Certification Report

NXP SE310 Series - Secure Element version SE310_SE A0.1.000 J2

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

Evaluation facility:

TÜV Informationstechnik GmbH
Am TÜV 1
45307 Essen
Germany

Report number:	**NSCIB-CC-2200031-01-CR**
Report version:	**2**
Project number:	NSCIB-**2200031-01**
Author(s):	**Wim Ton**
Date:	**28 November 2023**
Number of pages:	**12**
Number of appendices:	**0**

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.

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 SE310 Series - Secure Element version SE310_SE A0.1.000 J2. The developer of the NXP SE310 Series - Secure Element version SE310_SE A0.1.000 J2 is NXP Semiconductors Germany 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 TOE incorporates a high frequency clocked ARM Cortex M33 processor augmented with its dedicated coprocessor for symmetric cryptography (SYM-lite), a secure copy machine (SMA), a Public-Key Cryptography (PKC) coprocessor, and a random number generator.

On-chip memories are Flash memory, ROM and RAMs. The ROM contains the IC dedicated software for factory testing, program upload, and the flash memory drivers.

In addition, the hardware embeds sensors which ensure the 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 the confidentiality of the stored data. The IC hardware is shielded against physical attacks. And the “lockstep” (redundant) CPU provides protection against faults in the CPU.The TOE has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 27-5-2023 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 SE310 Series - Secure Element version SE310_SE A0.1.000 J2, 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 SE310 Series - Secure Element version SE310_SE A0.1.000 J2 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) , ALC_FLR.1 (Basic flaw remediation), ASE_TSS.2 (TOE summary specification with architectural design summary), and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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.

Version 2: NSCIB-CC-2200031-01-CR version 2 was issued on 28 November 2023 to correct an error in the TOE name.

[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 SE310 Series - Secure Element version SE310_SE A0.1.000 J2 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP SN310 Series - Secure Element	A0.1.000 J2
IC dedicated software in ROM	FactoryOS	3.4.4
	BootOS	3.4.2
	Flash Driver Software	3.4.5

To ensure secure usage a set of guidance documents is provided, together with the NXP SE310 Series - Secure Element version SE310_SE A0.1.000 J2. 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:

- the integrity and confidentiality of code and data stored in its memories;
- the different CPU modes with the related capabilities for configuration and memory access;
- the integrity, the correct operation and the confidentiality of security functionality provided by the TOE.

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

The TOE provides a hardware platform for an implementation of a smartcard application with:

- hardware to perform computations on multi-precision integers, which are suitable for public-key cryptography
- hardware to provide True Random Numbers
- memory management control;
- an ISO/IEC 7816 contact interface with UART.
- Serial Peripheral Interface (SPI)
- 2x I^2C interfaces
- I^3C interface (shared pins with second I^2C interface)
- SPMI Interface
- GPIO interface by use of Special Function Registers

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 secure operation of cryptographic functionality in 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

