

EUCC Certification Report

NXP SE310 Series - Secure Element, version SE310_SE A0.1000 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: **EUCC-3110-2026-2600001-01 Certification Report**

Report version: **1**

Project number: **EUCC-2600001-01**

Author(s): **Certifier Wim Ton, TrustCB B.V.**
contact: eucc@trustcb.com

Date: **21 September 2026**

Number of pages: **18**

Number of appendices: **0**

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

CONTENTS

Foreword	3
International recognition of the certificate	4
1 Executive Summary	5
2 ICT Product details	7
2.1 Identification of the ICT Product	7
2.2 Contact information related to the evaluation of the ICT Product	7
2.3 Security services and policies	7
2.3.1 Security services	7
2.3.2 Vulnerability management	8
2.3.3 Assurance Continuity policies	8
2.3.4 Lifecycle management processes and production facilities	8
2.3.5 Patch management process	8
2.4 Assumptions and Clarification of Scope	8
2.4.1 Assumptions	8
2.4.2 Clarification of scope	8
2.5 Architectural Information	9
2.6 Supplementary Cybersecurity Information	9
3 Evaluation summary	11
3.1 Identification of used assurance components	11
3.2 EUCC State of the Art documents and Protection Profiles	11
3.3 ICT Product testing	11
3.3.1 Testing approach and depth	11
3.3.2 Independent penetration testing	11
3.3.3 Test configuration	12
3.3.4 Test results	12
3.4 ICT Product evaluation	12
3.4.1 Reused evaluation results	12
3.4.2 Evaluated configuration	12
3.4.3 Assessment against each assurance requirement	12
3.5 Results of the evaluation	14
3.6 Certificate information and scheme label	15
3.7 Comments and Recommendations	15
4 Security Target	16
5 Glossary	16
6 Bibliography	17

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

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

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

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

International recognition of the certificate

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

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is NXP Semiconductors Germany GmbH located in Hamburg, Germany and they also act as the sponsor of the evaluation.

This Certification Report is intended to assist prospective consumers when judging the suitability of the ICT security properties of the ICT product for their particular requirements. This ICT Product is only sold to consumers in combination with separately certified software (JCOP, OS, etc.).

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 claims conformance to the following Protection Profiles [PP]:

- Security IC Platform Protection Profile including Functional Packages, version 2.0, 16 December 2025, registered under the reference BSI-CC-PP-0084-V2-2026

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate. The certificate identifier is **EUCC-3110-2026-2600001-01**, dated 21-09-2026 and with a 5-year validity.

The evaluation of the TOE was performed by TÜV Informationstechnik GmbH located in Essen. The evaluation was completed on 21-09-2026 with the issuance of the evaluation technical report [ETR]. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 [CEM] for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 [CC] (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report [ETR]¹ for this product provide sufficient evidence that the TOE meets the EAL5: augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) ALC_FLR.2 "Flaw Reporting Procedures", ASE_TSS.2 (TOE summary specification with architectural design summary), and AVA_VAN.5 (Advanced methodical vulnerability analysis). It also includes the assurance Composite product package as defined in [CC](Part 5).

This assurance level is recognised by article 52 of [CSA] as 'high'.

Consumers of this ICT Product are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

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

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

Note that the certification results apply only to the specific version of the product as evaluated.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product NXP SE310 Series - Secure Element, version SE310_SE A0.1000 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	SE310_SE	A0.1.000
Software	FactoryOS	3.4.4
	BootOS (ROM)	3.4.2
	Flash Driver Software	3.4.5

Additional requirements for the operational environment of the certified ICT product are described in section 1.3.4 of the [ST].

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, "Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

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

Developer of the certified ICT Product

ICT product developer	NXP Semiconductors Germany GmbH
-----------------------	---------------------------------

Identification of CAB

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

TrustCB point of contact: EUCC@trustcb.com

Identification of ITSEF

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

TÜV Informationstechnik GmbH located in Essen

2.3 Security services and policies

2.3.1 Security services

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;

- side channel protected CPU instructions for data manipulation
- 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 calculate the Advanced Encryption Standard (AES) with different key lengths and different modes.
- hardware to provide True Random Numbers
- memory management control;
- an ISO/IEC 7816 contact interface with UART.
- Serial Peripheral Interface (SPI)
- 2x I²C interfaces
- GPIO interface by use of Special Function Registers

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2

Document reference: <https://www.nxp.com/support/support/product-security-vulnerability:PSIRT>

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

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

2.3.5 Patch management process

Not applicable to this evaluation

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

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

2.4.2 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 2.3 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.

