Version 2023-11

Certification Report

NXP SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10

Sponsor and developer: ***NXP Semiconductors GmbH***
Beiersdorfstraße 12
22529 Hamburg
Germany

Evaluation facility: ***TÜV Informationstechnik GmbH***
Am TÜV 1
45307 Essen
Germany

Report number: **NSCIB-CC-2400072-01-CR**

Report version: **1**

Project number: NSCIB-**2400072-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **12 December 2024**

Number of pages: **11**

Number of appendices: **0**

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

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

CONTENTS

Foreword 3

Recognition of the Certificate 4

International recognition 4
European recognition 4

1 Executive Summary 5

2 Certification Results 6

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 7
2.3.1 Assumptions 7
2.3.2 Clarification of scope 7
2.4 Architectural Information 7
2.5 Documentation 8
2.6 IT Product Testing 8
2.6.1 Testing approach and depth 8
2.6.2 Independent penetration testing 8
2.6.3 Test configuration 8
2.6.4 Test results 8
2.7 Reused Evaluation Results 9
2.8 Evaluated Configuration 9
2.9 Evaluation Results 9
2.10 Comments/Recommendations 9

3 Security Target 10

4 Definitions 10

5 Bibliography 11

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

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.

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

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.

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10. The developer of the NXP SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10 is NXP Semiconductors GmbH 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 SN330 A0 Single Chip Secured (NFC) Controller Series 1 combines on a single die an Embedded Secure Element and a NFC Controller. The two subsystems are called "SN330_SE" and "SN330_NFC". The NFC Controller is not part of the TOE. The Embedded Secure Element SN330_SE is based on a Flash-based secure microcontroller platform. A high frequency clocked ARM Cortex M33 core along with state of the art cryptographic hardware coprocessors brings secured applications to a new level in performances and security. The TOE is integral part of the SN330 A0 IC.

The TOE has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 12 December 2024 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

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 SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10, 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 SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10 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 *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic flaw remediation) and ASE_TSS.2 (TOE summary specification with architectural design summary).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP SN330 A0 Series - Secure Element	SN330_SE A0.1.000 J10
Software	Test Software / FactoryOS	6.0.5
	Boot Software / Boot OS	6.0.6
	Flash Driver Software	6.0.3

To ensure secure usage a set of guidance documents is provided, together with the NXP SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10. 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 security functionality of the TOE is designed to act as an integral part of a security system composed of hardware and Security IC Embedded Software to strengthen it as a whole. Several security mechanisms of the TOE are completely implemented in and controlled by the SN330 A0 Secure Element. Other security mechanisms must be treated by Security IC Embedded Software. All security functionality is targeted for use in a potential insecure environment, in which the TOE maintains

- correct operation of the security functionality
- integrity and confidentiality of data and code stored to its memories and processed in the device

This is ensured by the construction of TOE and its security functionality.

The TOE provides a hardware platform for an implementation of a smartcard

application with:

- 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), 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

In addition, 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, EMFI detector, light sensing and other security functionality. Memory encryption and masking mechanisms are implemented to preserve confidentiality of data. The IC hardware is shielded against physical attacks. And the lockstep (redundant) CPU ensures protection against faults in the CPU.

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

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 4.2.1 of the *[ST]*.

