Certification Report

SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Troplowitzstrasse 20
22529 Hamburg
Germany

Evaluation facility:

Riscure B.V.
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-0258298-CR3**
Report version:	**3**
Project number:	**0258298_3**
Author(s):	**Wim Ton**
Date:	**21 October 2022**
Number of pages:	**16**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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

The 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 SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37. The developer of the SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37 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 single chip secure element with a crypto library that can be used as a platform for highly secure operating systems and applications. Outside of the TOE, the chip also contains an NFC controller and a power management unit.

The TOE was evaluated initially by Riscure B.V. located in Delft, The Netherlands and was certified on 16 August 2021. The re-evaluation of the TOE (comprising two re-evaluation activities) has also been conducted by Riscure B.V. and was completed on 21 October 2022 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 two “recertification with major changes” activities. The major changes are:

- Hardware:

  Adding a second manufacturer “SMIC”

- C37 Software:

  Getting more entropy from the TRNG to seed the DRNG, and an improved heath test

  Adding the AES-XTS mode

  Hardening of the elliptic curve arithmetic

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

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37, 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 SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37 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, ASE_TSS.2 (TOE summary specification with architectural design summary), and ALC_FLR.1 (Basic flaw remediation).

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).

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

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The IC can be manufactured by two factories, GF1 and SMIC. The hardware from each factory has a unique hardware identifier (HW_ID) as detailed in the tables below.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Hardware	SN220_SE B0.1	C13 HW_ID: 0x35 GF1 0x3D SMIC
Software Specific for C13 configuration	IC Dedicated Software: Factory OS Boot OS (ROM) Flash driver	 9.0.4 9.0.3 9.0.2
	Configuration Data: Factory Page System Page Common BootOS patch	 21043 21031 9.0.3 PL1v1
	Security Software: Services Library Crypto Library	 9.17.4 2.2.0

Table 1 TOE version C13 components

Delivery item type	**Identifier**	**Version**
Hardware	SN220_SE B0.1	C37 HW_ID: 0x33 GF1 0x37 SMIC
Software Specific for C37 configuration	IC Dedicated Software: Factory OS Boot OS (ROM) Flash driver	 10.0.2 10.0.2 10.0.0
	Configuration Data: Factory Page System Page Common BootOS patch	 21043 21031 10.0.2 PL1v1
	Security Software: Services Library Crypto Library	 10.17.6 2.3.1

Table 2 TOE version C37 components

To ensure secure usage, a set of guidance documents is provided, together with the SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37. 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 SN220_SE is designed to act as an integral part of a security system composed of SN220_SE and Security IC Embedded Software to strengthen it as a whole. Several security mechanisms of SN220_SE are completely implemented in and controlled by SN220_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 SN220_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 SN220_SE and its security functionality.

The SN220_SE provides:

- hardware to perform computations on multi-precision 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 the 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 the Galois/Counter Mode (GCM) of operation and the Galois Message Authentication Code (GMAC) for symmetric-key cryptographic block ciphers
- hardware to calculate Cyclic Redundancy Checks (CRC)
- hardware to provide True Random Numbers
- hardware and service software to control access to memories and hardware components.

In addition, SN200_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.

Crypto library:

The following symmetric cryptographic primitives are supported and included within the TSF, with the modes ECB, CBC, CBC-MAC, CTR, CFB, OFB:

- 3DES with 112- and 168-bit keys for encryption/decryption and MAC generation/verification including Retail-MAC
- AES with 128-, 192- and 256-bit keys for encryption/decryption (including GCM and XTS) and MAC generation and verification including CCM.

