Certification Report

NXP JCOP 5.1 on SN100.C48 Secure Element

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20, D-22529** **Hamburg**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2200049-01-CR**
Report version:	**1**
Project number:	**NSCIB-2200049-01**
Author(s):	**Andy Brown**
Date:	**19 April 2023**
Number of pages:	**13**
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.

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 NXP JCOP 5.1 on SN100.C48 Secure Element. The developer of the NXP JCOP 5.1 on SN100.C48 Secure Element 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 composite TOE, consisting of a Java Card smart card operating system and an underlying platform, which is a secure micro controller. The TOE provides Java Card 3.0.5 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.3.

It includes also NXP Proprietary Functionality: Secure Box, Config Applet, OS Update Component, 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). Furthermore, the TOE provides random number generation according to class DRG.3 of AIS 20.

Note that proprietary applications such as FeliCa and Mifare API have been included in the TOE, but as there are no security claims on these applications in this certificate, these applications have not been assessed, only the self-protection of the TSF.

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 30 April 2019 (CC-19-221699)

The first re-evaluation of the TOE was also conducted by SGS Brightsight B.V and was completed on 29 November 2019 with the approval of the ETR under the accreditation of TÜV Rheinland Nederland (CC-19-221699-2).

The second issue of the Certification Report was a result of a "recertification with major changes". The major changes were related to a change of the commercial name, reduced claims in the ST due to reduced claims in the underlying ST without change of the software, a minor change in the guidance not impacting the security functionality of the certified product. The identification of the maintained product was modified to NXP JCOP5.1 eSE on SN100.C48 Secure Element.

Users of the previous certificate are reminded that the following SFRs were removed due to the changes in the underlying ST: FCS_CKM.2 and FCS_CKM.3. The SFR FCS_RNG changed from DRG.4 to DRG.3.

The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis was not made. No renewed testing was necessary.

This current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 19 April 2023 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 major changes from previous evaluations are:

- The ST has been updated to modify the version of the user manuals;

- The User Guidance Manual has been updated;

- A development site has been added.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made. Additional testing has been performed.

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 5.1 on SN100.C48 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 5.1 on SN100.C48 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 provide 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), 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]* (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 NXP JCOP 5.1 on SN100.C48 Secure Element from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SN100x IC Package (as part of SN100 certificate)	B2.1 C48
Software	Factory OS (part of SN100 certificate)	4.2.0
	Boot OS (part of SN100 certificate)	4.2.0
	Flash Driver Software (part of SN100 certificate)	4.0.8
	Services Software (part of SN100 certificate, specific to C48)	4.13.7.1
	Crypto Library (part of SN100 certificate)	1.0.0
	JCOP5.1 OS, native applications and OS Update Component	R1.00.1

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP 5.1 on SN100.C48 Secure Element. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.2.

2.2 Security Policy

This TOE is a composite TOE, consisting of a Java Card smart card operating system, an OS updater, 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 3.0.5 functionality with post-issuance applet loading, card content management and secure channel features as specified in Global Platform 2.3 including SCP03. It includes also NXP proprietary functionalities:

- Secure Box: Enables the TOE to run third party native code (Secure Box Native Lib) on the micro-controller.
- Config Applet: JCOP5.1 OS includes a Config Applet that can be used for configuration of the TOE.
- OS Update Component: Proprietary functionality that can update JCOP5.1 OS or UpdaterOS.
- 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.

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 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 such as FeliCa and Mifare API have been included in the TOE, but as there are no security claims on these applications in this certificate, these applications have not been assessed, only the self-protection of the TSF.

2.4 Architectural Information

The logical architecture, originating from the Security Target 1ST], of the TOE can be depicted as follows:

2.5 Documentation

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

Identifier	Version
JCOP 5.1 R1.00.1 User Guidance Manual	Rev 2.3
JCOP 5.1 R1.00.1 User Guidance Manual Addendum SEMS	Rev 1.1

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 TSFI, 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.

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 *[HW-ETRfC]* 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.

For the second re-certification the vulnerability analysis did not lead to additional testing.

For this current evaluation, the vulnerability analysis was refreshed again. The vulnerability analysis was assured via selected testing: 50% were perturbation attacks, 50% were side channel testing.

2.6.3 Test configuration

The TOE was tested in the following configuration: NXP JCOP5.1 R1.00.1 (J5U2M001F3560600). A subset of the test campaign was performed on a previously certified product JCOP5.0 R1.11.0(J5T2M001B39100, NSCIB-CC-195714) as the potential vulnerabilities tested are shared between both products. For details see *[ETRfC]*.

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.

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. The remaining security level still exceeds 80 bits, so this is considered sufficient. Therefore, no exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Reused Evaluation Results

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

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 6 Site Technical Audit Report{s}.

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 5.1 on SN100.C48 Secure Element.

The TOE can only be in a single evaluated configuration. Changes that can be made using the Config Applet are within this configuration.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2]. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the NXP JCOP 5.1 on SN100.C48 Secure Element, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with AVA_VAN.5, ALC_DVS.2, 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 “Documentation” 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 concerning 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 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

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

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.

Users of the first certificate are reminded that the following SFRs have been removed from subsequent certifications of the TOE due to the changes in the underlying ST: FCS_CKM.2 and FCS_CKM.3. The SFR FCS_RNG has changed from DRG.4 to DRG.3.

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: MIFARE and Felica.

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 NXP JCOP 5.1 on SN100.C48 Secure Element Security Target, Revision 2.8, 17 March 2023 *[ST]* is included here by reference.

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

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
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
PP	Protection Profile
RMI	Remote Method Invocation
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]	Evaluation Technical Report “NXP JCOP 5.1 SN100.C48 Secure Element” – EAL5+, 22-RPT-055, Version 2.0, 31 March 2023
[ETRfC]	Evaluation Technical Report for Composition "NXP JCOP 5.1 SN100.C48 Secure Element"– EAL5+, 23-RPT-053, Version 2.0, 31 March 2023
[HW-CERT]	SN100 Series – Secure Element with Crypto Library SN100_SE B2.1 C25/C48/C58, CC-22-174263, 174263_6, 29 November 2022
[HW-ETRfC]	Evaluation Technical Report for Composition SN100 Series - Secure Element with Crypto Library B2.1 C25, C48, and C58, Product Update F EAL6+, Version 2.0, 25 November 2022
[HW-ST]	Security Target, SN100 Series - Secure Element with Crypto Library, version v3.5, 21 April 2021
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 22 August 2022
[PP]	Java Card Protection Profile - Open Configuration, Version 3.0.5, December 2017, registered under BSI-CC-PP-0099-2017
[ST]	NXP JCOP 5.1 on SN100.C48 Secure Element Security Target, Revision 2.8, 17 March 2023
[ST-lite]	NXP JCOP 5.1 on SN100.C48 Secure Element, Revision 2.7, 17 March 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)