TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Certification Report

SN200 Series - Secure Element with Crypto Library
SN200_SE B1.1 C04

Sponsor and developer:	**NXP Semiconductors Germany GmbH** **Troplowitzstrasse 20** **22529 Hamburg** **Germany**
Evaluation facility:	**Riscure** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-217812-CR**
Report version:	**1**
Project number:	**217812**
Author(s):	**Hans-Gerd Albertsen**
Date:	**4 July 2019**
Number of pages:	**16**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-217812**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

NXP Semiconductors Germany GmbH

Troplowitzstrasse 20, 22529 Hamburg, Germany

Product and assurance level

SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04

Assurance Package:
- EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2

Protection Profile Conformance:
- Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014

Project number **217812**

Evaluation facility

Riscure BV located in Delft, the Netherlands

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS
IT SECURITY CERTIFIED

SOGIS Mutual Recognition Agreement for components up to EAL 7

Validity

Date of 1st issue : **08-07-2019**

Certificate expiry : **08-07-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch
Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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 license 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, in order 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 authorized provided the report is reproduced in its entirety.

TÜVRheinland®
Precisely Right.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

TÜVRheinland®
Precisely Right.

1   Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04. The developer of the SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04 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 SN200x 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 "SN200_SE", "SN200_PMU", and "SN200_NFC". The TOE is the SN200_SE. The NFC Controller and the PMU are not part of the TOE.

The TOE is the SN200_SE B1.1 in one configuration SN200_SE B1.1 C04. 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 has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 4 July 2019 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 SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04, 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 SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04 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 provides sufficient evidence that the TOE meets the EAL 6 augmented (EAL 6(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2   Certification Results

2.1   *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components (taken from *[ST]*):

Item	Identifier	Version
Hardware	SN200_SE (Base layer and fixed metal masks)	B1.1
Software (IC Dedicted Support Software)	Factory OS	7.0.6
	Boot OS	7.0.5
	Flash Driver Software	7.0.1

Table 1 Components common for all SN200_SE B1.1

Item	Identifier	Version
Configuration Data	Factory Page	19554
	System Page Common	20103
	BootOS Patch	7.0.5 PL3 v9
Security Software	Services Software	4.13.3.0
	Crypto Library	1.0.0

Table 2 Components of SN200_SE B1.1 specific for C04

To ensure secure usage a set of guidance documents is provided together with the SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04. Details can be found in section 2.5 Documentation of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[PP]* and *[ST]*, chapter 1.3.3

2.2   *Security Policy*

The security functionality of SN200_SE is designed to act as an integral part of a security system composed of SN200_SE and Security IC Embedded Software to strengthen it as a whole. Several security mechanisms of SN200_SE are completely implemented in and controlled by SN200_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 SN200_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 SN200_SE and its security functionality.

SN200_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,

TÜVRheinland®
Precisely Right.

- 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, 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.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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 SN200x 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 "SN200_SE", "SN200_PMU", and "SN200_NFC". The TOE is the SN200_SE. The NFC Controller and the PMU are not part of the TOE.

The TOE is the SN200_SE B1.1 in one SN200_SE B1.1 C04. 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 SN200x 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 "SN200_SE", "SN200_PMU", and "SN200_NFC". The TOE is the SN200_SE. The NFC Controller and the PMU are not part of the TOE.

The TOE is the SN200_SE B1.1 in one SN200_SE B1.1 C04. The TOE will be provided with Crypto Library and Services Software as part of the IC Dedicated Software.

The hardware part of the SN200_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.

