Certification Report

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

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Business Unit Security & Connectivity
Beiersdorfstrasse 12
22529 Hamburg
Germany

Evaluation facility: ***Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-2300181-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300181-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**10 May 2024**
Number of pages:	**14**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

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

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

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 SN220 Series - Secure Element with Crypto Library B0.1 C13/C37. The developer of the SN220 Series - Secure Element with Crypto Library B0.1 C13/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 and NFC Controller Series combines on a single die an Embedded Secure Element and a NFC Controller. The two subsystems are called "SN220_SE" and "SN220_NFC". The NFC Controller is not part of the TOE.

The TOE was previously evaluated by Riscure B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 21 October 2022 (CC-22-0258298). The current evaluation of the TOE has also been conducted by Riscure B.V. and was completed on 10 May 2024 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB].*

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

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

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

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

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/C37 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SN220_SE B0.1	C13
	SN220_SE B0.1	C37
Software specific for C13 configuration	IC Dedicated Support Software: Factory OS Boot OS Flash Driver Software	 9.0.4 9.0.3 9.0.2
	Configuration Data Factory Page System Page Common BootOS Patch	 21043 21031 9.0.3 PL1 v1
	Security Software Services Software Crypto Library	 9.17.4 2.2.0
Software specific for C37 configuration	IC Dedicated Support Software: Factory OS Boot OS Flash Driver Software	 10.0.2 10.0.2 10.0.0
	Configuration Data Factory Page System Page Common BootOS Patch	 21043 21031 10.0.2 PL1 v1
	Security Software Services Software Crypto Library	 10.17.6 2.3.1

To ensure secure usage a set of guidance documents is provided, together with the SN220 Series - Secure Element with Crypto Library B0.1 C13/C37. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST-lite]*, 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.

SN220_SE 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, SN220_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 consists of several binary packages that are pre-loaded to the ROM memory of the TOE with the exception of micro-code for public key cryptography co- processor for usage by the Security IC Embedded Software. The Crypto Library provides:

- AES
- Triple-DES (3DES)
- Multi-precision arithmetic operations including exact division, secure modular addition, secure modular subtraction, secure modular multiplication, secure modular inversion, secure arithmetic comparison and secure exact addition.
- RSA
- RSA key generation
- RSA public key computation
- ECDSA (ECC over GF(p)) signature generation and verification
- 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, SHAKE128/256 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, SHAKE128/256 algorithms
- HMAC algorithms
- eUICC authentication functions (MILENAGE, TUAK and CAVE)
- Hash-based key derivation function according to ANSI X9.63

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.

Note that the Crypto Library also implements:

- KoreanSeed
- OSCCA SM2, OSCCA SM3 and OSCCA SM4
- Felica

However, these library elements are not in the scope of evaluation.

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-Lite]*.

