES	Triple-DES coprocessor
SS.AES	AES coprocessor
SS.GCM	GCM coprocessor
SS.SGI	Symmetric General Interface functions
SS.CRC	CRC coprocessor

- Security Features

Security Features	Name
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.FOS-USE	FactoryOS use restrictions
SF.MEM-ACC	Memory Access Control
SF.SFR-ACC	Special Function Register Access Control
SF.FLASH-SVC	Flash Services

The software part of the ICT product has the following features:

- Security Functionality

Name	Title
SF.JCVM	Java Card Virtual Machine
SF.AM	Applet Migration
SF.CONFIG	Configuration Management
SF.OPEN	Card Content Management
SF.CRYPTO	Cryptographic Functionality
SF.RNG	Random Number Generator
SF.DATA_STORAGE	Secure Data Storage
SF.OSU	Operating System Update
SF.OM	Java Object Management
SF.MM	Memory Management

SF.PIN	PIN Management
SF.PERS_MEM	Persistent Memory Management
SF.EDC	Error Detection Code API
SF.HW_EXC	Hardware Exception Handling
SF.RM	Restricted Mode
SF.PID	Platform Identification
SF.SMG_NSC	No Side-Channel
SF.SENS_RES	Sensitive Result
SF.CONT_SEP	Context Separation

4.2 Vulnerability handling policy

4.2.1 Reference

[Incident-Resp] Product Security Incident Response Process, NXPOMS-1719007347-4179, 14 Mar 2024, NXP Semiconductors

4.2.2 Description

The vulnerability management process mandated by (EU) 2024/482 Chapter VI and the supplemented information required by (EU) 2024/482 Article 11 paragraph 4 bullet (c) has been provided in [PSIRT], and ALC_FLR.2 aspects have been assessed by the evaluator. The result was reported in [22-RPT-035].

The ITSEF has established that [PSIRT] has been provided to the Certification Body in order to meet (EU) 2024/482 regulation and has also verified that email-address psirt@nxp.com and NXP website www.nxp.com/psirt exist. All evaluator analysis with respect to vulnerability handling has been made within the ITSEF accreditations, such as ISO17025, leaving the developer responsibilities with NXP. The developer has explicitly been made aware of these (EU) 2024/482 responsibilities for a certificate holder.

4.3 Assurance continuity policy

N/A

4.4 Patch management procedure

N/A

5 Assumptions and clarification of scope

5.1 Assumptions on the ICT's product usage and deployment

As part of the evaluation activities of the AGD assurance class, the evaluator ensured that the guidance supplied as part of the TOE, – identified in the [ST] section 1.6- guarantees ICT product's usage and deployment in the form of minimum requirements, such as proper installation and configuration and hardware requirements being satisfied.

The positive verdict on the AGD evaluation activity serves also as verification that the security objectives for the environment identified in [ST] section are addressed by the guidance delivered together with the ICT product.

5.2 Assumptions for the environment for compliant operation

Assumptions about the operating environment are described in the [ST] sections 4.1.4 and 4.2.4 for the Security IC and the Java Card System, respectively.

The assumptions from [PP0084] applicable to the Security IC are listed below:

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Resp-Appl	Treatment of user data of the Composite TOE

The assumptions from [PP0099] applicable to the Embedded Software are listed below. Note that the assumption A.DELETION as defined in PP is excluded. The Card Manager is part of the TOE and therefore the assumption is no longer relevant.

A.CAP_FILE	**Applets without Native Methods** CAP Files loaded post-issuance do not contain native methods. The Java Card specification explicitly "does not include support for native methods" ([16]) outside the API.
A.VERIFICATION	**Bytecode Verification** All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. The latest available version of the verifier should be used.
A.USE_DIAG	**Usage of TOE's Secure Communication Protocol by OE** It is assumed that the operational environment supports and uses the secure communication protocols offered by the TOE.
A.USE_KEYS	**Protected Storage of Keys Outside of TOE** It is assumed that the keys which are stored outside the TOE and which are used for secure communication and authentication between Smart Card and terminals are protected for confidentiality and integrity in their own storage environment. This is especially true for D.APSD_KEYS, D.ISD_KEYS, and D.VASD_KEYS. **Info**: This is to assume that the keys used in terminals or systems are correctly protected for confidentiality and integrity in their own environment, as the disclosure of such information which is shared with the TOE but is not under the TOE control, may compromise the security of the TOE.
A.PROCESS-SEC-IC	**Protection during Packaging, Finishing and Personalisation** It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately. The assets to be protected are: The information and material produced and/or processed by the Security IC Embedded Software Developer in Phase 1 and by the Composite Product Manufacturer can be grouped as follows: 1. the Security IC Embedded Software including specifications, implementation and related documentation, 2. pre-personalisation and personalisation data including specifications of formats and memory areas, test related data, 3. the User Data and related documentation, and 4. material for software development support as long as they are not under the control of the TOE Manufacturer.

5.3 Threats to the ICT product not countered by its security functions

Threats are described in [ST] sections 4.1.2 and 4.2.2 for the Security IC and the Embedded Software, respectively.

All threats affecting the Security IC are countered by the TOE, whereas certain threats are partially addressed by the environment, as shown in the table below built upon the data in [ST] section 5.3.2.1.