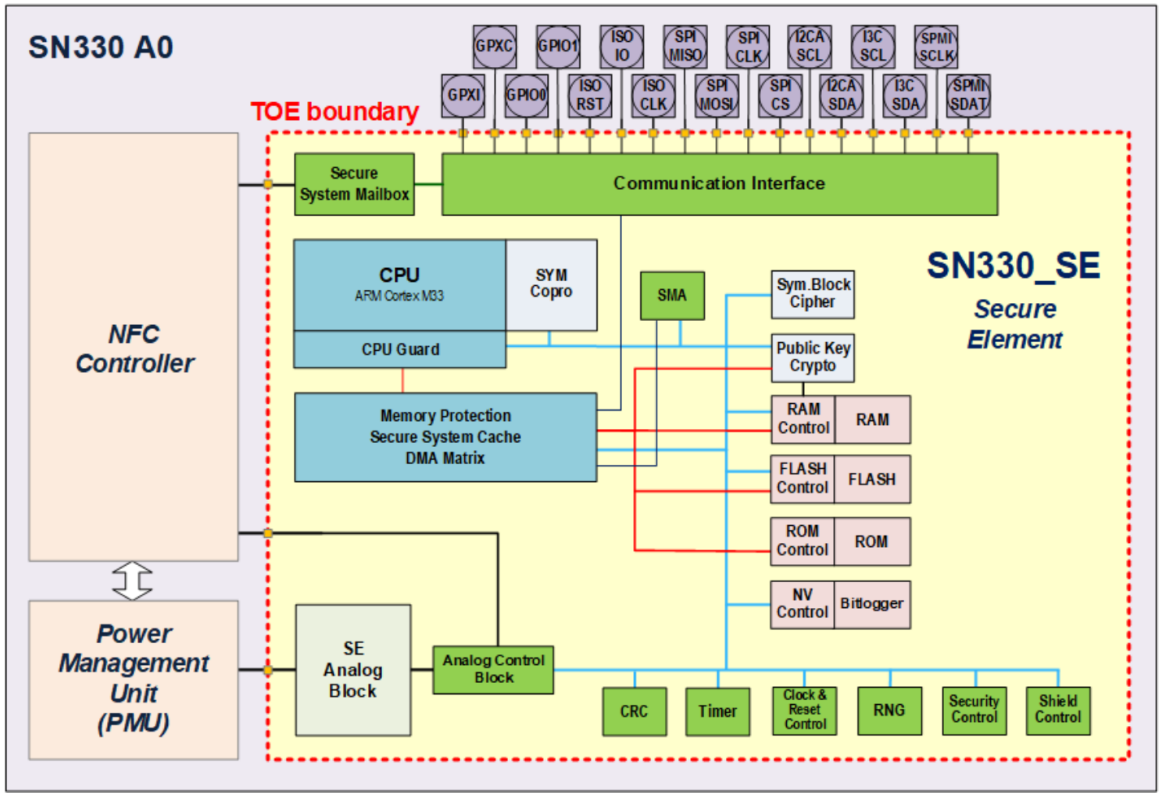
2.3.2 Clarification of scope

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

The secure operation of cryptographic functionality in section 2.2 requires a Cryptographic Library which is not part of this TOE. Therefore, Security Services and Security Features using this cryptographic functionality need to be evaluated in the composite product together with Cryptographic Library as part of the Security IC Embedded Software. As a consequence, for the cryptographic functionality the scope of this evaluation is confined to protection against physical manipulation.

2.4 Architectural Information

The TOE architecture can be depicted as follows:



The TOE incorporates an high frequency clocked ARM Cortex M33 processor augmented with its dedicated coprocessor (SYM-lite), a secure copy machine (SMA), and a Public-Key Cryptography (PKC) coprocessor, which are all connected to a bus system. This bus system gives access to memories, hardware peripherals and communication interfaces. The PKC coprocessor provides large integer arithmetic operations, which can be used by Security IC Embedded Software for asymmetric-key cryptography. Hardware peripherals include coprocessors for symmetric-key cryptography and for calculation of error-detecting codes, and also a random number generator. On-chip memories are Flash memory, ROM and RAMs. The Flash memory can be used to store data and code of Security IC Embedded Software. It is designed for reliable non-volatile storage.

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

2.5 Documentation

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

Identifier	Version
SN330_SE A0 Information on Guidance and Operation, Dated 09 February 2024	0.1
SN330U; Single Chip Secured (NFC) controller, Product data sheet, Dated 22 November 2024	1.2
SN330 TOE Identification (for A0), Data sheet addendum, Dated 06 May 2024	1.0
SN330_SE Programmer's Manual, Application Note, Dated 26 February 2024	1.0
ARM® Cortex®-M33 Processor Technical Reference Material	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 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 was conducted along the following steps:

- Systematic search for potential vulnerabilities and known attacks in public domain sources, use of a list of vulnerabilities, and from a methodical analysis of the evaluation documents.
- Analysis why these vulnerabilities are unexploitable in the intended environment of the TOE.
- If the rationale is suspect in the opinion of the evaluator penetration tests are devised.
- Even if the rational is convincing in the opinion of the evaluator, penetration tests are devised for some vulnerabilities, especially to support the argument of non- practicability of exploiting time in case of SPA, DPA and FI attacks.

The total test effort expended by the evaluators was 61 days. During that test campaign, 85% of the total time was spent on Perturbation attacks, and 15% on side-channel testing.

2.6.3 Test configuration

The following configuration was used for testing:

- NXP SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10

2.6.4 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.

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

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

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 25 site certificates.

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 SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, 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 SN330 A0 Series - Secure Element SN330_SE A0.1.000 J10, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2**. 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_0084]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" 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.

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

3 Security Target

The NXP SN330 A0 Series - Secure Element Security Target, Rev 1.2, Dated 27 November 2024 *[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:

AES	Advanced Encryption Standard
BAC	Basic Access Control
CA	Chip Authentication
CAM	Chip Authentication Mapping
CBC	Cipher Block Chaining (a block cipher mode of operation)
CFB	Cipher Feedback
CGM	Galois/Counter Mode
CRC	Cyclic Redundancy Checks
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
OFB	Output Feedback
PP	Protection Profile
TOE	Target of Evaluation
TRNG	True Random Number Generator

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

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 I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report Summary (ETR Summary), 8122598088 / NSCIB-CC-2400072-01, Version 2, Dated 29 November 2024
[ETRfC]	ETR for Composite Evaluation (ETR COMP), 8122598088 / NSCIB-2400072-01, Version 2, Dated 29 November 2024
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP_0084]	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 SN330 A0 Series - Secure Element Security Target, Rev 1.2, Dated 27 November 2024
[ST-lite]	NXP SN330 A0 Series - Secure Element Security Target Lite, Rev 1.2, Dated 27 November 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)

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