2.5 Architectural Information

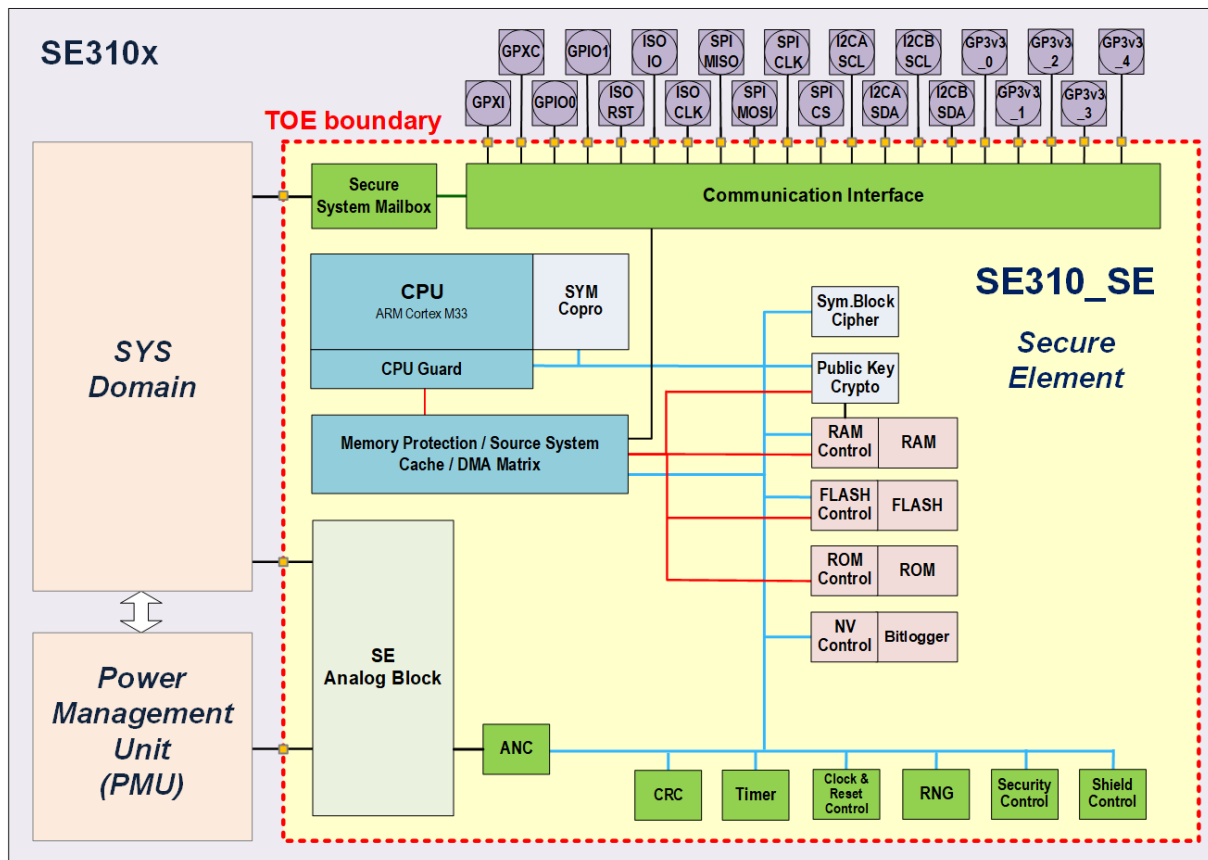


Figure 1 TOE Architecture

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.

2.6 Supplementary Cybersecurity Information

The following website link was provided for the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

<https://www.nxp.com/products/nxp-product-information/eucc-certified-products:EUCC-CERTIFIED#cybersupport>

This link provides further details and links on:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2.

- The period during which the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates, is stated as 5 years aligned with the validity of the issued EUCC certificate.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2.
- The online ENISA repository listing publicly disclosed vulnerabilities related to the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2 and to any relevant cybersecurity advisories.

