TrustCB B.V.

Certification Report

SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58

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-2400058-02**
Report version:	**1**
Project number:	NSCIB-**2400058-02**
Author(s):	**Alireza Rohani, Haico Haak**
Date:	**10 February 2025**
Number of pages:	**16**
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 SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58. The developer of the SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58 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 SN100x Single Chip Secure Element and NFC controller Series combines on a single die an Embedded Secure Element, an NFC Controller, and the Power Management Unit. The three subsystems are called "SN100_SE", "SN100_PMU", and "SN100_NFC". The TOE is the SN100_SE. The NFC Controller and the PMU are not part of the TOE

The TOE is the SN100_SE B2.1 in three configurations SN100_SE B2.1 C25, SN100_SE B2.1 C48 and SN100_SE B2.1 C58. The TOE will be provided with Crypto Library and Services Software as part of the IC Dedicated Software

The TOE is a Security Integrated Circuit Platform for various operating systems and applications with high security requirements

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 05 July 2024. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 10 February 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 second issue of the Certification Report is a result of a "recertification with major changes".

There are no changes on the TOE, its parts or its environment from this last recertification. Only the evaluation methodology changed from CC v3.1R5 to CC:2022

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made.

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

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58, 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 SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58 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 following multi assurance package:

Global conformance EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ALC_FLR.1, ATE_COV.3, ATE_FUN.2, AVA_VAN.5, and ASE_TSS.2.

The MPU/MMU memory management sub-TSF meets EAL6 augmented with ALC_FLR.1 and ASE_TSS.2.

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]*.

---

[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 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58 from NXP Semiconductors Germany located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SN100x	B2.1
Software	Factory OS	4.2.0
	Boot OS	4.2.0
	Flash Driver Software	4.0.8

Table 1 Components common for all SN100_SE B2.1

Delivery item type	Identifier	Version
Configuration Data	Factory Page	18218
	System Page Common	18468
	BootOS Patch	4.2.0 PL3 v4
Security Software	Services Software	4.13.3.0
	Crypto Library	1.0.0

Table 2 Components of SN100_SE B2.1 specific for C25

Delivery item type	Identifier	Version
Configuration Data	Factory Page	18652
	System Page Common	18468
	BootOS Patch	4.2.0 PL5 v16
Security Software	Services Software	4.13.7.1
	Crypto Library	1.0.0

Table 3 Components of SN100_SE B2.1 specific for C48

Delivery item type	Identifier	Version
Configuration Data	Factory Page	18218
	System Page Common	18468
	BootOS Patch	4.2.0 PL5 v16
Security	Services Software	4.14.0.1

Software	Crypto Library	2.0.0

Table 4 Components of SN100_SE B2.1 specific for 58

To ensure secure usage a set of guidance documents is provided, together with the SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58. 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 SN100_SE is designed to act as an integral part of a security system composed of SN100_SE and Security IC Embedded Software to strengthen it as a whole. Several security mechanisms of SN100_SE are completely implemented in and controlled by SN100_SE. 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 SN100_SE maintains:

- correct operation of the security functionality
- integrity and confidentiality of data and code stored to its memories and processed in the device
- controlled access to memories and hardware components supporting separation of different applications

This is ensured by the construction of SN100_SE and its security functionality. SN100_SE basically provides:

- 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 and Galois Message Authentication Code (GMAC) for symmetric-key cryptographic block ciphers
- hardware to calculate Cyclic Redundancy Checks (CRC)
- hardware to serve with True Random Numbers
- hardware and service software to control access to memories and hardware components

In addition, SN100_SE 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. Encryption and masking mechanisms are implemented to preserve confidentiality of data and code. The IC hardware is shielded against physical attacks.

The Crypto Library consists of several binary packages that are pre-loaded to the Flash memory of the TOE for usage by the Security IC Embedded Software. The Crypto Library provides:

- AES
- Triple-DES (3DES)
- RSA
- RSA key generation
- RSA public key computation
- ECDSA (ECC over GF(p)) signature generation and verification
- ECDSA (ECC over GF(p)) key generation
- ECDH (ECC Diffie-Hellmann) key exchange
- MontDH (Diffie Hellman key exchange on Montgomery Curves over GF(p)) key generation
- MontDH (Diffie Hellman key exchange on Montgomery Curves over GF(p)) key exchange
- EdDSA (Edwards-curve Digital Signature Algorithm) signature generation and verification
- EdDSA (Edwards-curve Digital Signature Algorithm) key generation
- ECDAA related functions
- Full point addition (ECC over GF(p))

- Standard security level SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512 algorithms
- High security level SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512 algorithms
- HMAC algorithms
- eUICC authentication functions (MILENAGE, TUAK and CAVE)

In addition, the Crypto Library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the TOE. The Crypto Library also provides a secure copy routine, a secure memory compare routine, cyclic redundancy check (CRC) routines, and includes internal security measures for residual information protection.