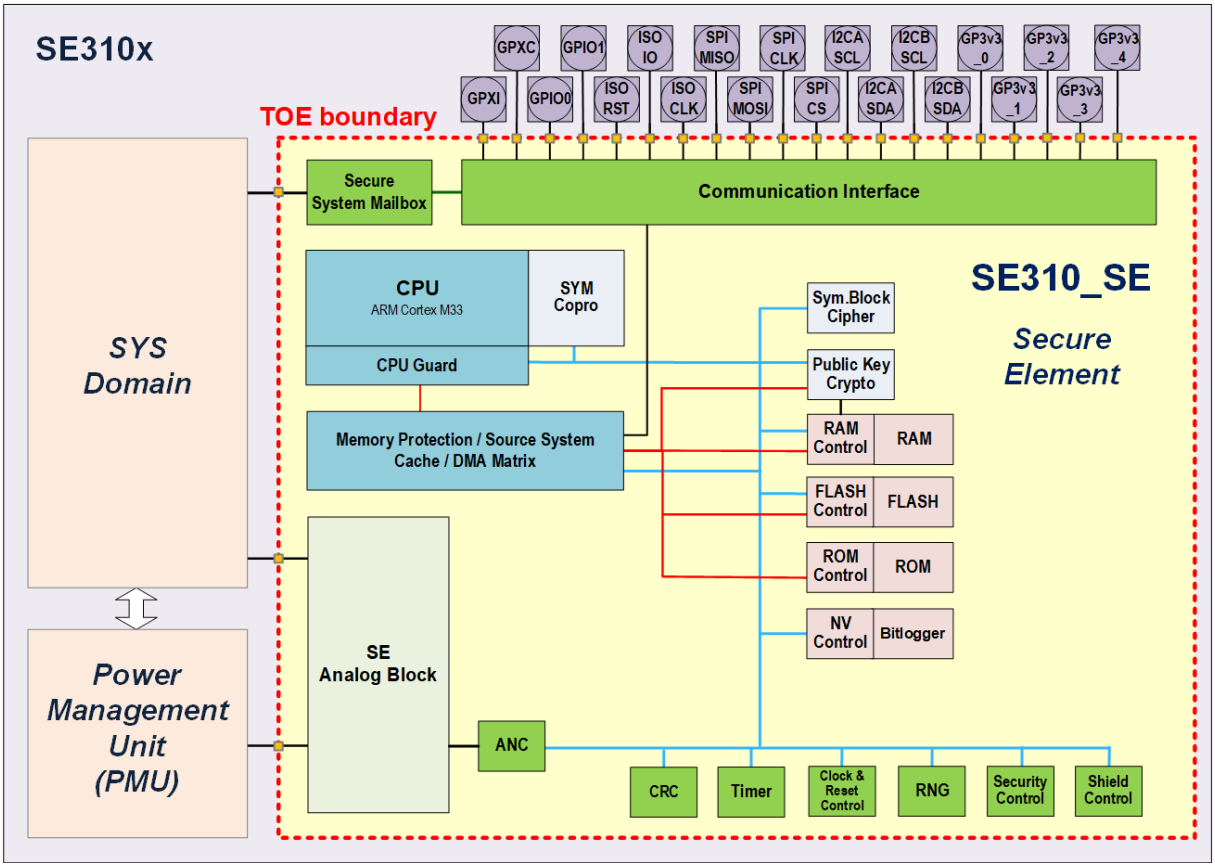

Figure 1 TOE Architecture

The TOE contains two separate busses. One peripheral control bus is provided for I/O communication. The secure peripheral bus serves protected internal communication.

The TOE implements a complex security functionality to protect code and data during processing and while stored to the device. This includes appropriate memory encryptions and masking schemes to preserve confidentiality.

Error detection codes (the Flash Secure Fetch Plus) are used to protect the integrity and manifold light sensing with EMFI detector are integrated to detect perturbations which could lead to integrity violation.

The “CPU Guard” detects errors in the program execution, and the memory protection separates the memory spaces of the various applications.

Active shielding is present and the operating conditions are monitored by sensors for the temperature, power supplies and frequencies.

2.5 Documentation

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

Identifier	Version
SN310_SE B2 Information on Guidance and Operation	0.1
SE310S Embedded Secure Element, Product data sheet	3.1
SE310 TOE Identification (for A0), Data sheet addendum,	1.0
SN310_SE Programmer's Manual, Application Note	0.1
ARM® Cortex®-M33 Processor Technical Reference Material	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 developers' testing effort can be summarised in the following aspects.

TOE test configuration:

Functional tests have been performed by the evaluator on the TOE as part of the penetration testing. Additionally, developer tests performed on emulators and simulators have been reviewed.

Developer's testing approach:

All TSFs and related security mechanisms, subsystems and modules are tested in order to assure complete coverage of all SFRs.

Different classes of tests are performed to test the TOE in a sufficient manner.

- Verification Testing during Development:
- Simulation tests (tool based and on FPGA),
- Validation of key parameters before tape-out.
- Evaluation and Characterization Testing on Silicon:
- Evaluation Testing to confirm results from Verification Testing (see above),
- Characterization testing over process, voltage and temperature (PVT) after Evaluation Testing.
- Characterization Testing during production under PVT conditions.
- Production Testing of each produced sample.

The developer testing reaches a code coverage of over 98% on the flash software. Boot OS and factory OS have a code coverage of 90-94%. A rationale has been given for the missing coverage.

2.6.2 Independent penetration testing

The vulnerability analysis used know public vulnerabilities, [JIL-AM], and the findings from ADV_IMP.

The following TOE security functionalities were tested:

- SS.RNG: Random number generation,
- SF.OPC: Control of operational conditions,
- SF.PHY: Protection against physical manipulation,
- SF.LOG: Logical protection, and
- SF.FOS-USE: FactoryOS protection.

With perturbation using light and EMFI.

Information leakage was measured from power consumption and EM radiation.

The total test effort expended by the evaluators was 51 days. During that test campaign, 82% of the total time was spent on Perturbation attacks, and 18% on side-channel testing..

2.6.3 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

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 28 site certificates and/or Site Technical Audit Reports.

One site certificate was 3 weeks out of date at the time of certification. A new audit for this site has been conducted already.

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 SE310 Series - Secure Element version SE310_SE A0.1.000 J2. The [SE310 TOE Identification (for A0), Data sheet addendum] and the [SE310S Embedded Secure Element, Product data sheet] provide detailed information on how the user can identify the TOE version.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2]. 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 SE310 Series - Secure Element version SE310_SE A0.1.000 J2, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 , ALC_FLR.1, ASE_TSS.2, and AVA_VAN.5**.

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

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

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.

---

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The NXP SE310 Series - Secure Element, Security Target, Revision 0.1.1, 22 May 2023. *[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:

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
TOE	Target of Evaluation
AES	Advanced Encryption Standard
BBI	Body Bias Injection
CGA	Certificate Generation Application
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EM	Electromagnetic
EMA	Electromagnetic Analysis
EMFI	Electromagnetic Fault Injection
IC	Integrated Circuit
JIL	Joint Interpretation Library
LFI	Laser Fault Injection
MAC	Message Authentication Code
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SCA	Side Channel Analysis.
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm

TRNG	True Random Number Generator
VFI	Voltage Fault Injection

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
[ETR]	EVALUATION TECHNICAL REPORT SUMMARY, 2200031-01_ETR_230525_v3, 3.0, 25-May-2023
[ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION, 2200031-01_ETR-COMP_230525_v3, 3.0, 25-May-2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AM]	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]	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 SE310 Series - Secure Element, Security Target, Revision 0.1.1, 22 May 2023.
[ST-lite]	NXP SE310 Series – Secure Element, Security Target Lite, Rev. 0.1.1 — 22 May 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)