Certification Report

NXP JCOP on SN100.C25 Secure Element

Sponsor and developer: ***NXP Semiconductors GmbH***
Business Unit Security and Connectivity
Troplowitzstrasse 20
22529 Hamburg
Germany

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-195714-CR3**
Report version:	**3**
Project number:	**195714**
Author(s):	**Andy Brown**
Date:	**01 October 2020**
Number of pages:	**15**
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

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 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.

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 NXP JCOP on SN100.C25 Secure Element. The developer of the NXP JCOP on SN100.C25 Secure Element 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 TOE consists of the certified embedded Secure Element (eSE), including an associated Crypto Library and Security Software, and a software stack (JCOP) which is stored and executed on the eSE. The Secure Element is embedded in a micro-controller which also includes an Integrated NFC controller and a System Mailbox which provides the communication interface for the TOE, The TOE provides Java Card 3.0.4 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.2.1.
It includes also NXP proprietary functionalities: Config Applet, OS Update Component, Applet Migration, Restricted Mode and Error Detection Code (EDC) API.

Cryptographic functionality includes 3DES, AES, RSA and RSA CRT ; SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms, HMAC, ECC over GF(p), Twisted Edwards Curve 25519 for signature generation and verification (EdDSA), Diffie-Hellman Key Exchange on Montgomery Curve (25519). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20.

Note that proprietary applications have been included in the TOE, but as there are no security claims on these functionalities, these application's functionality has not been assessed, only the self-protection of the TSF.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 13 March 2019. The re-evaluation also took place by Brightsight B.V. and was completed on 01 October 2020 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 third issue of the Certification Report is a result of a "recertification with major changes".

The major changes are the inclusion of the JCOP 6.1 variant and associated guidance.

The security evaluation re-used 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 NXP JCOP on SN100.C25 Secure Element, 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 NXP JCOP on SN100.C25 Secure Element 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis), 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]*.

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

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP on SN100.C25 Secure Element from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware (Part of SN100 certificate)	"NXP SN100 Series Secure Element with Crypto Library" SN100_SE B2.1 C25	B2.1 C25
Software / Firmware (Part of SN100 certificate)	Factory OS	4.2.0
	Boot OS	4.2.0
	Flash Driver Software	4.0.8
	Factory Page	18218
	Systems Page Common	18468
	BootOS Patch	4.2.0 PL3 v4
	Services Software	4.13.3.0
	Crypto Library	1.0.0
Software	JCOP5.0 OS, native applications and OS Update Component	R1.11.0
	JCOP6.0 OS, native applications and OS Update Component	R1.13.0
	JCOP6.1 OS, native applications and OS Update Component	R1.04.0

To ensure secure usage a set of guidance documents is provided together with the NXP JCOP on SN100.C25 Secure Element. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.3.2.

2.2 Security Policy

This TOE is a composite TOE, consisting of a Java Card smart card operating system, an OS updater, an applet migration feature, a restricted mode and an underlying platform, which is composed of a library which provides cryptographic functions and a secure micro controller. The TOE provides Java Card 3.0.4 functionality (and preparation for Java Card 3.0.5 functionality) with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.2.1 including SCP03.

It includes also NXP Proprietary Functionality

- Config Applet: JCOP OS includes a Config Applet that can be used for configuration of the TOE.
- OS Update Component: Proprietary functionality that can update JCOP OS or UpdaterOS.
- Applet Migration: Keep User Data, Key Data or PIN Data after updating an applet.

- Restricted Mode: In Restricted Mode only very limited functionality of the TOE is available such as, e.g.: reading logging information or resetting the Attack Counter.
- Error Detection Code (EDC) API.

Cryptographic functionality includes 3DES, AES, RSA and RSA CRT ; SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms, HMAC, ECC over GF(p), Twisted Edwards Curve 25519 for signature generation and verification (EdDSA), Diffie-Hellman Key Exchange on Montgomery Curve (25519). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20.

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 5.2 of the *[ST]*.