SN200_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 SN200_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 SN200_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.
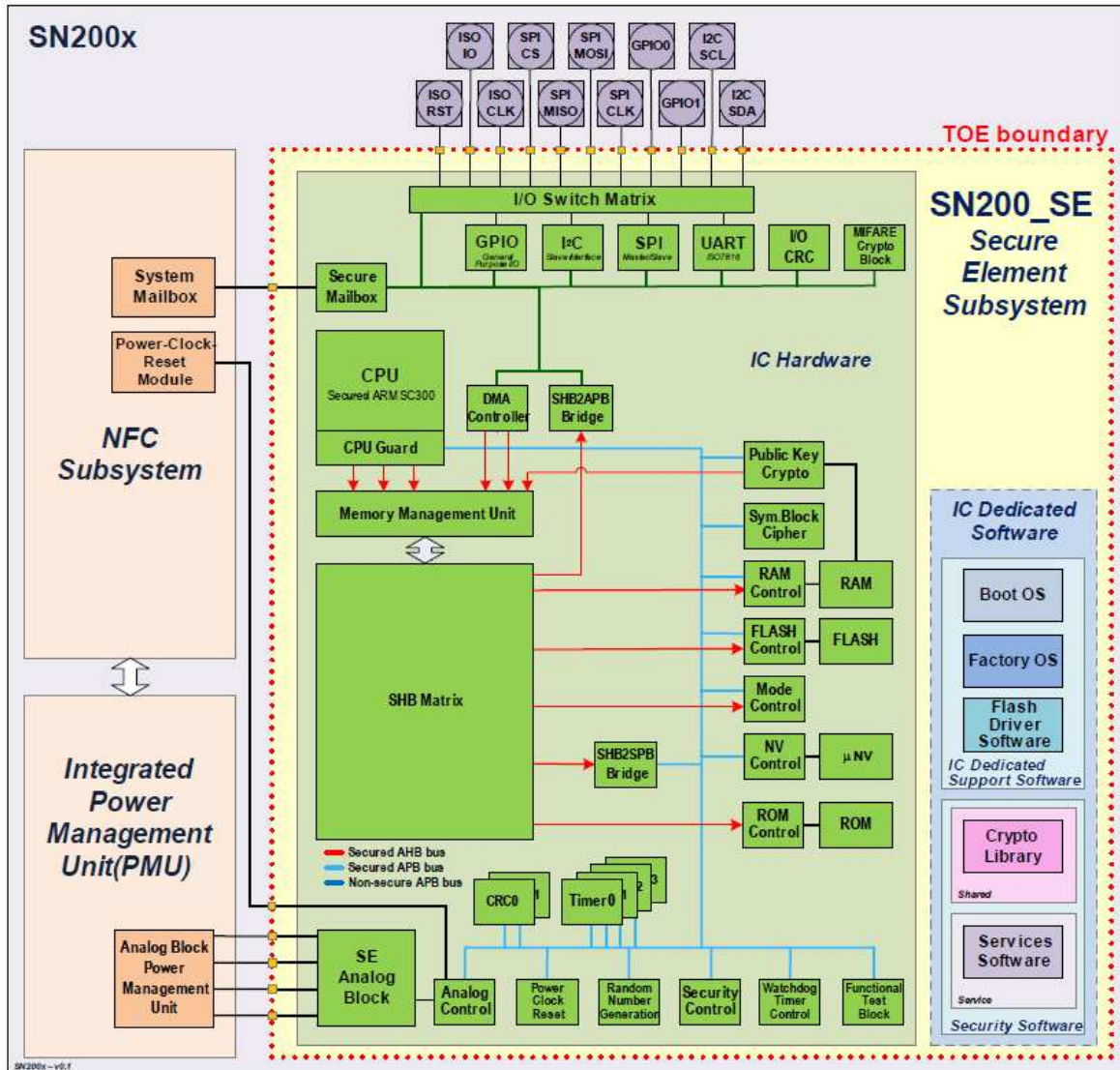

Figure 1 Logical architecture of the TOE

2.5   Documentation

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

Documentation for SN200_SE B1.1 common for any logical configuration

Item	Identifier	Version
Manuals	SN200x_SE High-performance secure element subsystem, Product data sheet	1.0

	SN200x_SE - SFR Tables for Celle core	0.8
	SN200x Wafer and Delivery Specification, Product data sheet addendum	1.0
	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	ID120114 (ARM website)