The following asymmetric cryptographic primitives are supported and included within the TSF

- RSA and RSA-CRT for encryption/decryption, signature generation/verification with a modulus length between 512 and 4096 bits and various padding modes.
- ECDSA signature generation/verification with a key length between 128 and 640 bits.
- ECDAA signature generation with a key length between 128 and 640 bits.
- EC point multiplication and addition with a key length between 128 and 640 bits
- EDDSA signature generation/verification using Edward curves with a key length between 128 and 640 bits.
- Diffie-Hellman key exchange using Montgomery curves with a key length between 128 and 640 bits. For example, Curve25519
- Key generation for the above asymmetric algorithms

The following hash operations are supported and included within the TSF in a secure and in a standard version:

- SHA-1,
- SHA-224, SHA-256, SHA-384, SHA-512,
- SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512,
- SHAKE-128, SHAKE-256
- HMAC generation using the above hash algorithms

Key derivation with an output length between 128 and 256 bits according to ANSI X9.63

eUICC authentication with the following algorithms:

- MILENAGE
- TUAK
- CAVE

A deterministic random number generator, seeded by an on-chip physical random number generator

Secure operations:

- Copy
- Compare
- CRC
- Modular arithmetic

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 4.3 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 SN220x Single Chip Secure Element and NFC Controller Series combines on a single die an Embedded Secure Element, an NFC Controller and a shared Power Management Unit (PMU). The subsystems are called "SN220_SE", "SN220_NFC" and "SN220_PMU", respectively. The NFC Controller and the PMU are not part of the TOE.

The hardware part of the SN220_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.