Table 1 Threats countered by the environment

Threat	Security Objective for the environment
T.CONFID-UPDATE-IMAGE.LOAD	OE.CONFID-UPDATE IMAGE.CREATE
T.CONFID-APPLI-DATA	OE.VERIFICATION
T.CONFID-JCS-CODE	OE.VERIFICATION
T.CONFID-JCS-DATA	OE.VERIFICATION
T.INTEG-APPLI-CODE	OE.VERIFICATION OE.CODE-EVIDENCE
T.INTEG-APPLI-CODE.LOAD	OE.CODE-EVIDENCE
T.INTEG-APPLI-DATA	OE.VERIFICATION OE.CODE-EVIDENCE
T.INTEG-APPLI-DATA.LOAD	OE.CODE-EVIDENCE
T.INTEG-JCS-CODE	OE.CODE-EVIDENCE
T.INTEG-JCS-DATA	OE.VERIFICATION OE.CODE-EVIDENCE
T.EXE-CODE.1	OE.VERIFICATION
T.EXE-CODE.2	OE.VERIFICATION
T.NATIVE	OE.VERIFICATION

6 Architectural information

The TOE is the "JCOP 7.x on SN300 B1.1 J9 Secure Element" which combines a Java Card Operating System on an Embedded Secure Element with a NFC Controller on a single die. It also provides a Power Management Unit and IC specific software services.

The Main Operating System (SMK) creates separate and independently updatable secondary Operating Systems (Guest OS) providing a converged product consisting of

- A Java Card Secure Element (eSE) Operating System
- A Java Card eUICC Operating System with UICC functionality in accordance with the GSMA Specification and external ISO-7816 connectivity (not in scope)

All Secondary OSs at the platform level are underpinned by the same Java Card and Global Platform technology, but are dedicated to their own application.

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

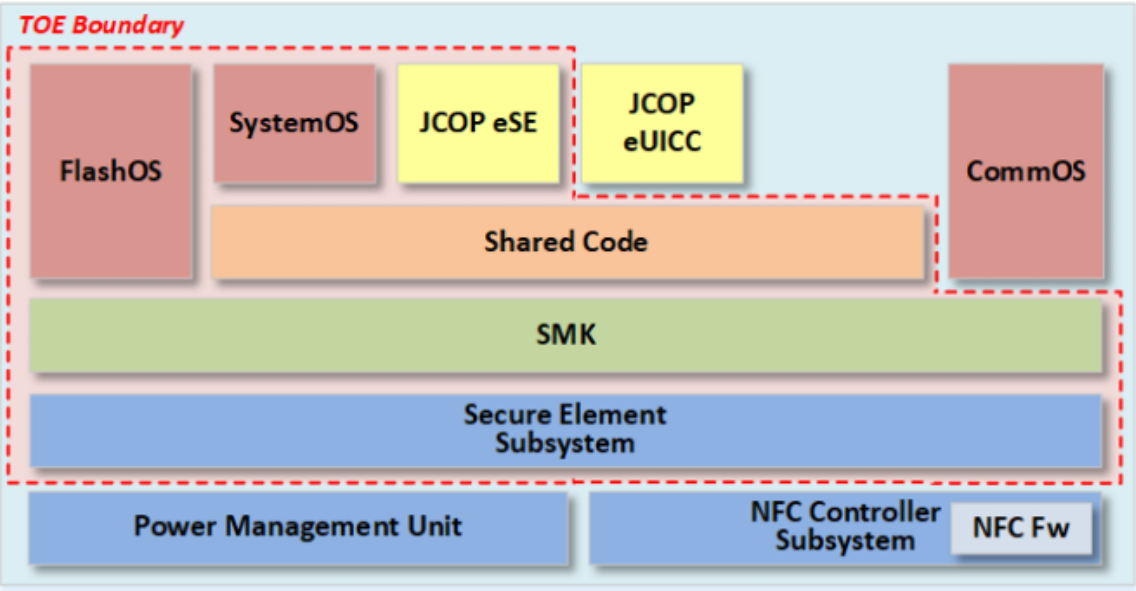


Figure 1. Logical architecture of the TOE.

The TOE has the following features:

- Hardware-supported features
  - hardware to perform computations on multi-precision 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)[1], Output Feedback (OFB) 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
- hardware to control access to memories and hardware components.

- 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 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 sensitive data. In addition, the Crypto Library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the TOE.
  - Random number generation according to class DRG.3 or DRG.4 of AIS20

- Java Card 3.1 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.

Note 1: AES_CFB is not supported and not claimed for JCOP 7.4.

- Optional JC3.1 Cryptographic APIs are not implemented. A call to those APIs throw an exception of type ISO7816.SW_FUNC_NOT_SUPPORTED in this case.

- 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, SCP11, SCP04).
  - Delegated Management, DAP (RSA 1024 and ECC 256).

- 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 System OS. This component allows only NXP authorised 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.
  - 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.

- Functionality without specific security claims
  - 5G features as per SIM Alliance 2.3
  - eUICC features hosted in eUICC domain outside the boundaries of the TOE
  - Programmable Timeout for SMB with Limitations
  - CPLC data made available through SystemInfo
  - Proprietary Bytecode Compression applied after BCV. Some standard bytecodes are replaced by optimized byte codes (one to one) with exactly the same operation.
  - Compliance to Secure Element configuration, Common Implementation Configuration, UICC Configuration, and UICC Configuration Contactless Extension.

