Certification Report

SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48

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

Evaluation facility: ***Brightsight BV***
Brasserplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-174263-CR**
Report version:	**1**
Project number:	**174263**
Author(s):	**Hans-Gerd Albertsen/Wouter Slegers**
Date:	**18 January 2019**
Number of pages:	**14**
Number of appendices:	**0**

Headoffice:
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 Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-174263**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors GmbH** **Business Unit Security & Connectivity** **Troplowitzstrasse 20, 22529 Hamburg, Germany**
Product and assurance level	**SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48** Assurance Package: ▪ EAL6 augmented with ALC_FLR.1 and ASE_TSS.2 Protection Profile Conformance (if appropriate): • Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the referenced BSI-PP-0084-2014
Project number	**174263**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

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.

Validity	Date of 1st issue : **22-01-2019** Certificate expiry : **22-01-2024**

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.

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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48. The developer of the SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48 is NXP Semiconductors 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 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 two configurations SN100_SE B2.1 C25 and SN100_SE B2.1 C48. 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 Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 13 January 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 SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48, 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 SN100_SE B2.1 C25/C48 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+ 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]*.

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 SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Item	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

Item	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

Item	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

To ensure secure usage a set of guidance documents is provided together with the SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48. Details are listed in table 4 and table 6 of this document. can be found in section ”Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[PP0084]*.

2.2 Security Policy

The TOE is the SN100_SE B2.1 in two configurations SN100_SE B2.1 C25 and SN100_SE B2.1 C48. 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.

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

For further details see Figure 1 below.

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

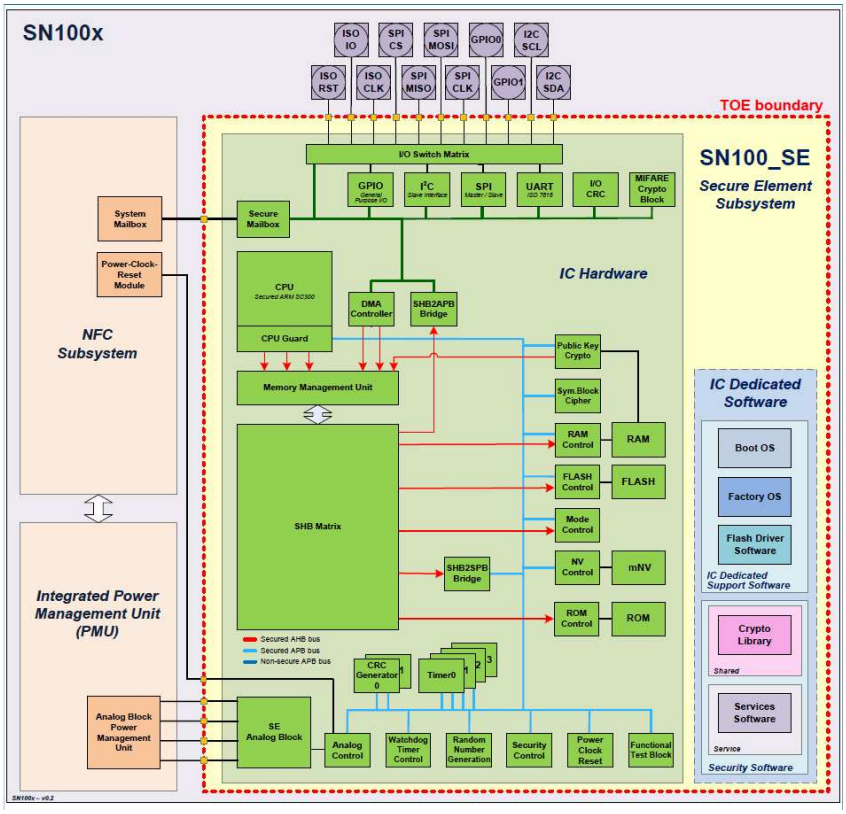

Figure 1 Logical architecture of the TOE.