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 and 4.3 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

2.4   Architectural Information

The SN100x Single Chip Secure Element and NFC controller Series combines on a single die an Embedded Secure Element, an NFC Controller, and the Power Management Unit. The three subsystems are called "SN100_SE", "SN100_PMU", and "SN100_NFC". The TOE is the SN100_SE. The NFC Controller and the PMU are not part of the TOE.

The TOE is the SN100_SE B2.1 in three configurations SN100_SE B2.2 C25/C48/C58. The TOE will be provided with Crypto Library and Services Software as part of the IC Dedicated Software.

A block diagram is given in Figure 1 below.

IC Hardware

The hardware part of the SN100_SE incorporates a high frequency clocked ARM SC300 processor, a Public-Key Cryptography (PKC) coprocessor and a Direct Memory Access (DMA) controller, which are all connected over a Memory Management Unit (MMU) to a bus system. This bus system gives access to memories, hardware peripherals and communication interfaces.

The ARM SC300 processor is a security enhanced variant of the ARM Cortex M3. It includes the SC300 core and the Nested Vector Interrupt Controller (NVIC). The core implements the ARMv7-M architecture, which supports a subset of the Thumb instruction set. 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. The DMA controller manages data transfers over communication interfaces like ISO/IEC 7816 compliant interface, Serial Peripheral Interface (SPI), I2C interface and the Secure Mailbox Interface. 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.

SN100_SE is offered with the NXP Trust Provisioning Service, which involves secure reception, generation, treatment and insertion of customer data and code at NXP. The documentation of SN100_SE includes a product data sheet, several product data sheet addenda, a user guidance and operation manual, and service documentation. This documentation describes secure configuration and secure use of SN100_SE as well as the services provided with it.

Also, the IC Dedicated Support Software is considered part of the IC Hardware, as it is stored to the ROM of the TOE. It consists of the Factory OS, the Boot OS and the Flash Driver Software.

Security Software

The IC Dedicated Software provides Security Software that can be used by the Security IC Embedded Software. The Security Software is composed of Services Software and Crypto Library.

The Services Software consists of Flash Services Software, Services Framework Software and the part of the Services HAL (Hardware Abstraction Layer) that is not stored to ROM. The Flash Services Software manages technical demands of the Flash memory and serves the Security IC Embedded Software with an interface for Flash erase and/or programming. The Services Framework Software represents a collection of different abstractions and utility functions that provide a runtime environment to the individual Services. The Services HAL provides an interface for the Services Software to the hardware that controls the Flash memory.