7 Supplementary cybersecurity information

In relation with information to be made available by the certificate holder according to (EU) 2024/482 Chapter VII, https://www.nxp.com/products/nxp-product-information/eucc-certified-products:EUCC-CERTIFIED and www.nxp.com/psirt is stated to contain guidance and information needed by the user, provide information up to five years after the certificate validity, and to describe the process of responsible disclosure of vulnerabilities.

8 ICT product evaluation summary and evaluated configuration

8.1 Required information

Assurance Components used	• EAL5, augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2
State of the Art documents and other criteria used	• "Minimum Site Security Requirements", version 2, February 2025 • "Application of CC to Integrated Circuits", version 2, December 2024 • "Security Architecture Requirements for Smart Cards and Similar Devices", version 1.1, 31 January 2024 • "Application of Attack Potential to Smartcards", version 2, 19 December 2025 • "STAR methodology", version 1, 25 March 2025 • "Agreed Cryptographic Mechanisms", Version 2, May 2025 • "GUIDELINES ON VULNERABILITY MANAGEMENT AND DISCLOSURE", Version 1.1, January 2025 • "Application of CC to integrated circuits", Version 2, December 2024 • "CERTIFICATION OF "OPEN" SMART CARD PRODUCTS", Version 1.1, October 2023 • "Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs", Version 1.1, October 2023 • Methodology used for vulnerability analysis: ITSEF proprietary method
Protection profile details:	[PP]

8.2 Product settings and configuration

The TOE comprises the following hardware and software:

	Name	Version
Hardware	NXP SN300 Series Secure Element	SN300_SE B1.1 J9
Software	JCOP 7.0 R1.62.0.1	R1.62.0.1 N5A2M50001380000
	JCOP 7.1 R1.04.0.1	R1.04.0.1 N5A2M500020A0000
	JCOP 7.2 R1.09.0.1	R1.09.0.1 N5A2M500028D0000
	JCOP 7.3 R1.07.0.1	R1.07.0.1 N5A2M500030B0000
	JCOP 7.4 R1.07.0.1	R1.07.0.1 N5A2M500033B0000

The TOE can be in one of the following configurations: 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 or JCOP 7.4 R1.07.0.1. Each configuration exists in a single evaluated configuration. The TOE can be configured using the Config Applet, and all changes that can be made using the Config Applet are within the scope of the evaluation.

9 Results of the evaluation and information regarding the certificate

9.1 Required information

Certificate identifier	EUCC-3100-2026-0002
Certificate date of issuance	2026-10-20
Certificate period of validity	5 years
Assurance level	High
Assurance requirements that are met	EAL5, augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2

9.2 Assurance requirements

The chosen assurance level is EAL5, augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2, ASE_TSS.2. A detailed decomposition of the evaluation results can be found in Appendix A.

9.3 Testing approach and results

9.3.1 Testing approach and depth

9.3.2 Penetration testing

The vulnerability analysis was performed according to the AVA_VAN.5 requirements in line with the methodologies mandated by the technical domain, resulting in a test plan reported in the [ETR].

9.3.3 Test results

The testing activities, including configurations, test cases and 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 [ST] and functional specification.

No exploitable vulnerabilities were found with the penetration test plan devised by the evaluator.

The test results reveal that the TOE is resistant to a basic attack potential associated to the attack rating in the scope of AVA_VAN.5.

10 Security target

The certification refers to the following security target:

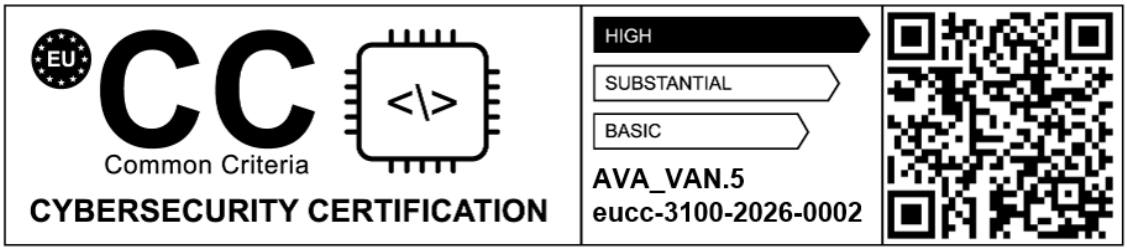
ST reference	NXP JCOP 7.x on SN300 Secure Element, Security Target, Revision 3.8, 27 July 2026

Please note that the version published together with this certification report has been sanitized in line with [CCDB-2006-04-004], resulting in [ST-lite].

brightsight

By SGS

11 Mark or label associated to the scheme



12 Glossary

No terms have been used that are not already defined by the CC or CEM.