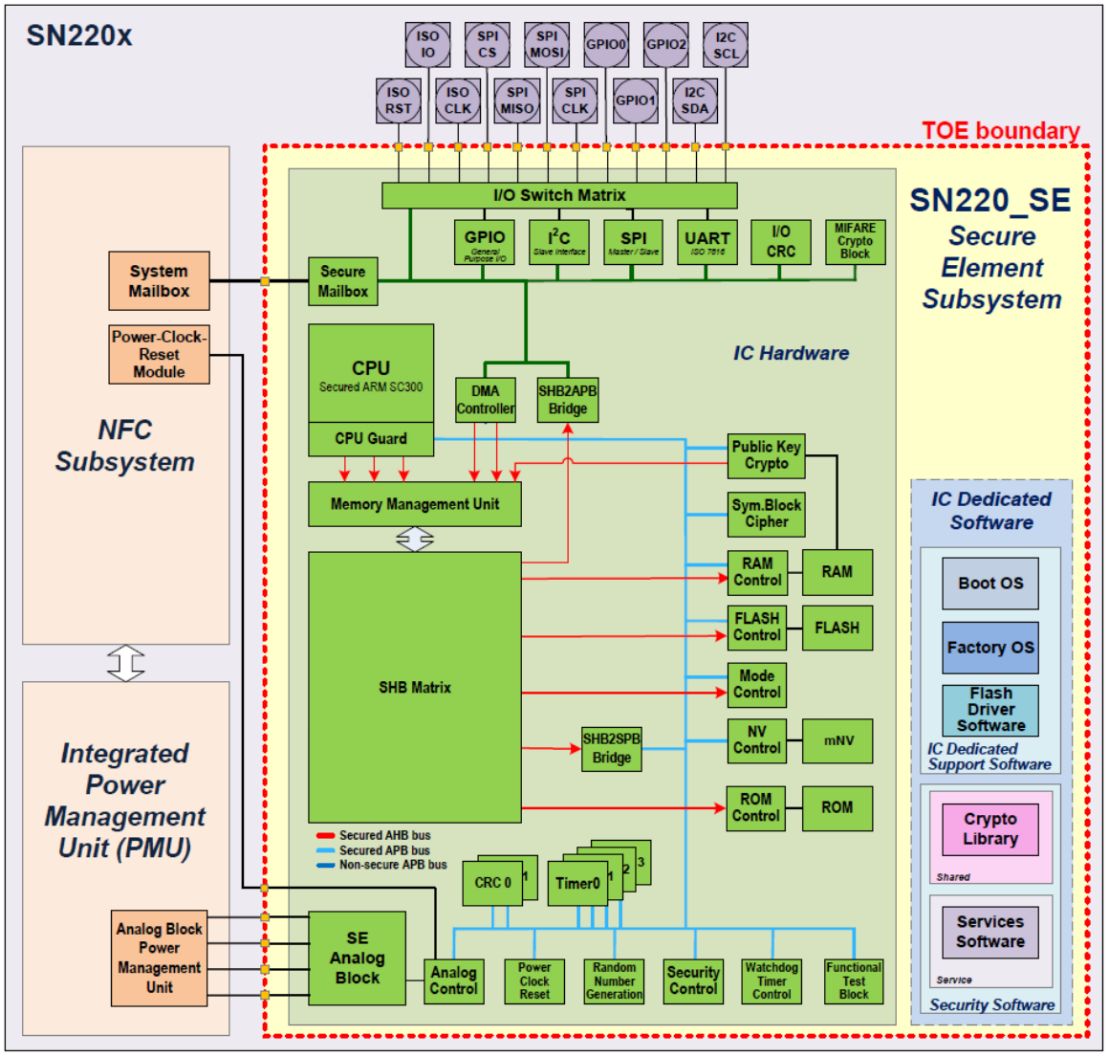
2.3.2 Clarification of scope

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 and a NFC Controller. The two subsystems are called "SN220_SE" and "SN220_NFC". The NFC Controller is not part of the TOE.

The hardware part of the SN220_SE incorporates an 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.



2.5 Documentation

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

Identifier	Version
SN220x_SE High-Performance secure element subsystem, Product data sheet, dated 24 August 2022	Rev 1.3
SN220x_SE SFR Tables for Coburg core, dated 12 August 2020	Rev 0.1
SN220x Wafer and delivery specification, Product data sheet addendum, dated 24 August 2022	Rev 1.3
P73 family SC300 User Manual, Product Data sheet addendum, dated 12 August 2015	Rev 1.0
P73 family DMA Controller PL080 User manual, Product data sheet addendum, dated 18 August 2015	Rev 1.0
P73 Family Chip Health Mode, Application note, dated 09 August 2018	Rev 1.0
P73 Family Code Signature Watchdog, Application note, dated 12 November 2018	Version 1.1
ARM®v7-M Architecture Reference Manual, dated 2 December 2014	DDI 0403E.b (ID120114), Issue E.b
SN220_SE Information on Guidance and Operation, dated 12 July 2021	Rev 1.0
SN220 Services User Manual - API and Operational Guidance, dated 1 October 2020 for C13, 05 May 2022 for C37	Rev 1.0 for C13 Rev 1.1 for C37
SN220 Services Addendum - Additional API and Operational Guidance, dated 1 October 2020 for C13, 05 May 2022 for C37	Rev 1.0 for C13 Rev 1.1 for C37
SN220x Crypto Library Information on Guidance and Operation, dated 12 July 2021 for C13, 31 August 2022 for C37	Rev 1.1 for C13 Rev 1.3 for C37
SN220x Crypto Library: User Manual: RNG, dated 10 June for C13, 1 December 2020 for C37	Rev 1.0 for C13 Rev 1.1 for C37
SN220x Crypto Library: User Manual: Utils, dated 23 June 2020	Rev 1.0
SN220x Crypto Library: User Manual: SymCfg, dated 23 June 2020 for C13, 25 February 2022 for C37	Rev 1.0 for C13 Rev 1.1 for C37
SN220x Crypto Library: User Manual: RSA, dated 21 July 2020 for C13, 15 December 2020 for C37	Rev 1.0 for C13 Rev 1.1 for C37
SN220x Crypto Library: User Manual: RSA Key Generation, dated 30 July 2020	Rev 1.0
SN220x Crypto Library: User Manual: ECC over GF(p), dated 17 June 2020	Rev 1.0
SN220x Crypto Library: User Manual: ECDAA, dated 17 June 2020	Rev 1.0
SN220x Crypto Library: User Manual: SHA, dated 19 June 2020	Rev 1.0
SN220x Crypto Library: User Manual: SecSHA, dated 19 June 2020	Rev 1.0
SN220x Crypto Library: User Manual: SHA3, dated 10 August 2020	Rev 1.0
SN220x Crypto Library: User Manual: SecSHA3, dated 10 August 2020	Rev 1.0
SN220x Crypto Library: User Manual: HMAC, dated 19 June 2020	Rev 1.0
SN220x Crypto Library: User Manual: HASH, dated 19 June 2020	Rev 1.0