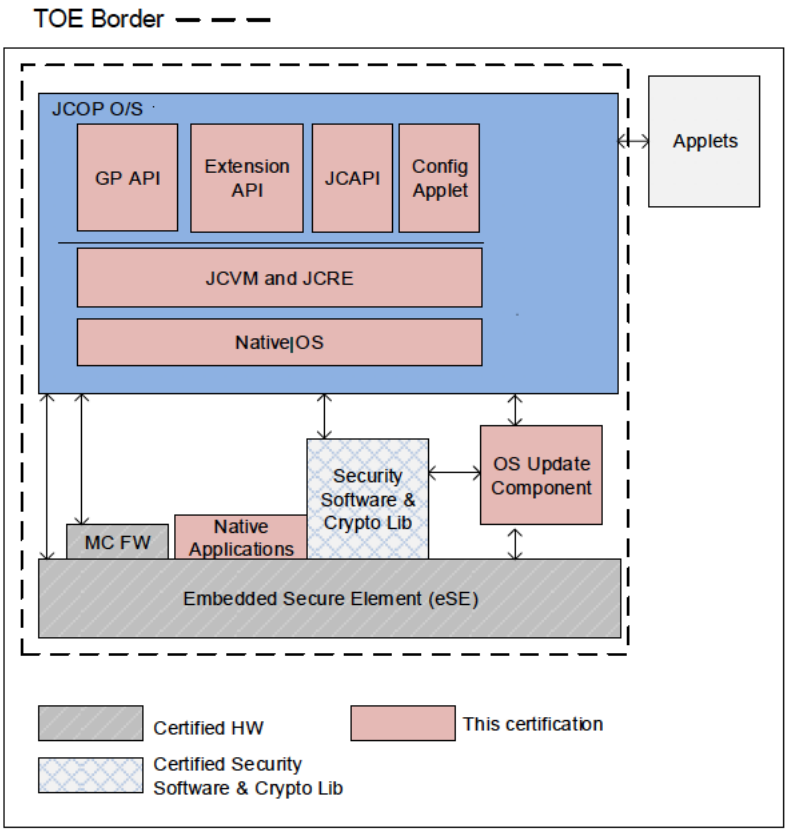
2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that proprietary applications have been included in the TOE, but as there are no security claims on these functionalities, these applications' functionality has not been assessed, only the self-protection of the TSF.

2.4 Architectural Information

The logical architecture, originating from the Security Target *[ST],* of the TOE can be depicted as follows:



The TOE provides a variety of security features. The hardware of the Micro Controller already protects against physical attacks by applying various sensors to detect manipulations and by processing data in ways which protect against leakage of data by side channel analysis. With the software stack the TOE provides many cryptographic primitives for encryption, decryption, signature generation, signature verification, key generation, secure management of PINs and secure storage of confidential data (e.g. keys, PINs). Also the software stack implements several countermeasures to protect the TOE against attacks.

2.5 Documentation

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

For JCOP 5.0:

Identifier	Version
JCOP 5.0 R1.11.0, User Guidance Manual	Rev. 1.10, 2019-07-09
JCOP 5.0 R1.11.0, User Guidance Addendum	Rev. 1.8, 2018-04-10
JCOP 5.0 R1.11.0, Anomaly Sheet	Rev. 1.11, 2018-08-30

For JCOP 6.0:

Identifier	Version
JCOP 6.0 R1.13.0, User Guidance Manual	Rev. 1.14, 2019-07-09
JCOP 6.0 R1.13.0, User Guidance Addendum	Rev. 1.13, 2019-04-16
JCOP 6.0 R1.13.0, Anomaly Sheet	Rev. 1.13, 2019-04-16

For JCOP 6.1:

Identifier	Version
JCOP 6.1 R1.04.0, User Guidance Manual	Rev. 3.3, 2020-02-24
JCOP 6.1 R1.04.0, User Guidance Addendum	Rev. 3.3, 2020-02-26
JCOP 6.1 R1.04.0, Anomaly Sheet	Rev. 3.3, 2020-02-27

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 tests cover all security functions and aspects of the TSF. Testing is performed during development as well as for acceptance/release. The developer used a set of test suites (industry standard and proprietary ones) and tools to test the TOE as well as an emulator, PC Platform and FPGA tool as some tests could only be performed in such environment. The identification was checked based on the SVN number. The developer uses a distributed test environment to allow usage of a vast amount of simultaneously driven testing equipment.

The developer has performed extensive testing on FSP, subsystem, module and module interface level. The tests are performed by NXP through execution of the test scripts using an automated and distributed system. Test tools and scripts are extensively used to verify that the tests return expected values.

Code coverage analysis is used by NXP to verify overall test completeness. Test benches for the various TOE parts are executed using code coverage measurement and analysis tools to determine the code coverage (i.e. lines, branches and/or instructions, depending on tool) of each test bench. Cases with incomplete coverage are analysed. For each tool, the developer has investigated and documented inherent limitations that can lead to coverage being reported as less than 100%. In such cases the developer provided a "gap" analysis with rationales (e.g. attack counter not hit due to redundancy checks).

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.

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.

Tests from different test benches that are testing different parts of the functionality of the TOE were selected for witnessing at the developer location. The tests were running at the network of the developer.

Besides the repetition of develop tests, the evaluator defined spot-checks on the calculation of code-coverage as used by the developer to demonstrate their completeness of testing. As developer functional testing is quite rigorous, no other tests were defined by the evaluator.