13 Bibliography

13.1.1 Evaluation criteria

[CC]	Common Criteria for Information Technology Security Evaluation, Part 1, 2, 3, 4 and 5, CC:2022 Revision 1
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CC:2022 Revision 1
[CCMB-2025-001]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[AIS 20/31]	Functionality classes and evaluation methodology for deterministic/physical random number generators, version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[AIS 34]	Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6, version 3, 03.09.2009, Bundesamt für Sicherheit in der Informationstechnik
[AIS 46]	Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, version 3, 04.12.2013, Bundesamt für Sicherheit in der Informationstechnik
[NI002]	Content and presentation of evaluation review meeting version 1
[MSSR]	ENISA, Minimum Site Security Requirements, v2, February 2025
[CC_IC]	ENISA, Application of Common Criteria to Integrated Circuits, v2, December 2024
[SC_ARC]	ENISA, Security Architecture Requirements for Smart Cards and Similar Devices, v1.1, October 2023
[SC_OPEN]	ENISA, Certification of “open” Smart Card products, v1.1, October 2023
[SC_COMP]	ENISA, Composite Product Evaluation for smart cards and similar devices, v2.0
[AT_POT]	ENISA, Application of Attack Potential to Smartcards, v2.0

13.1.2 Evaluation technical report

[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 - JCOP 7.4 R1.07.0.1)” – EAL5 augmented with ALC_DVS.2, ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5, v3.0, 19 October 2026
[ETRfC]	Evaluation Technical Report for Composition “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 - JCOP 7.4 R1.07.0.1)” – EAL5 augmented with ASE_TSS.2, AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2, v2.0, 1 September 2026

13.1.3 Technical reference documentation

[PP]	Wrapper reference for [PP0084] and [PP0099]
[PP0084]	Security IC Platform Protection Profile including Functional Packages, version 2.0, 16 December 2025
[PP0099]	Java Card System – Open Configuration Protection Profile, version 3.2, July 2024

13.1.4 Developer documentation

[ST]	NXP JCOP 7.x on SN300 Secure Element Security Target, Rev. 3.8 — 27 July 2026
[ST-lite]	NXP JCOP 7.x on SN300 Secure Element Security Target Lite, Rev. 3.8 — 27 July 2026
[UG-AD-JCOP 7.0]	NXP JCOP 7.0 User Guidance Manual Addendum, Rev. 1.24.1, 2024-04-09
[UG-AD-SM-JCOP 7.0]	NXP JCOP 7.1 User Guidance Manual Addendum System Management, Rev. 3.04.2, 2024-04-29
[UG-AS-JCOP 7.0]	NXP JCOP 7.0 Anomaly Sheet, Rev. 1.24.1, 2024-04-09
[UG-JCOP-eSE-7.0]	NXP JCOP 7.0 R1.62.0.1 (JCOP 7.0 17.4-1.62 User Guidance Manual for JCOP eSE, Rev. 1.20.7, 2025-02-24
[UG-JCOP-eSE-AD-7.0]	NXP JCOP 7.0 User Guidance Manual Addendum for JCOP eSE, Rev. 1.24.1, 2024-04-09
[UG-JCOP 7.0]	NXP JCOP 7.0 User Guidance Manual, Rev. 1.24.7, 2025-02-24
[UG-AD-JCOP 7.1]	NXP JCOP 7.1 User Guidance Manual Addendum, Rev. 3.04.1, 2024-04-02
[UG-AD-SM-JCOP 7.1]	NXP JCOP 7.2 User Guidance Manual Addendum System Management, Rev. 4.05.0, 2024-02-28
[UG-AS-JCOP 7.1]	NXP JCOP 7.1 Anomaly Sheet, Rev. 3.04.1, 2024-04-02
[UG-JCOP-eSE-7.1]	NXP JCOP 7.1 R1.04.0.1 (JCOP 7.1 19.4-1.04) User Guidance Manual for JCOP eSE, Rev. 3.06.4, 2025-02-17
[UG-JCOP-eSE-AD-7.1]	NXP JCOP 7.1 User Guidance Manual Addendum for JCOP eSE, Rev. 3.05.1, 2024-04-02
[UG-JCOP 7.1]	NXP JCOP 7.1 User Guidance Manual, Rev. 3.05.4, 2025-02-17
[UG-AD-JCOP 7.2]	NXP JCOP 7.2 User Guidance Manual Addendum, Rev. 4.05.0, 2024-02-28
[UG-AD-SM-JCOP 7.2]	NXP JCOP 7.2 User Guidance Manual Addendum System Management, Rev. 4.05.0, 2024-02-28
[UG-AS-JCOP 7.2]	NXP JCOP 7.2 Anomaly Sheet, Rev. 4.05.0, 2024-02-28
[UG-JCOP-eSE-7.2]	NXP JCOP 7.2 R1.09.0.1 (JCOP 7.2 20.4-1.06) User Guidance Manual for JCOP eSE, 4.05.3, 2025- 02-18
[UG-JCOP-eSE-AD-7.2]	NXP JCOP 7.2 User Guidance Manual Addendum for JCOP eSE, Rev. 4.05.0, 2024-02-28
[UG-JCOP 7.2]	NXP JCOP 7.2 User Guidance Manual, Rev. 4.05.3, 2025-02-18
[UG-AD-JCOP 7.3]	JCOP 7.3 User Guidance Manual Addendum, Rev. 5.6.0, 2025-03-07
[UG-AD-SM-JCOP 7.3]	JCOP 7.3 User Guidance Manual Addendum System Management, Rev. 5.6.0, 2025-03-07