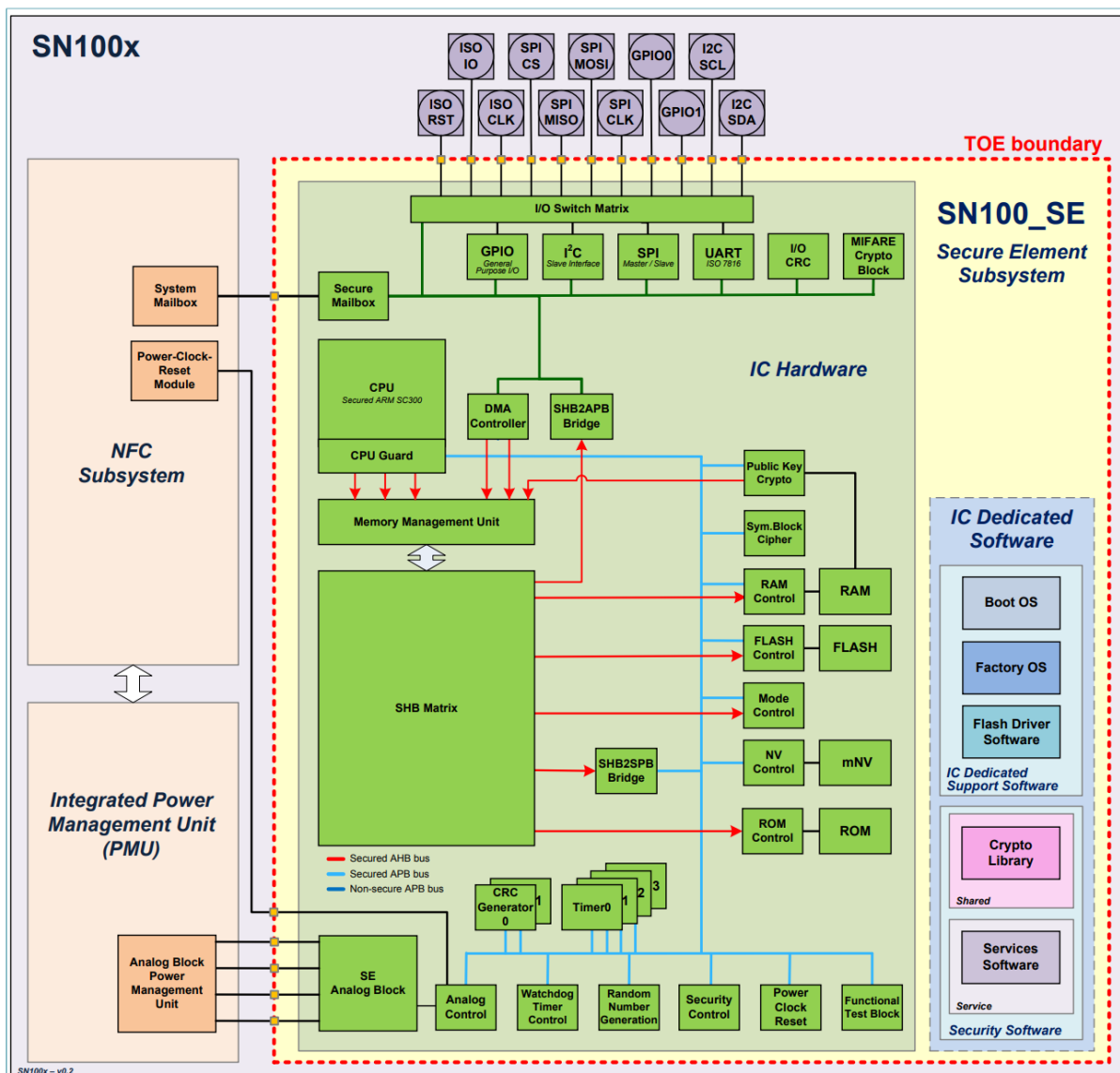The Services Software is considered part of the Service Code and is stored in the Flash memory of the TOE.

Figure 1 Logical architecture of the TOE

2.5   Documentation

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

Identifier	Version
SN100x_SE High-performance secure element subsystem, Product data sheet	1.0
SN100x_SE - SFR Tables for Berlin core	0.5
SN100x Wafer and Delivery Specification, Product data sheet addendum	1.2
P73 family SC300 User Manual, Product Data sheet addendum	1.0
P73 family DMA Controller PL080 User manual, Product data sheet addendum	1.0
P73 Family Chip Health Mode, Application note	1.0
P73 Family Code Signature Watchdog, Application note	1.1
ARM®v7-M Architecture Reference Manual	DDI 0403E.b (ID120114)

Table 5 Manuals common for all SN100_SE B2.1

Identifier	Version
SN100_SE Information on Guidance and Operation	1.4
SN100 Services User Manual – API and Operational Guidance	4.12
SN100 Services Addendum - Additional API and Operational Guidance	0.4
SN100x Crypto Library Information on Guidance and Operation	1.10
SN100x Crypto Library: Errata sheet	1.0
SN100x Crypto Library: User Manual – RNG Library	1.4
SN100x Crypto Library: User Manual – SHA Library	0.3
SN100x Crypto Library: User Manual – Secure SHA Library	0.4
SN100x Crypto Library: User Manual – SHA-3 Library	0.2
SN100x Crypto Library: User Manual – Secure SHA-3 Library	0.2
SN100x Crypto Library: User Manual – HMAC Library	0.4
SN100x Crypto Library: User Manual – Rsa Library (Rsa)	1.3
SN100x Crypto Library: User Manual – RSA Key Generation Library (RsaKg)	0.7
SN100x Crypto Library: User Manual – ECC over GF(p) Library	1.4
SN100x Crypto Library: User Manual – ECDAA	1.0
SN100x Crypto Library: User Manual – TwdEdMontGfp Library	1.2
SN100x Crypto Library: User Manual – eUICC Library	0.5
SN100x Crypto Library: User Manual – Symmetric Cipher Library (SymCfg)	0.5
SN100x Crypto Library: User Manual – Utils Library	0.4
SN100x Crypto Library: User Manual – HASH Library	0.3