Table 3 Manuals common for all SN200_SE B1.1

Item	Identifier	Version
Manuals	SN200_SE Information on Guidance and Operation	1.1
	SN200 Services User Manual – API and Operational Guidance	4.13
	SN200 Services Addendum - Additional API and Operational Guidance	0.5
	SN200x Crypto Library Information on Guidance and Operation	1.4
	SN200x Crypto Library: User Manual – RNG Library	1.1
	SN200x Crypto Library: User Manual – SHA Library	1.0
	SN200x Crypto Library: User Manual – Secure SHA Library	1.0
	SN200x Crypto Library: User Manual – SHA-3 Library	1.0
	SN200x Crypto Library: User Manual – Secure SHA-3 Library	1.0
	SN200x Crypto Library: User Manual – HMAC Library	1.0
	SN200x Crypto Library: User Manual – Rsa Library (Rsa)	1.1
	SN200x Crypto Library: User Manual – RSA Key Generation Library (RsaKg)	1.0
	SN200x Crypto Library: User Manual – ECC over GF(p) Library	1.0
	SN200x Crypto Library: User Manual – ECDAA	1.0
	SN200x Crypto Library: User Manual – TwdEdMontGfp Library	1.0
	SN200x Crypto Library: User Manual – eUICC Library	1.0
	SN200x Crypto Library: User Manual – Symmetric Cipher Library (SymCfg)	1.1
	SN200x Crypto Library: User Manual – Utils Library	1.0
	SN200x Crypto Library: User Manual – HASH Library	1.0
	SN200x Crypto Library: Errata sheet	1.0

Table 4 Manuals of SN200_SE B1.1 specific for C04

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 has 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.

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have reproduced a selection of the 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.

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

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.

2.6.3 Test Configuration

Testing was performed on slightly different configurations of the TOE SN200_SE B1.1 C04. 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.

2.6.4 Testing 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. So, no exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 17 site certificates (GlobalLogic REC Wroclaw, NXP Bangalore, NXP Caen, NXP Eindhoven, NXP Glasgow 2, NXP Gratkorn, NXP Hamburg, NXP Leuven, NXP Mougins, NXP San Diego, NXP San Jose, AMTC Dresden, ASE Kaohsiung, NXP ATKH Kaohsiung (ATKH-WT&WTT Kaohsiung), Global Foundries Singapore, NXP Nijmegen, and Spil Taichung City (Taiwan).

No sites have been visited as part of this evaluation.

TÜVRheinland®
Precisely Right.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and configuration identifiers SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04. The user can identify the certified configuration by reading the TypeID bytes. The details are described in the guidance documentation.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to 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 SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04, to be CC Part 2 extended, CC Part 3 conformant, (check ST compliance claim) 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]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 for satisfying the AVA_VAN.5 "high attack potential". In order 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).

TÜVRheinland®
Precisely Right.

3 Security Target

The SN200 Series - Secure Element with Crypto Library Security Target, st_SN200_SE_1_1,pdf, 24.06.2019 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

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
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LAN	Local Area Network
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NSCIB	Netherlands scheme for certification in the area of IT security
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
SSH	Secure Shell
SSL	Secure Sockets Layer

TOE	Target of Evaluation
TCP	Transmission Control Protocol
TRNG	True Random Number Generator
VLAN	Virtual LAN

TÜVRheinland®
Precisely Right.

5 Bibliography

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

[CC]   Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM]   Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR]   Evaluation Technical Report SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04, NSCIB_217812-ETR_v1.0.pdf, v1.0, 01.07.2019.

[ETRfC]   ETR for Composite Evaluation SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04, NSCIB_217812-ETR-COMP_v1.0.pdf, v1.0, 01.07.2019.

[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, Version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014

[ST]   SN200 Series - Secure Element with Crypto Library Security Target, st_SN200_SE_1_1,pdf, 24.06.2019.

[ST-lite]   SN200 Series - Secure Element with Crypto Library Security Target Lite, st-lite_SN200_SE_1_1,pdf, 24.06.2019

[ST-SAN]   ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).