[UG-AS-JCOP 7.3]	JCOP 7.3 User Guidance Manual Anomaly Sheet, Rev. 5.6.1, 2025-04-09
[UG-JCOP-eSE-7.3]	JCOP 7.3 R1.07.0.1 (JCOP 7.3 SE 21.4-1.07) User Guidance Manual for JCOP Ese, Rev. 5.6.2, 2025- 09-03
[UG-JCOP-eSE-AD-7.3]	NXP JCOP 7.2 User Guidance Manual Addendum for JCOP eSE, Rev. 4.05.0, 2024-02-28
[UG-JCOP 7.3]	JCOP 7.3 User Guidance Manual, Rev. 5.6.2, 2025-08-07
[UG-AD-JCOP 7.4]	JCOP 7.4 User Guidance Manual Addendum, Rev. 6.6.0, 11 March 2026
[UG-AD-SM-JCOP 7.4]	JCOP 7.4 User Guidance Manual Addendum System Management, Rev. 6.6.0, 11 March 2026
[UG-AS-JCOP 7.4]	JCOP 7.4 User Guidance Manual Anomaly Sheet, Rev. 6.6.0, 11 March 2026
[UG-JCOP-eSE-7.4]	JCOP 7.4 R1.07.0.1 (JCOP 7.4 22.4-1.07) User Guidance Manual for JCOP Ese, Rev. 6.6.2, June 2026
[UG-JCOP-eSE-AD-7.4]	JCOP 7.4 User Guidance Manual Addendum for JCOP eSE, Rev. 6.6.0, 11 March 2026
[UG-JCOP 7.4]	JCOP 7.4 User Guidance Manual, Rev. 6.6.2, 11 June 2026
[Errata]	ES_JCOP7.x Documentation Errata Rev. 1.4 — 11 March 2026
[SN300-NFC][v3.1]	SN300 family; SN300V, SN300R and SN300W Single Chip Secured (NFC) controller, Objective data sheet, Rev. 3.1, 21 October 2022
[PSIRT]	Product Security Incident Response Process 14-MAR-2024

13.1.5 ITSEF documentation

[EAR]	wrapper reference for [23-RPT-815], [24-RPT-740], [25-RPT-845] and [26-RPT-470]
[26-RPT-469]	NXP JCOP 7.x on SN300 Secure Element - IR-ASE v0.5, 27 July 2026
[26-RPT-473]	NXP JCOP 7.x with eUICC-eSE on SN300 - ADV-AGD Reference Document v0.4, 20 July 2026
[22-RPT-057]	SN300 Series – Secure Element, ADV-AGD Reference Document, v1.0, 26 January 2022
[26-RPT-474]	NXP JCOP 7.x on SN300 Secure Element ALC v3.0, 19-10-2026
[22-RPT-035]	SN300 Series – Secure Element, ALC Presentation, v1.0, 2022-01-26
[26-RPT-471]	NXP JCOP 7.x with eUICC (eSE) on SN300 - ADV Presentation, v0.2, 20.07.2026
[26-RPT-472]	NXP JCOP 7.x with eUICC (eSE) on SN300 - SFR-TSFI Tracing, v0.2, 07/06/2026
[22-RPT-070]	SN300 Series – Secure Element, ADV Presentation, v3.0, 19 April 2022
[26-RPT-476]	NXP JCOP 7.x eSE on SN300 - ATE Presentation v2.0, 28.09.2026
[22-RPT-911]	DRG Test Results, v1.0, 25 March 2021
[22-RPT-234]	ATE Witnessing Test Plan, v1.0, 15 March 2022
[25-MEM-017]	NXP JCOP 7.x on SN300 Secure Element ATE test plan and test result v1.2, 24 July 2025

[26-MEM-003]	JCOP7.4_SN300_Star_eSE_witnessing TestPlan and Test Results v3.0, 17 July 2026
[22-RPT-201]	ATE presentation EAL4+ NXP SN300 Series, v2.0, 04/04/2022
[25-RPT-1403]	NXP JCOP 7.x eSE on SN300 - ATE Presentation v2.0, 1 December 2025
[26-RPT-477]	NXP JCOP 7.x eSE on SN300 - AVA Presentation v2.0, 2026-09-24
[22-RPT-191]	Test Plan for JCOP 7.0 with eUICC/eSE v1.0, 3 March 2022
[25-RPT-004]	Code review and VA report - NXP JCOP 7.3 R1.07.0.1/2 Java Card implemented on the NXP SN300 Series B1.1 J9 microcontroller, v3.1, 23 April 2025
[25-RPT-845]	Evaluator Assessment of Changes Report (EAR) - 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), v2.0, 5 January 2026
[26-RPT-470]	Evaluator Assessment of Changes Report (EAR) - 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 - JCOP 7.4 R1.07.0.1), v0.4, 31 July 2026
[24-RPT-740]	Evaluator Assessment of Changes Report (EAR) - 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), v3.0, 24 September 2024
[23-RPT-1157]	EMVCo Platform Delta Security evaluation of NXP JCOP 7.1 R2.01.0.1 Java Card implemented on the NXP SN300 Series B1.1 J9 microcontroller, Version 1.0, October 2023
[23-RPT-1429]	Code review and VA report - NXP JCOP 7.2 R1.09.0.1 Java Card implemented on the NXP SN300 Series B1.1 J9 microcontroller, v4.0, 8 March 2024
[23-RPT-815]	Evaluator Assessment of Changes Report (EAR) NXP JCOP7.x on SN300 B1.1 Secure Element, Version 3.0, 6 September 2023
[23-RPT-132]	EMVCo Platform Delta Security Evaluation of the NXP JCOP 7.1 R1.04.0.1 Java Card implemented on the NXP SN300 Series B1.1 J9 microcontroller, Version 1.0, 14 April 2023
[23-RPT-315]	EMVCo Platform Security Renewal evaluation of the NXP JCOP 7.0 Java Card platforms implemented on the NXP SN300 Series B1.1 J9 microcontroller, version 2.0, 6 April 2023
[22-RPT-944]	EMVCo Platform Delta Security evaluation of NXP JCOP 7.0 R2.04.0.1 Java Card implemented on the NXP SN300 Series B1.1 J9 microcontroller, Version 3.0, 7 November 2022
[22-RPT-232]	Code Review, Vulnerability Analysis – JCOP 7.0 eSE on SN300, v7.0,
[22-RPT-492]	JCOP 7.0 with eUICC on SN300 Series – Secure Element, Test Results, v3.0, 28 June 2022
[22-RPT-119]	Code review of NXP JCOP 7.0 with eUICC extension on SN300 Secure Element, v1.0, 31 March 2022
[22-RPT-034]	Code Review, Vulnerability Analysis – Crypto Library, v2.0, 20 April 2022