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to assist users with the secure configuration of the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2:

Identifier	Version
SE310_SE Information on Guidance and Operation	0.3
SE310S Embedded Secure Element, Product data sheet	3.1
SE310 TOE Identification (for A0), Data sheet addendum	1.0
SE310_SE Programmer's Manual, Application Note	0.1
ARM® Cortex®-M33 Processor Technical Reference Material	r1p0

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 5 augmented with ALC_DVS.2, ASE_TSS.2, ALC_FLR.2 and AVA_VAN.5**

as defined by, and detailed in, [CC] and [CEM].

3.2 EUCC State of the Art documents and Protection Profiles

EUCC state-of-the-art documents [SotA Documents] were applied as referenced in the Bibliography.

The following Protection Profile was applied:

Security IC Platform Protection Profile with Augmentation Packages, Version 2.0, 16 December 2025, registered under the reference BSI-CC-PP-0084-V2-2026

3.3 ICT Product testing

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

3.3.1 Testing approach and depth

The 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.

3.3.2 Independent penetration testing

The vulnerability analysis used known public vulnerabilities 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 for the first evaluation was 45 days. During that test campaign, 80% of the total time was spent on Perturbation attacks, and 20% on side-channel testing.

For this evaluation, the test effort was 25 day. During this test campaign, 58% of the total time was spent on Perturbation attacks using light, and 42% on overcoming sensors and filters.

3.3.3 Test configuration

The evaluator testing and penetration testing was performed on the TOE with a special version of the JCOP runtime.

The TOE was tested in the following configurations:

- FPGA Emulator
- TOE ("Wafer Level Chip Scale Package" (WLCSP) and with an exposed backside)
- Using T=0, T=1 (ISO/IEC 7816)

3.3.4 Test results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

This was a new certification under EUCC.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 24 Site Technical Audit Reports.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number NXP SE310 Series - Secure Element, version SE310_SE A0.1000 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.

3.4.3 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.2

The TOE introduction, conformance claim, security problems, security objectives, extended components, security requirements and TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2. No issues or deviations were identified.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.5
Implementation representation	ADV_IMP.1
Well-structured internals	ADV_INT.2
TOE design	ADV_TDS.4

The evaluation has demonstrated that the developer's evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. The subsystem/module level model is sensible, useful, and shows TSFIs and subsystem/module decomposition. The security architecture is thoroughly explained, design compliance rationale is complete and coherent, and necessary evidence is extracted per alternative approach. The evaluator confirmed why the TSF is well-structured. SFRs were inspected, with findings mapped to the implementation representation in both evaluation meetings. Accordingly, the ADV activities meet the assurance requirements for EAL5, with no issues or deviations identified.

AGD

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

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements for EAL5, with no issues or deviations identified.

ALC

ALC	
CM capabilities	ALC_CMC.4
CM Scope	ALC_CMS.5
Delivery	ALC_DEL.1
Development security	ALC_DVS.2
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2
Tools and techniques	ALC_TAT.2

The evaluation has demonstrated that the developer's evidence meets ALC specified. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in accordance with the CM plan to maintain all configuration items by automated means. Delivery procedures were well-documented, ensuring security during TOE distribution. Security measures for protecting the confidentiality and integrity of the TOE in physical, procedural, personnel, logical and other areas were

justified as sufficient. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. The development life-cycle model provided necessary control; tools were well-defined with clear documentation and implementation standards have been applied by the developer. Accordingly, the ALC activities satisfy the assurance requirements for EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2, with no issues or deviations identified.

ATE

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.3
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2

The evaluation has demonstrated that the developer's evidence for ATE requirements meets all specified requirements. The testing approach used by the developer effectively covered the TSFIs and modules. The developer's rationale for testing all TSFIs and modules was presented and verified. The developer test results show that for all tests either the result was pass or a proper rationale was given why the test failed. For the evaluator's independent testing, the overall approach for test selection, goals for the witnessing session, and independent test plan were clearly outlined. The evaluator's testing results showed that all sampled tests were passed. Accordingly, the ATE activities satisfy the assurance requirements for EAL5 with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.5

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can 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 is performed on the TOE. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis it was performed according to the [SotA_AAPS].
- The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE type. No potential vulnerabilities were identified.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes, information from the public domain and information from previous evaluations of the TOE. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

Consequently, the AVA activities were performed in full compliance with the assurance requirements EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ALC_FLR.2 and ASE_TSS.2, providing a high level of confidence in the TOE's resistance to exploitation.

