TrustCB B.V.

Certification Report

NXP SN300 Series - Secure Element SN300_SE B1.1 J9

Sponsor and developer:	***NXP Semiconductors Germany*** **Beiersdorfstraße 12** **22529 Hamburg** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300122-02-CR**
Report version:	**1**
Project number:	NSCIB-**2300122-02**
Author(s):	**Haico Haak**
Date:	**01 May 2025**
Number of pages:	**11**
Number of appendices:	**0**

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

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

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

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

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP SN300 Series - Secure Element SN300_SE B1.1 J9. The developer of the NXP SN300 Series - Secure Element SN300_SE B1.1 J9 is NXP Semiconductors Germany located in Hamburg, Germany 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 Security Integrated Circuit Platform for operating systems and applications with high security requirements. The SN300x Single Chip Secure Element and NFC Controller Series combines on a single die an Embedded Secure Element and a NFC Controller (the "x" in SN300x indicates the type of the SN300 series, representing for example the NFC Controller configuration). The two subsystems are called "SN300_SE" and "SN300_NFC". The NFC Controller is not part of the TOE. The Embedded Secure Element SN300_SE is based on a Flash-based secure microcontroller platform.

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 13 May 2022. This re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 1 May 2025 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are consisting of

- an update to CC:2022 and the resulting changes in the ST,

- modification of two sites

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the NXP SN300 Series - Secure Element SN300_SE B1.1 J9, 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 SN300 Series - Secure Element SN300_SE B1.1 J9 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report [EAR] [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM:2022 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

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

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the NXP SN300 Series - Secure Element SN300_SE B1.1 J9 from NXP Semiconductors Germany located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SN300_SE	B1.1
Software	FactoryOS	1.11.3
	BootOS (ROM)	1.11.1
	Flash Driver Software (FlashROM)	1.11.2

To ensure secure usage a set of guidance documents is provided, together with the NXP SN300 Series - Secure Element SN300_SE B1.1 J9. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the [ST], Chapter 1.3.3.

2.2 *Security Policy*

The TOE maintains:

- Memory encryption and masking mechanisms are implemented to preserve confidentiality of data
- The hardware embeds sensors, which ensure proper operating conditions of the device.
- Integrity protection of data and code involves error correction and error detection codes, light
- sensing and other security functionality.
- The IC hardware is shielded against physical attacks.
- The lockstep (redundant) CPU ensures protection against faults in the CPU.
- Hardware to serve with True Random Numbers

2.3 *Assumptions and Clarification of Scope*

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

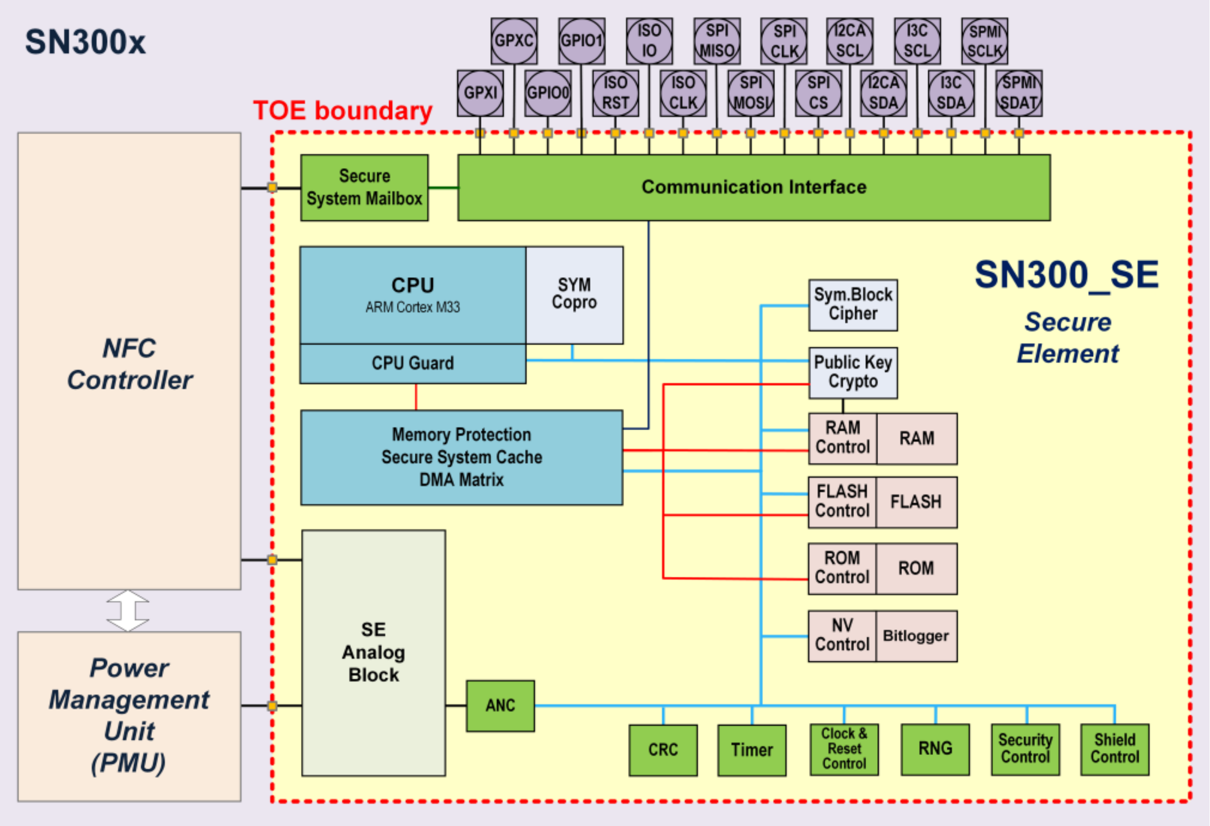
The SN300x chip combines on a single die an Embedded Secure Element and an NFC Controller. The two subsystems are called "SN300_SE" and "SN300_NFC". Both subsystems use a shared Power Management Unit ("SN300_PMU"). Only the “SN300_SE” is part of the TOE (see the figure in section 2.4).