[21-RPT-1241]	Hardware Review, v4.0, 2 May 2022
[21-RPT-1318]	Code Review of the IC Dedicated Support Software, v3.0, 17 March 2022
[21-RPT-1236]	NXP SN300 Series - Secure Element - AVA Test Plan, v3.0, 2 February 2022
[22-RPT-222]	AVA and ATE Test Results “NXP SN300 Series – Secure Element” v3.0, 2 May 2022
[26-RPT-010]	EMVCo Platform Delta Security Evaluation of the NXP JCOP 7.4 R1.07.0.1 Java Card implemented on the NXP SN300 Series B1.1 J9 microcontroller, v4.0, 28 September 2026
[24-RPT-1508]	JCOP 7.x on SN300 EMVCo Platform Security Renewal Evaluation Report EMVCo Platform Security Renewal evaluation of the NXP JCOP 7.x Java Card Platforms implemented on the NXP SN300 Series B1.1 J9 microcontroller, v2.0, 24 March 2025
[25-RPT-348]	JCOP7.3 SN300 R1.07.0.1 EMVCo Platform ETR, v1.0, 24 April 2025
[25-RPT-291]	25-RPT-291 Evaluator Assessment of Changes Report NXP JCOP 7.x with eUICC extension on SN300 B1.1 Secure Element v4.0, 18 August 2025
[24-RPT-1495]	Evaluator Assessment of Changes Report (EAR) NXP SN300 Series - Secure Element – Partial ETR, Version 4.0, 1 May 2025
[24-RPT-416]	EMVCo Platform Security Renewal evaluation of the NXP JCOP 7.x Java Card Platform implemented on the NXP SN300 Series B1.1 J9, v3.0, 17 April 2024
[25-RPT-1364]	25-RPT-1364 NXP SN300 Series IC EMVCo Renewal Evaluation Report v3.0, 28 September 2026

brightsight

By SGS

A Mapping of evaluator actions and verdicts

A.1 ASE

Evaluator action	Content (CEM ID)	Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
ST introduction ASE_INT				
1.1E	1.1C (CEM:1-1)	[26-RPT-469] §2.1	Pass	Pass
	1.2C (1-2)	[26-RPT-469] §2.1	Pass	Pass
	1.3C (1-3/4)	[26-RPT-469] §2.1	Pass	Pass
	1.4C (1-5)	[26-RPT-469] §2.1	Pass	Pass
	1.5C (1-6/7)	[26-RPT-469] §2.1	Pass	Pass
	1.6C (1-8)	[26-RPT-469] §2.1	Pass	Pass
	1.7C (1-9)	[26-RPT-469] §2.1	Pass	Pass
	1.8C (1-10)	[26-RPT-469] §2.1	Pass	Pass
	1.9C (1-11)	[26-RPT-469] §2.1	Pass	Pass
1.2E	- (1-12)	[26-RPT-469] §2.1	Pass	Pass
Conformance claims ASE_CCL				
1.1E	1.1C (1-1)	[26-RPT-469] §2.2	Pass	Pass
	1.2C (1-2)	[26-RPT-469] §2.2	Pass	Pass
	1.3C (1-3)	[26-RPT-469] §2.2	Pass	Pass
	1.4C (1-4/5)	[26-RPT-469] §2.2	Pass	Pass
	1.5C (1-6/7/8/9 /10/11/12)	[26-RPT-469] §2.2	Pass	Pass
	1.6C (1-13, 1-14)	[26-RPT-469] §2.2	Pass	Pass
	1.7C (1-15)	[26-RPT-469] §2.2	Pass	Pass
	1.8C (1-16)	[26-RPT-469] §2.2	Pass	Pass
	1.9C (1-17)	[26-RPT-469] §2.2	Pass	Pass
	1.10C (1-18)	[26-RPT-469] §2.2	Pass	Pass
	1.11C (1-19)	[26-RPT-469] §2.2	Pass	Pass