SN220x Crypto Library: User Manual: TwdEdMontGfp, dated 23 June 2020	Rev 1.0
SN220x Crypto Library: User Manual: eUICC, dated 17 June 2020	Rev 1.0
SN220x Crypto Library: User Manual – Kdf Library, dated 23 June 2020	Rev 1.0
SN220x Crypto Library: User Manual – Utils Math, dated 23 June 2020	Rev 1.0

2.6 IT Product Testing

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

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

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.

2.6.2 Independent penetration testing

The vulnerability is performed based on the structure of the attack methods defined by JHAS [JIL.AM]. For each attack method, we describe the objective of the attack and how the attack method applies to the TOE. The following is considered for each attack method:

- The design and implementation of the features relevant for the attack method
- Specific attack techniques from the evaluator's attack repository
- Implemented countermeasures
- User guidance

All potential vulnerabilities were analysed using the knowledge from all the evaluation classes, from previous evaluations and information from the public domain. Assessments were made to determine the applicability of these vulnerabilities.

The total test effort expended by the evaluators was 32 days. During that test campaign, 47% of the total time was spent on Perturbation attacks, 47% on side-channel testing, and 6% on logical tests.

2.6.3 Test configuration

The samples used for testing are either in SN220x B0.1 002 or SN220x B0.1 C12 configuration depending on the type of test to be executed (IC or CL respectively). The only difference between this configuration and the certified configuration of the TOE is the sensor configuration. In the TOE configuration, there is a possibility to turn off the reaction to light sensors in case a faulty behaviour of the light sensors is observed in the field. However, the services software user guidance requirement blocks the final product from switching to this mode. The evaluated samples do not have the possibility to switch to this mode either. Therefore, the evaluated samples are effectively equivalent to the certified 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.

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 27 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/C37. Chapter 1.4.2 of the *[ST-Lite]* 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. 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/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_0084]*.

2.10 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. The requirements and recommendations on the operational environment are described in SN220_SE Information on Guidance and Operation, throughout sections 2 - 9. 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, OSCCA SM2, OSCCA SM3 and OSCCA SM4, Felica, which are out of scope as there are no security claims relating to these.

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 SN220 Series - Secure Element with Crypto Library Security Target, Rev 1.6, Dated 12 April 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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

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

[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, 20230432_V-D3, Version 1.1, Dated 18 April 2024
[ETRfC]	ETR for composite evaluation SN220 Series - Secure Element with Crypto Library B0.1 C13/C37, 20230432_V-D4, Version 1.1, Dated 18 April 2024
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP_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]	SN220 Series - Secure Element with Crypto Library Security Target, Rev 1.6, Dated 12 April 2024
[ST-lite]	SN220 Series - Secure Element with Crypto Library Security Target Lite, Rev 1.6, Dated 12 April 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)