Although the TOE has different dedicated cryptographic co-processors (e.g. PKC, AES, DES), the TOE has no security claims regarding cryptographic functionality.

Note that SN300x without any Security IC Embedded Software for the TOE is available for NXP internal use only

2.4 Architectural Information

The top level architecture and block diagram of the SN300_SE is depicted in the following figure.



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
SN300_SE Information on Guidance and Operation	Revision 1.6
SN300 family; Single Chip Secured (NFC) controller, Product data sheet.	Revision 1.E
SN300V TOE Identification, Data sheet addendum	Revision 1.3
SN300_SE Programmer's Manual, Application Note	Revision 0.22
Arm® Cortex®-M33 Processor, Technical Reference Manual	Revision r1p0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

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

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The independent vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities could 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 was performed on the TOE. During this attack-oriented analysis the protection of the TOE was analysed using the knowledge gained from all evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis used the attack methods in [JIL-AM] and [JIL-AAPS].
- All potential vulnerabilities were 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 were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The test effort in the baseline evaluation expended by the evaluators was 15 weeks. During that test campaign, 6% of the total time was spent on physical Attacks, 34% Perturbation attacks, 54% on side-channel testing, and 6% on logical tests.

The additional test effort in the first re-certification expended by the evaluators was 8 weeks. During that test campaign, 0% of the total time was spent on physical Attacks, 25% Perturbation attacks, 75% on side-channel testing, and 0% on logical tests.

The additional test effort in this re-certification expended by the evaluators was 7 weeks. During that test campaign, 0% of the total time was spent on physical Attacks, 29% Perturbation attacks, 71% on side-channel testing, and 0% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the [ST]. For some tests, testing was performed on an earlier revision of the TOE. The assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[EAR]*, 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.

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

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but 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 site certificates and their associated Site Technical Audit Reuse reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP SN300 Series - Secure Element SN300_SE B1.1 J9.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the [EAR], which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to [COMP] a derived document [ETRfC] was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the NXP SN300 Series - Secure Element SN300_SE B1.1 J9, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims ''strict' conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

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>.

3 Security Target

The "NXP SN300 Series - Secure Element" Security Target, Rev. 1.0.6, 19 February 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]*.

4 Definitions

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

IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
TOE	Target of Evaluation
TRNG	True Random Number Generator

5 Bibliography

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

[CC] Common Criteria for Information Technology Security Evaluation, Parts 1 to 5, CC:2022 Revision 1, November 2022

[CEM] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.6, April 2024

[EAR] Evaluator Assessment of Changes Report (EAR) NXP SN300 Series - Secure Element – Partial ETR, Version 4.0, 1 May 2025

[ETRfC] Evaluation Technical Report for Composition “NXP SN300 Series - Secure Element” – EAL4+, Version 3.0, 1 May 2025

[JIL-AAPS] Application of Attack Potential to Smartcards, Version 3.2.1, February 2024

[JIL-AMS] Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[PP] Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014

[ST] "NXP SN300 Series - Secure Element" Security Target, Rev. 1.0.6, 19 February 2025

[ST-lite] "NXP SN300 Series - Secure Element" Security Target Lite, Rev. 1.0.6, 19 February 2025

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)