Evaluator action	Content (CEM ID)	Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
	1.12C (1-20)	[26-RPT-469] §2.2	Pass	Pass
	1.13C (1-21)	[26-RPT-469] §2.2	Pass	Pass
Security problem definition ASE_SPD				
1.1E	1.1C (1-1)	[26-RPT-469] §2.3	Pass	Pass
	1.2C (1-2)	[26-RPT-469] §2.3	Pass	Pass
	1.3C (1-3)	[26-RPT-469] §2.3	Pass	Pass
	1.4C (1-4)	[26-RPT-469] §2.3	Pass	Pass
Security objectives ASE_OBJ				
2.1E	2.1C (2-1)	[26-RPT-469] §2.4	Pass	Pass
	2.2C (2-2)	[26-RPT-469] §2.4	Pass	Pass
	2.3C (2-3)	[26-RPT-469] §2.4	Pass	Pass
	2.4C (2-4)	[26-RPT-469] §2.4	Pass	Pass
	2.5C (2-5)	[26-RPT-469] §2.4	Pass	Pass
	2.6C (2-6)	[26-RPT-469] §2.4	Pass	Pass
Extended components definition (ASE_ECD)				
1.1E	1.1C (1-1)	[26-RPT-469] §2.5	Pass	Pass
	1.2C (1-2)	[26-RPT-469] §2.5	Pass	Pass
	1.3C (1-3/4)	[26-RPT-469] §2.5	Pass	Pass
	1.4C (1-5/6/7/8 /9/10/11)	[26-RPT-469] §2.5	Pass	Pass
	1.5C (1-12)	[26-RPT-469] §2.5	Pass	Pass
1.2E	- (1-13)	[26-RPT-469] §2.5	Pass	Pass
Security requirements (ASE_REQ)				
2.1E	2.1C (2-1/2)	[26-RPT-469] §2.6	Pass	Pass
	2.2C (2-3/4)	[26-RPT-469] §2.6	Pass	Pass
	2.3C (2-5/6/7/8)	[26-RPT-469] §2.6	Pass	Pass
	2.4C (2-9)	[26-RPT-469] §2.6	Pass	Pass
	2.5C (2-10)	[26-RPT-469] §2.6	Pass	Pass

Evaluator action	Content (CEM ID)	Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
	2.6C (2-11/12/13/14)	[26-RPT-469] §2.6	Pass	Pass
	2.7C (2-15)	[26-RPT-469] §2.6	Pass	Pass
	2.8C (2-16)	[26-RPT-469] §2.6	Pass	Pass
	2.9C (2-17)	[26-RPT-469] §2.6	Pass	Pass
	2.10C (2-18)	[26-RPT-469] §2.6	Pass	Pass
	2.11C (2-19)	[26-RPT-469] §2.6	Pass	Pass
TOE summary specification (ASE_TSS)				
1.1E	1.1C (2-1)	[26-RPT-469] §2.7	Pass	Pass
	2.2C (2-2)	[26-RPT-469] §2.7	Pass	Pass
	2.3C (2-3)	[26-RPT-469] §2.7	Pass	Pass
2.2E	- (2-4)	[26-RPT-469] §2.7	Pass	Pass

A.2 ADV

		Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
Security architecture (ADV_ARC)				
1.1E	1.1C	[26-RPT-471] Part 4	Pass	Pass
	1.2C	[26-RPT-471] Part 4	Pass	Pass
	1.3C	[26-RPT-471] Part 4	Pass	Pass
	1.4C	[26-RPT-471] Part 4	Pass	Pass
	1.5C	[26-RPT-471] Part 4	Pass	Pass
Functional specification ADV_FSP				
ADV_FSP.5.1E	5.1C	[26-RPT-471] Part 1	Pass	Pass
	5.2C	[26-RPT-471] Part 1	Pass	Pass
	5.3C	[26-RPT-473] Section 3.1	Pass	Pass
	5.4C	[26-RPT-473] Section 3.1	Pass	Pass
	5.5C	[26-RPT-473] Section 3.1	Pass	Pass
	5.6C	[26-RPT-473] Section 3.2	Pass	Pass

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
	5.7C	[26-RPT-473] Section 3.2	Pass	Pass
	5.8C	[26-RPT-471] Part 3	Pass	Pass
	5.9C	[26-RPT-471] Part 3	Pass	Pass
ADV_FSP.5.2E	-	[26-RPT-471] Part 4	Pass	Pass
Implementation representation ADV_IMP				
1.1E	1.1C	[26-RPT-471] Part 7	Pass	Pass
	1.2C	[26-RPT-471] Part 7	Pass	Pass
	1.3C	[26-RPT-471] Part 7	Pass	Pass
TSF internals ADV_INT				
ADV_INT.2.1E	2.1C	[26-RPT-471] Part 5	Pass	Pass
	2.2C	[26-RPT-471] Part 5	Pass	Pass
ADV_INT.2.2E		[26-RPT-471] Part 5, 7	Pass	Pass
TOE design ADV_TDS				
ADV_TDS.4.1E	4.1C	[26-RPT-471] Part 2	Pass	Pass
	4.2C	[26-RPT-471] Part 2	Pass	Pass
	4.3C	[26-RPT-471] Part 2	Pass	Pass
	4.4C	[26-RPT-471] Part 2	Pass	Pass
	4.5C	[26-RPT-471] Part 2	Pass	Pass
	4.6C	[26-RPT-471] Part 2	Pass	Pass
	4.7C	[26-RPT-471] Part 2	Pass	Pass
	4.8C	[26-RPT-471] Part 2	Pass	Pass
	4.9C	[26-RPT-471] Part 2	Pass	Pass
	4.10C	[26-RPT-471] Part 2	Pass	Pass
ADV_TDS.4.2E		[26-RPT-471] Part 3	Pass	Pass

A.3 AGD

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
Operational user guidance AGD_OPE				