Table 6 Manuals SN100_SE B2.1 C25 & C48

Identifier	Version
SN100_SE Information on Guidance and Operation	1.4

SN100 Services User Manual – API and Operational Guidance	4.13
SN100 Services Addendum - Additional API and Operational Guidance	0.5
SN100x Crypto Library Information on Guidance and Operation	2.4
SN100x Crypto Library: Errata sheet	1.0
SN100x Crypto Library: User Manual – RNG Library	1.4
SN100x Crypto Library: User Manual – SHA Library	0.3
SN100x Crypto Library: User Manual – Secure SHA Library	0.4
SN100x Crypto Library: User Manual – SHA-3 Library	0.2
SN100x Crypto Library: User Manual – Secure SHA-3 Library	0.2
SN100x Crypto Library: User Manual – HMAC Library	0.4
SN100x Crypto Library: User Manual – Rsa Library (Rsa)	2.0
SN100x Crypto Library: User Manual – RSA Key Generation Library (RsaKg)	0.7
SN100x Crypto Library: User Manual – ECC over GF(p) Library	2.0
SN100x Crypto Library: User Manual – ECDAA	1.0
SN100x Crypto Library: User Manual – TwdEdMontGfp Library	1.2
SN100x Crypto Library: User Manual – eUICC Library	0.5
SN100x Crypto Library: User Manual – Symmetric Cipher Library (SymCfg)	1.1
SN100x Crypto Library: User Manual – Utils Library	0.4
SN100x Crypto Library: User Manual – UtilsMath Library	1.0
SN100x Crypto Library: User Manual – KDF Library	1.0
SN100x Crypto Library: User Manual – HASH Library	0.3

Table 7 Manuals SN100_SE B2.1 C58

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. 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.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

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. As no changes were made to the TOE the evaluators determined that no additional independent functional testing was necessary

2.6.2   Independent penetration testing

The evaluator independent penetration tests were conducted according to the following testing approach:

- During evaluation of the ADV, ATE and ALC classes the evaluators hypothesized possible vulnerabilities. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained in particular from the source code analysis in IMP. This resulted in a shortlist of potential vulnerabilities to be tested.

- Next the evaluators analysed the TOE design and implementation for resistance against the JIL attacks. This resulted in further potential vulnerabilities to be tested.

- The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ARC has assessed all information.

- The evaluators concluded that a number of areas could be potentially vulnerable for attackers possessing a high attack potential. Consequently, practical penetration testing was performed for absolute assurance.

The total test effort expended by the evaluators was 7.5 weeks. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 0% perturbation attacks, 20% retrieving keys with FA, 60% side channel attacks, 0% exploitation of test features, 20% attacks on RNG, 0% ill-formed Java Card application, 0% software attacks, and 0% application isolation penetration tests. For this re-certification, no tests were performed.

2.6.3   Test configuration

Testing performed during this re-evaluation was executed on slightly different configurations of the TOE SN100_SE B2.1 C25/C48/C58. The differences (i.e. no services software, no crypto lib) between these configurations and the TOE have been analysed. They have no impact on the test results, hence the test results apply to the TOE.

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.

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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. 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 29 site certificates and Site Technical Audit 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 SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58. The user can identify the certified configuration by reading the TypeID bytes.

The wafer fab can be identified (i) physically by reading the laser marking (an "s" indicates sample from GF7 Diffusion center, an "L" indicates a sample from GF1 Diffusion center, and an "SJ" indicates a sample from SMNC Diffusion center) and/or (ii) logically by reading the ECID of the sample - by means of the implemented Operation System or in Chip Health Mode. A 0xC2 as first byte indicates a sample from diffusion center GF7, a 0xC0 indicates a sample from GF1, and 0x80 indicates a sample from SMNC diffusion center. Only the certified configurations C48 and C58 can be manufactured in all three wafer fabs, the certified configuration C25 only in GF7.

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 SN100 Series – Secure Element with Crypto Library, versions B2.1 C25/C48/C58, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of:

EAL 5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ALC_FLR.1, ATE_COV.3, ATE_FUN.2, AVA_VAN.5, and ASE_TSS.2 for Global conformance.

The assurance conformance of MPU/MMU memory management sub-TSF is **EAL6 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.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3   Security Target

The SN100 Series - Secure Element with Crypto Library Security Target, Rev. 4.3 — 12 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
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
EC	Elliptic Curve
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
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TDES	Triple DES
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 1.5.1, May 2018
[ETR]	Evaluation Technical Report SN100 Series - Secure Element with Crypto Library B2.1 C25, C48, and C58, 24-RPT-1370, Version 3.0, 27 January 2025
[ETRfC]	Evaluation Technical Report for Composition SN100 Series - Secure Element with Crypto Library B2.1 C25/C48/C58, 24-RPT-1371, Version 3.0, 27 January 2025
[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)
[JIL-SPM-INT]	JIL, ADV_SPM.1 interpretation for [CC:2022] transition, Version 1.0, May 2024
[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]	SN100 Series - Secure Element with Crypto Library Security Target, Rev. 4.3 — 12 November 2024
[ST-lite]	SN100 Series - Secure Element with Crypto Library, Security Target Lite, Rev. 4.3 — 12 November 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)