2.5 Documentation

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

Item	Identifier	Version
Manuals	SN100x_SE High-performance secure element subsystem, Product data sheet	1.0
	SN100x 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 4 Manuals common for all SN100_SE B2.1

Item	Identifier	Version
Manuals	SN100_SE Information on Guidance and Operation	1.3
	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	1.8
	SN100x Crypto Library: Errata sheet	1.0
	SN100x Crypto Library: User Manual – RNG Library	1.3
	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)	1.2
	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)	0.4
	SN100x Crypto Library: User Manual – Utils Library	0.4
	SN100x Crypto Library: User Manual – HASH Library	0.3

Table 5 Manuals of SN100_SE B2.1 specific for C25

Item	Identifier	Version
Manuals	SN100_SE Information on Guidance and Operation	1.3
	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	1.8
	SN100x Crypto Library: Errata sheet	1.0
	SN100x Crypto Library: User Manual – RNG Library	1.3
	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)	1.2
	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)	0.4
	SN100x Crypto Library: User Manual – Utils Library	0.4
	SN100x Crypto Library: User Manual – HASH Library	0.3

Table 6 Manuals of SN100_SE B2.1 specific for C48

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 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, Brightsight's test environment was used for these ATE_IND tests.

2.6.2 Independent Penetration Testing

The Vulnerability Analysis is performed based on the structure of the attack methods defined by JHAS. For each attack method, the evaluator has analysed and described the objective of the attack and how the attack method applies to the TOE.

2.6.3 Test Configuration

The TOE has two different configurations: SN100_SE B2.1 C25 and SN100 B2.1 C48. The difference is in the Factory Page, BootOS Patch Level, and Services Software. As agreed with the certifier, the evaluator performed the tests on slightly different configurations. These differences compared to the TOE have been analysed and regarded as not relevant for the testcases. Details are described in the Evaluation Technical Report *[ETR]*. Therefore, the testing results apply to all variants.

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. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80 bits, this is considered sufficient. 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 16 site certificates (GlobalLogic REC Wroclaw, NXP Bangalore, NXP Caen, NXP Eindhoven, NXP Glasgow, NXP Gratkorn, NXP Hamburg, NXP Leuven, NXP Mougins, NXP San Diego, AMTC Dresden, ASE Kaohsiung, ATKH-WT& WTT Kaohsiung, ATKH Global Foundries Singapore, NXP Nijmegen, and Spil Taichun City (Taiwan).

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 SN100_SE B2.1 C25/C48. 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]*[2] 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 SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48, to be CC Part 2 extended, CC Part 3 conformant, and to meet the requirements of EAL 6 augmented by 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. There are no particular obligations or recommendations for the user apart from following the user guidance.

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

Please note that for the C25 configuration the user of the SN100_SE B2.1 C25 shall not use Deep Power Down mode with RAM retention ON.

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: PUF (out of scope), 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", 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, Revision 2.2, NXP Semiconductors, Date 2018-11-30 *[ST]* and the S100 Series - Secure Element with Crypto Library Security Target Lite, Revision 2.2, NXP Semiconductors, Date 2018-11-30 *[ST-Lite]* are included here by reference.

Please note that the 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:

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
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands scheme for certification in the area of IT security
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
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 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] Delta Evaluation Technical Report for SN100 Series – Secure Element with Crypto Library SN100_SE B2.1 C25/C48, Version 2.1, 19. December 2018.

Evaluation Technical Report for SN100 Series – Secure Element with Crypto Library SN100_SE B2.1 C25, Version 6.0, 07. January 2019.

[ETRfC] ETR for Composition for SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48, Version 7.0, 07. January 2019.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September April 2017.

[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 referenced BSI-PP-0084-2014

[ST] SN100 Series - Secure Element with Crypto Library Security Target, Revision 2.2, NXP Semiconductors, Date 2018-11-30.

[ST-Lite] SN100 Series - Secure Element with Crypto Library Security Target Lite, Revision 2.2, NXP Semiconductors, Date 2018-11-30.

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

(This is the end of this report).