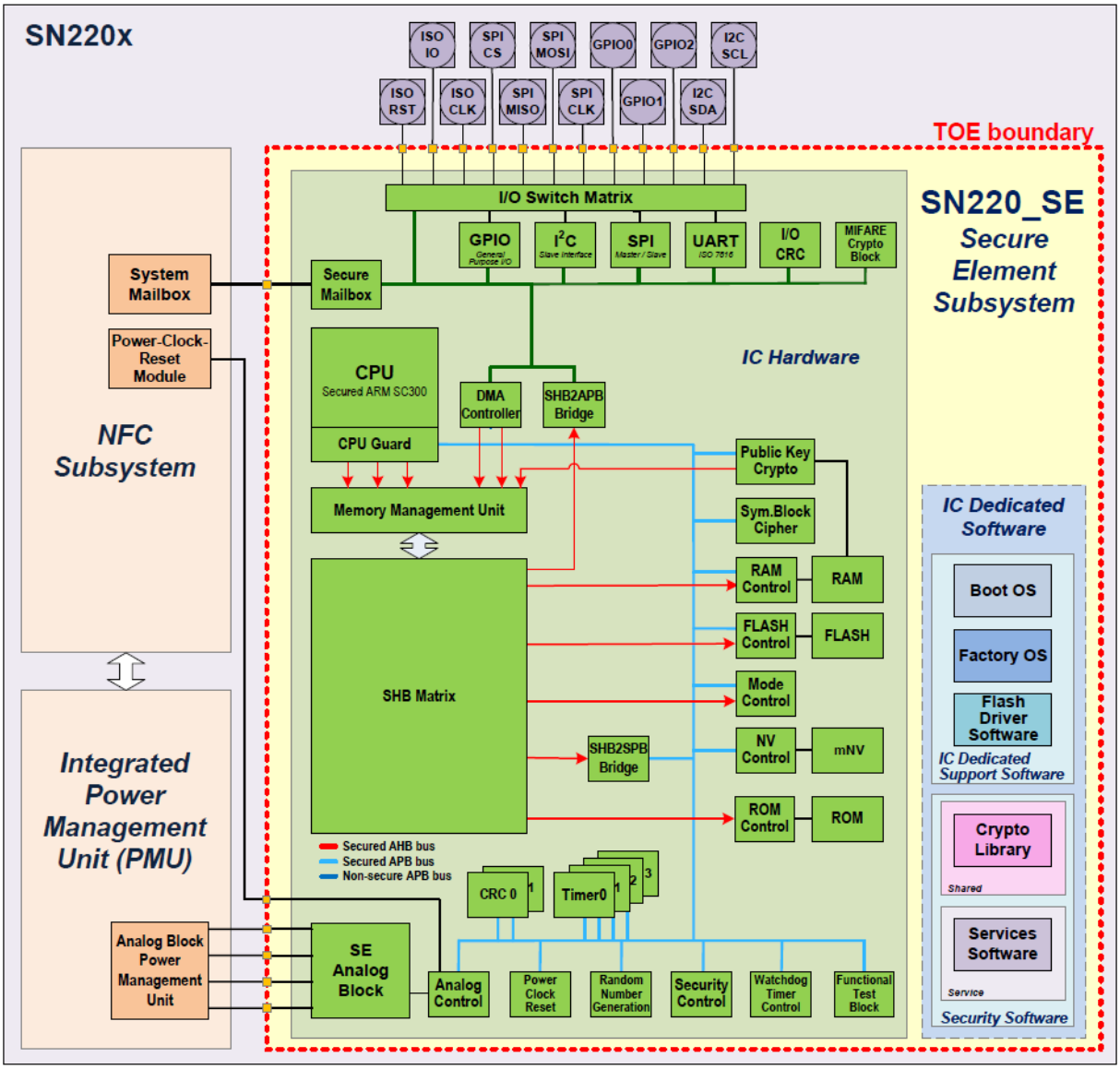

Figure 1 SN220x overview

The TOE is an integral part of the SN220x IC.

The IC Dedicated Software consists of IC Dedicated Support Software and Security Software:

- The Security Software, composed of Services Software and a Crypto Library, can be used by the Security IC Embedded Software.
- The Crypto Library consists of several binary packages for usage by the Security IC Embedded Software.
- The Services Software consists of Flash Services Software and Services Framework Software. The Flash Services Software manages technical demands of the Flash memory and provides an interface for Flash erase and/or programming for the Security IC Embedded Software. The Services Framework Software represents a collection of different abstractions and utility functions that provide a runtime environment to the individual Services.

2.5 Documentation

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

Identifier	Version
SN220x_SE High-performance secure elements subsystem, Product Data Sheet	v1.2
SN220x_SE – SFR Tables for Coburg Core	v0.1
SN220x Wafer and Delivery Specification, Product Data Sheet addendum	v1.3
P73 Family SC300 User Manual, Product Data Sheet addendum	v1.0
P73 Family DMA Controller PL080 User Manual, Product Data Sheet addendum DocID 341410	v1.0
P73 Family Chip Health Mode, Application note	v1.0
P73 Family Code Signature Watchdog, Application note	v1.1

Table 3 SE220x_SE documentation

Identifier	Version
SN220x Crypto Library Information on Guidance and Operation	1.1
SN220x Crypto Library: User Manual - RNG Library	1.0
SN220x Crypto Library: User Manual - RSA Library	1.0
SN220x Crypto Library: User Manual – RSA Key Generation Library (RsaKg)	1.0
SN220x Crypto Library Symmetric Cipher Library (SymCfg) Library	1.0
SN220x Crypto Library: User Manual – ECDAA	1.0
SN220x Crypto Library: User Manual – HASH Library	1.0
SN220x Crypto Library: User Manual – SHA-3 Library	1.0
SN220x Crypto Library: User Manual – Secure SHA Library	1.0
SN220x Crypto Library: User Manual – Secure SHA-3 Library	1.0
SN220x Crypto Library: User Manual – HMAC Library	1.0
SN220x Crypto Library: User Manual – Kdf Library	1.0
SN220x Crypto Library: User Manual –TwdEdMontGfp Library	1.0
SN220x Crypto Library: User Manual – eUICC Library	1.0
SN220x Crypto Library: User Manual – Utils Library	1.0
SN220 Services User Manual API and Operational Guidance	1.1
SN220 Services Addendum Additional API and Operational Guidance	1.1

Table 4 IC Dedicated Software documentation for version B01 C31

Identifier	Version
SN220x Crypto Library Information on Guidance and Operation	1.3
SN220x Crypto Library: User Manual - RNG Library	1.1

SN220x Crypto Library: User Manual - RSA Library	1.1
SN220x Crypto Library: User Manual – RSA Key Generation Library (RsaKg)	1.0
SN220x Crypto Library Symmetric Cipher Library (SymCfg) Library	1.1
SN220x Crypto Library: User Manual – ECDAA	1.0
SN220x Crypto Library: User Manual – HASH Library	1.0
SN220x Crypto Library: User Manual – SHA-3 Library	1.0
SN220x Crypto Library: User Manual – Secure SHA Library	1.0
SN220x Crypto Library: User Manual – Secure SHA-3 Library	1.0
SN220x Crypto Library: User Manual – HMAC Library	1.0
SN220x Crypto Library: User Manual – Kdf Library	1.0
SN220x Crypto Library: User Manual –TwdEdMontGfp Library	1.0
SN220x Crypto Library: User Manual – eUICC Library	1.0
SN220x Crypto Library: User Manual – Utils Library	1.0
SN220 Services User Manual API and Operational Guidance	1.1
SN220 Services Addendum Additional API and Operational Guidance	1.1