3.5 Results of the evaluation

The evaluation lab documented their evaluation results in the [ETR], which references an ASE Intermediate Report, other evaluator documents and developer documentation [DEV_DOCS] and Site Technical Audit Report(s) for the referenced site(s).

To support composite evaluations according to [COMP] a derived document [ETRFc] was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

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

Based on the evaluation results the evaluation lab concluded the NXP SE310 Series - Secure Element, version SE310_SE A0.1000 J2, to be **CC:2022 R1 1 Part 2 extended, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as 'High' with **AVA_VAN.5** and to meet the requirements of **EAL 5 augmented with ALC_DVS.2, ALC_FLR.2, ASE_TSS.2, and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target [ST].

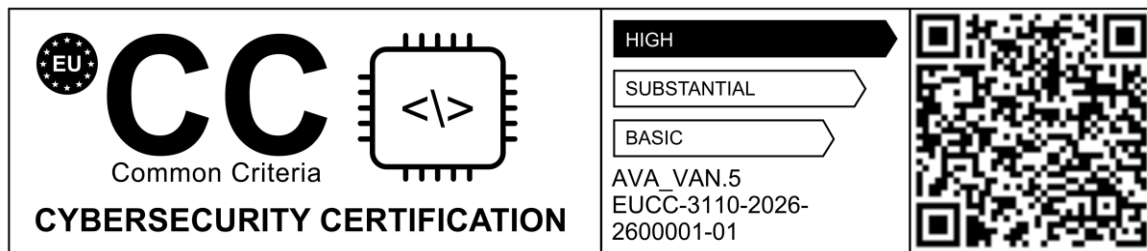
The Security Target claims 'strict' conformance to the Protection Profile [PP].

3.6 Certificate information and scheme label

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

Unique identifier: EUCC-3110-2026-2600001-01

Date of issuance: 21-09-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

4 Security Target

The certification references the following security target:

NXP SE310 Series - Secure Element Security Target, Rev 3.4, 18 September 2026 [ST].

Please note that, to satisfy the need for publication, a public version [ST-lite] has been created and verified according to [ST-SAN].

5 Glossary

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

IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report
ACL	Access Control List
AES	Advanced Encryption Standard
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
EMA	Electromagnetic Analysis
IC	Integrated Circuit
JIL	Joint Interpretation Library
MAC	Message Authentication Code
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
SM	Secure Messaging
SPA/DPA	Simple/Differential Power Analysis
TRNG	True Random Number Generator

6 Bibliography

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

[CC]	Common Criteria for Information Technology Security Evaluation, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[CC2022_TP]	Transition Policy to CC:2022 and CEM:2022
[DEV_DOCS]	SE310_SE Information on Guidance and Operation, Version 0.3 SE310S Embedded Secure Element, Product data sheet, Version 3.1 SE310 TOE Identification (for A0), Data sheet addendum, Version 1.0 SE310_SE Programmer's Manual, Application Note, Version 0.1 ARM® Cortex®-M33 Processor Technical Reference Material Version, r1p0
[ETR]	Evaluation Technical Report Summary (ETR Summary), Version 3, 21 September 2026
[ETRFC]	Evaluation Technical Report for Composite Evaluation (ETR COMP), Version 3, 21 September 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[PP_0084]	Security IC Platform Protection Profile including Functional Packages, version 2.0, 16 December 2025, registered under the reference BSI-CC-PP-0084-V2-2026
[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA_CC_IC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Common Criteria to integrated circuits Version 2.0, December 2024
[SotA_COSP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT CERTIFICATION OF "OPEN" SMART CARD PRODUCTS VERSION 1.1, October 2023.
[SotA_SARC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, version 1.1, October 2023

[ST]	NXP SE310 Series - Secure Element Security Target, Rev 3.4, 18 September 2026
[ST-lite]	NXP SE310 Series - Secure Element Security Target Lite, Rev 3.4, 18 September 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2 ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)