The TOE exists in three configurations, i.e.: "JCOP 5.0 R1.11.0", "JCOP 6.0 R1.13.0" and "JCOP 6.1 R1.04.0". Each configuration exists in a single evaluated configuration.

The TOE has three configurations. Since the first and second certified configurations, i.e. JCOP 5.0 R1.11.0 and JCOP 6.0 R1.13.0, have not changed since being certified, the test results (both of the developer and evaluator) for these configurations remain valid. The evaluator then verified that the added configuration, i.e. JCOP 6.1 R1.04.0, was tested and performed his own independent testing sample on this configuration. This means that all tests have been performed on the all configurations of the TOE.

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ADV and AGD potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour. From the ASE class, no potential vulnerabilities were identified.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed according to the attack list in *[JIL-AP]*. An important source for assurance against attacks in this step is the *[ETRfC-HW]* of the underlying platform; no additional potential vulnerabilities were concluded from this.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For most of the potential vulnerabilities a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

On the original certification, in total 11 test cases were described. The test effort is a fulltime occupation during to the test period as described in the test descriptions. It results in an overall effort of 21 weeks.

In the first re-certification, 3 perturbation tests, 3 side channel analysis tests, and 2 logical tests were performed.

In this second re-certification, 1 perturbation test and 1 logical test were performed to supplement previous tests (which have been shown to be still valid on this configuration in the vulnerability analysis phase).

See details in *[ETRfC].*

2.6.3 Test Configuration

The TOE was tested in both the JCOP 5.0, JCOP 6.0 and JCOP 6.1 configurations. For some test cases, development versions of the TOE were used. The differences in these versions have been analysed and all tests are applicable to the actual version of the TOE in all of its configurations.

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.

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

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

Testing (both functional and penetration) results from the previous certification activities have been re-used. Re-use has been made based on argumentation that the re-used tests were less than a year old and there were no changes to the first configuration ("JCOP 5.0 R1.11.0") nor the second configuration ("JCOP 6.0 R1.13.0") of the TOE. To address the third configuration of the TOE ("JCOP 6.1 R1.04.0"), testing also used in EMVco certifications has been used in this recertification, as well as testing only for the CC certification.

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 7 Site Technical Audit Re-use report approaches:

- NXP Semiconductors in Hamburg,
- NXP Semiconductors in Gratkorn,
- NXP Semiconductors India Private limited,
- NXP San Diego,
- NXP San Jose,
- NXP Eindhoven HTC60.
- DIGITAL REALTY Data Center, Phoenix.

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 NXP JCOP on SN100.C25 Secure Element (with configurations "JCOP 5.0 R1.11.0", "JCOP 6.0 R1.13.0" and "JCOP 6.1 R1.04.0").

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 NXP JCOP on SN100.C25 Secure Element, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 5** augmented with ALC_DVS.2, AVA_VAN.5, ASE_TSS.2 and ALC_FLR.1. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' 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.

For users of the previous certification results: note that the RNG claim has been changed from DRG.4 to DRG.3 at the first recertification.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations:

- none (note that any algorithms implemented by the proprietary applets is out of scope for this certifications).

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).

3 Security Target

The Security Target, NXP JCOP on SN100.C25 Secure Element, Rev 3.4, 25 August 2020, NXP Semiconductors GmbH *[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
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
RMI	Remote Method Invocation
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.

[HW-CL-CERT] 19-RPT-876 v4.0 Evaluation Technical Report for Composition SN100 Series – Secure Element with Crypto Library B2.1 C25, C48 and C58 with GF1 EAL6+, Certification id: NSCIB-CC-174263-3.

[HW-CL-ETRfC] Certification Report SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48/C58, version 1, CR-174263-CR3, 31 December 2019

[ETR] Evaluation Technical Report “NXP JCOP on SN100.C25 Secure Element” – EAL5+, 19-RPT-948, Version 4.0, 01 October 2020.

[ETRfC] Evaluation Technical Report for Composition “NXP JCOP on SN100.C25 Secure Element” – EAL5+, 19-RPT-949, Version 4.0, 01 October 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[JC PP] Java Card Protection Profile – Open Configuration, Version 3.0.5, December 2017 (certified with reference BSI-CC-PP-0099-2017).

[ST] Security Target, NXP JCOP on SN100.C25 Secure Element, Rev 3.4, 25 August 2020, NXP Semiconductors GmbH.

[ST-LITE] Security Target Lite, NXP JCOP on SN100.C25 Secure Element, Rev 3.1, 25 August 2020, NXP Semiconductors GmbH

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

(This is the end of this report).