Table 5 IC Dedicated Software documentation for version B01 C37

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 modules (according to EAL6 requirements). The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used 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 in the baseline evaluation, the developers provided samples and a test environment. The evaluators reproduced a selection of developer tests as well as a small number of test cases designed by the evaluator. For the evaluator defined tests the developer delivered samples (and support in writing scripts). However, Riscure's test environment was used for these ATE_IND tests.

As part of the re-evaluation, the evaluator examined the changes to the TOE and the results of the baseline certification. Some configuration fixes had to be made to the TOE to improve the yield of the SMIC fab. Therefore, it was concluded that the physical properties of samples from this fab may differ from the samples manufactured at GF1. Hence, in this re-evaluation, the evaluators performed verification tests to assess the resistance to side channel attacks of the samples manufactured at the SMIC fab.

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 specified in *[JIL-AAPS]* and *[JIL-AM]*. 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.

The total test effort expended by the evaluators during the baseline evaluation was 24 weeks. During that test campaign, 60% of the total time was spent on Perturbation attacks, 35% on side-channel testing, and 5% on logical tests.

During the re-evaluation, the evaluator performed further penetration testing resulting from the updated vulnerability and to consider the update of the IC Dedicated Software and the addition of the manufacturer “SMIC”:

The test effort expended by the evaluators during the re-evaluation was 55 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 configuration

Testing was performed on slightly different configurations of the SN220_SE, that allowed the light sensor to be turned off. Otherwise, the light sensor would interfere with the tests. The differences 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. The tests were executed on the SN220_SE B0.1 C37 with SMIC hardware.

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.

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 twenty-eight (28) site certificates and twenty-six (26) 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 SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37. Chapter 3.1.2 of the *[ST*] describes how the user can read 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 Reports for the sites *[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 SN220 Series - Secure Element with Crypto Library B0.1 C13 and B0.1 C37, 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]*.

2.9.1 Comments/Recommendations

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

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in sections 2.1, and 4.1 of SN220_SE Information on Guidance and Operation and sections 6.1.5, 6.2.8 of SN220x Crypto Library Information on Guidance and Operations (both as referenced in the [ST]). Therefore, it is vital to maintain meticulous adherence to the user guidance of both the software and the hardware part of the TOE.

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

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

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: KoreanSeed (out of scope), OSCCA SM2, OSCCA SM3 and OSCCA SM4 (out of scope), and FeliCa (out of scope).

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).

[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 SN220 Series - Secure Element with Crypto Library Security Target, v1.5, 29 September 2022 *[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
ARM	Advanced Risc Machines
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
DMA	Direct Memory Access
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
GCM	Galois Counter Mode
GF1	Global Foundry Fab 1
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
KDF	Key Derivation Function
MAC	Message Authentication Code
MMU	Memory Management Unit
NFC	Near Field Communication
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OSCCA	Office of the State Commercial Cryptography Administration
PP	Protection Profile
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SMIC	Semiconductor Manufacturing International Corporation
SHA	Secure Hash Algorithm

SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator
XTS	XEX Tweakable block cipher with ciphertext Stealing

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 for SN220 Series - Secure Element with Crypto Library B0.1 C13/C37, 20210539-D3, Version 1.6, 6 October 2022
[ETRfC]	ETR for Composite Evaluation, SN220 Series - Secure Element with Crypto Library B0.1 C13/C37, 20210539-D4, Version 1.6, 6 October 2022
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[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 2.5, 28 March 2019
[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]	SN220 Series - Secure Element with Crypto Library Security Target, v1.5, 29 September 2022
[ST-lite]	SN220 Series - Secure Element with Crypto Library Security Target Lite, v1.5, 29 September 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)