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
AGD_OPE.1.1E	1.1C	[26-RPT-473] Chapter 4	Pass	Pass
	1.2C	[26-RPT-473] Chapter 4	Pass	Pass
	1.3C	[26-RPT-473] Chapter 4	Pass	Pass
	1.4C	[26-RPT-473] Chapter 4	Pass	Pass
	1.5C	[26-RPT-473] Chapter 5	Pass	Pass
	1.6C	[26-RPT-473] Chapter 6	Pass	Pass
	1.7C	[26-RPT-473] Chapter 4 - 8	Pass	Pass
Preparative procedures AGD_PRE.				
AGD_PRE.1.1E	1.1C	[26-RPT-473] Chapter 7	Pass	Pass
	1.2C	[26-RPT-473] Chapter 6 and 8	Pass	Pass
AGD_PRE.1.2E		[26-RPT-473] Part 5	Pass	Pass

A.4 ALC

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
CM capabilities ALC_CMC				
ALC_CMC.4.1E	4.1C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.2C	[26-RPT-474] 1st meeting	Pass	Pass
	4.3C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.4C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.5C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.6C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.7C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.8C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.9C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
	4.10C	[26-RPT-474] 2nd meeting. ALC_CMC	Pass	Pass
CM Scope ALC_CMS				
ALC_CMS.5.1E	5.1C	[26-RPT-474] 1st meeting	Pass	Pass
	5.2C	[26-RPT-474] 2nd meeting. ALC_CMS	Pass	Pass

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
	5.3C	[26-RPT-474] 2nd meeting. ALC_CMS	Pass	Pass
Delivery ALC_DEL				
ALC_DEL.1.1E	1.1C	[26-RPT-474] 2nd meeting. ALC_DEL	Pass	Pass
Development security ALC_DVS				
ALC_DVS.2.1E	2.1C	[26-RPT-474] 2nd meeting. ALC_DVS	Pass	Pass
	2.1C	[26-RPT-474] 2nd meeting. ALC_DVS	Pass	Pass
ALC_DVS.2.2E		[26-RPT-474] 2nd meeting. ALC_DVS	Pass	Pass
Life cycle definition ALC_LCD				
ALC_LCD.1.1E	1.1C	[26-RPT-474] 2nd meeting. ALC_LCD	Pass	Pass
	1.2C	[26-RPT-474] 2nd meeting. ALC_LCD	Pass	Pass
Tools and techniques ALC_TAT				
ALC_TAT.2.1E	2.1C	[26-RPT-474] 2nd meeting. ALC_TAT	Pass	Pass
	2.2C	[26-RPT-474] 2nd meeting. ALC_TAT	Pass	Pass
	2.3C	[26-RPT-474] 2nd meeting. ALC_TAT	Pass	Pass
ALC_TAT.2.2E		[26-RPT-474] 2nd meeting. ALC_TAT	Pass	Pass
Flaw remediation ALC_FLR				
ALC_FLR.2.1E	2.1C	[26-RPT-474] ALC_FLR	Pass	Pass
	2.2C	[26-RPT-474] ALC_FLR	Pass	Pass
	2.3C	[26-RPT-474] ALC_FLR	Pass	Pass
	2.4C	[26-RPT-474] ALC_FLR	Pass	Pass
	2.5C	[26-RPT-474] ALC_FLR	Pass	Pass
	2.6C	[26-RPT-474] ALC_FLR	Pass	Pass
	2.7C	[26-RPT-474] ALC_FLR	Pass	Pass
	2.8C	[26-RPT-474] ALC_FLR	Pass	Pass

A.5 ATE

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
Coverage ATE_COV				

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
ATE_COV.2.1E	2.1C	[26-RPT-476] Part 2	Pass	Pass
	2.2C	[26-RPT-476] Part 2	Pass	Pass
Depth ATE_DPT				
ATE_DPT.3.1E	3.1C	[26-RPT-476] Part 3	Pass	Pass
	3.2C	[26-RPT-476] Part 3	Pass	Pass
	3.3C	[26-RPT-476] Part 3	Pass	Pass
Functional tests ATE_FUN				
ATE_FUN.1	1.1C	[26-RPT-476] Part 1	Pass	Pass
	1.2C	[26-RPT-476] Part 1	Pass	Pass
	1.3C	[26-RPT-476] Part 1	Pass	Pass
	1.4C	[26-RPT-476] Part 1	Pass	Pass
Independent testing ATE_IND				
ATE_IND.2.1E	2.1C	[26-RPT-476] Part 5	Pass	Pass
	2.2C	[26-RPT-476] Part 4 and Part 5	Pass	Pass
ATE_IND.2.2E		[26-RPT-476] Part 4 and Part 5	Pass	Pass
ATE_IND.2-3E		[26-RPT-476] Part 4 and Part 5	Pass	Pass

A.6 AVA

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
Vulnerability analysis AVA_VAN.5.1				
AVA_VAN.5.1E	5.1C	[26-RPT-477] Vulnerability analysis / Test Plan	Pass	Pass
	5.2C	[26-RPT-477] Vulnerability analysis	Pass	Pass
AVA_VAN.5.2E		[26-RPT-477] Vulnerability analysis	Pass	Pass
AVA_VAN.5.3E		[26-RPT-477] Vulnerability analysis	Pass	Pass
AVA_VAN.5.4E		[26-RPT-477] Test Plan / Results	Pass	Pass