Certification Report

NXP JCOP 5.2 on SN100.C58 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-2200050-01-CR**
Report version:	**1**
Project number:	NSCIB-2200050-01
Author(s):	**Andy Brown**
Date:	**19 April 2023**
Number of pages:	**16**
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 5.2 on SN100.C58 Secure Element. The developer of the NXP JCOP 5.2 on SN100.C58 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 Java Card with GP functionality, extended with eUICC and CSP functionality. It can be used to load, install, instantiate and execute off-card verified Java Card applets. The eUICC part is a UICC embedded in a consumer device and may be in a removable form factor or otherwise. It connects to a given mobile network, by means of its currently enabled MNO profile. The CSP part offers Cryptographic Service Provider functionality.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft. The evaluation 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 TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 10 December 2019 under the accreditation of TÜV Rheinland Nederland on 2 December 2019 (CC-19-0023577). A re-evaluation took place by SGS Brightsight B.V. and was completed on 08 July 2020 and a maintenance activity was subsequently completed on 23 October 2020. This further re-evaluation also took place by SGS Brightsight and was completed on 14 June 2021 with the approval of the ETR.

The third issue of the Certification Report was a result of a “recertification with major changes”.

The major changes were:

Addition of a further TOE configuration, namely JCOP 5.2. R3.01.1 with plug-in 195 and with plug-in 196, which is compliant to the GSMA SGP.22 version 2.2.2 June 2020 (instead of version 2.2.1 that is used for the JCOP 5.2. R1 and JCOP 5.2. R2).

Removal of CAT-TP support.

Extension of UAI query to include Amendment H Status.

Addition of 5th logic channel

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.

Note that in first re-certification of the TOE (reported in the second issue of the Certification Report) the major changes are the introduction of two new configurations (JCOP 5.2 R2.01.1 and JCOP 5.2 R2.02.1). A maintenance activity was then performed to include JCOP 5.2 R2.03.1.

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. 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 5.2 on SN100.C58 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 5.2 on SN100.C58 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 ASE_TSS.2 “TOE summary specification with architectural design summary”, ALC_DVS.2 (Sufficiency of security measures), ALC_FLR.1 (flaw remediation) and AVA_VAN.5 (Advanced methodical vulnerability analysis)

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 5.2 on SN100.C58 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 (platform)	SN100x IC Package (as part of SN100 certificate)	B2.1 C58
Data configuration (platform)	Factory Page	18652
	System Page Common	18468
	BootOS Patch (part of SN100 certificate)	4.2.0 PL5 v16
Software (platform)	Factory OS (part of SN100 certificate)	4.2.0
	Boot 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 C58)	4.14.0.1
	Crypto Library (part of SN100 certificate, specific to C58)	2.0.0
Software	JCOP 5.2 on SN100.C58 R1.01.1 with plugin version 129	
	JCOP5.2 OS, native applications, OS Update Component, eUICC R1.01.1 component and CSP component	R1.01.1
	eUICC plug-in	1.5.129
	JCOP 5.2 on SN100.C58 R2.01.1 with plugin version 146	
	JCOP5.2 OS, native applications, OS Update Component, eUICC component and CSP component	R2.01.1
	eUICC plug-in	1.5.146
	JCOP 5.2 on SN100.C58 R2.02.1 with plugin version 148	
	JCOP5.2 OS, native applications, OS Update Component, eUICC component and CSP component	R2.02.1
	JCOP 5.2 on SN100.C58 R2.03.1 with plugin version 148	
	JCOP5.2 OS, native applications, OS Update Component, eUICC component and CSP component	R2.03.1
	eUICC plug-in	1.5.148
	JCOP 5.2 on SN100.C58 R3.01.1 with plugin version 195 or plugin version 196	
	JCOP5.2 OS, native applications, OS Update Component, eUICC component and CSP component	R3.01.1
	eUICC plug-in	1.5.195
	eUICC plug-in	1.5.196

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP 5.2 on SN100.C58 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 1.3.3.

2.2 Security Policy

The TOE is a composite product on top of CC certified Hardware, Firmware and Crypto Library. The overall product consists of a Secure Micro-Controller and a software stack. The Micro-Controller provides an Integrated NFC controller and an embedded Secure Element core. The software stack creates 2 separate domains to provide a converged product consisting of a familiar Java Card Secure Element domain and an eUICC domain providing UICC functionality and external ISO-7816 connectivity.

The TOE has the following features:

- Cryptographic algorithms and functionality:
  - 3DES for en-/decryption (CBC and ECB) and MAC generation and verification (2-key 3DES, 3-key 3DES, Retail-MAC, CMAC and CBC-MAC)
  - AES (Advanced Encryption Standard) for en-/decryption (GCM, CBC and ECB) and MAC generation and verification (CMAC, CBC-MAC)
  - RSA and RSA CRT for en-/decryption and signature generation and verification
  - RSA and RSA CRT key generation
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithm
  - Secure SHA-1, Secure SHA-224, Secure SHA-256, Secure SHA-384, Secure SHA-512 hash algorithm
  - HMAC
  - ECC over GF(p) for signature generation and verification (ECDSA)
  - ECC over GF(p) key generation for key agreement
  - Random number generation according to class DRG.3 of AIS 20
- Java Card 3.0.5 functionality
- GlobalPlatform 2.3 functionality including Amendments A,B,C,D,E,F,H and I and is compliant with the Common Implementation Configuration
- GSMA ’Remote SIM Provisioning Architecture for consumer Devices’
- Cryptographic Service Provider (CSP) features
- NXP Proprietary Functionality:
  - MiFare functionality accessible via Applets using the MiFare API – no security functionality is claimed
  - OSSCA (Chinese Crypto) functionality accessible via Applets using the OSSCA API – No security functionality is claimed
  - Felica functionality accessible via Applets using the Felica API - no security functionality is claimed for this functionality
  - Config Applet: JCOP5.2 OS includes a Config Applet that can be used for configuration of the TOE
  - OS Update Component: Proprietary functionality that can update JCOP5.2 OS or UpdaterOS
  - UAI update component: Proprietary functionality that is can update JCOP5.2 OS- no security functionality is claimed
  - 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

The following functionality was added (and assessed) with the JCOP 5.2 R2 configuration:

- CAT-TP, with limitations as described in the JCOP 5.2 R2 User Guidance Manual, Section 8.1(20)

- 5G features as per SIM Alliance 2.3, see JCOP 5.2 R2 User Guidance Manual Section 2.4.4. and 8.1(15)
- Extension to Global Platform Amendment H, UGM see JCOP 5.2 R2 User Guidance Manual Section 3.5.7
- CPLC data made available through SystemInfo, UGM see JCOP 5.2 R2 User Guidance Manual Section 2.1.3.22

The following functionality was changed (and assessed) with the JCOP 5.2 R3 configuration:

- R3 is compliant to the GSMA SGP.22 version 2.2.2 June 2020, whilst previous versions are (R1 and R2) are compliant to GSMA SGP.22 version 2.2.1 Dec 2018
- CAT-TP is not supported in the R3 product
- UAI query extended to include Amendment H Status see JCOP 5.2 R3.01.1.User Guidance Manual Section 7.1.2
- Addition of 5th Logical Channel JCOP 5.2 see R3.01.1.User Guidance Manual Section 8.4

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

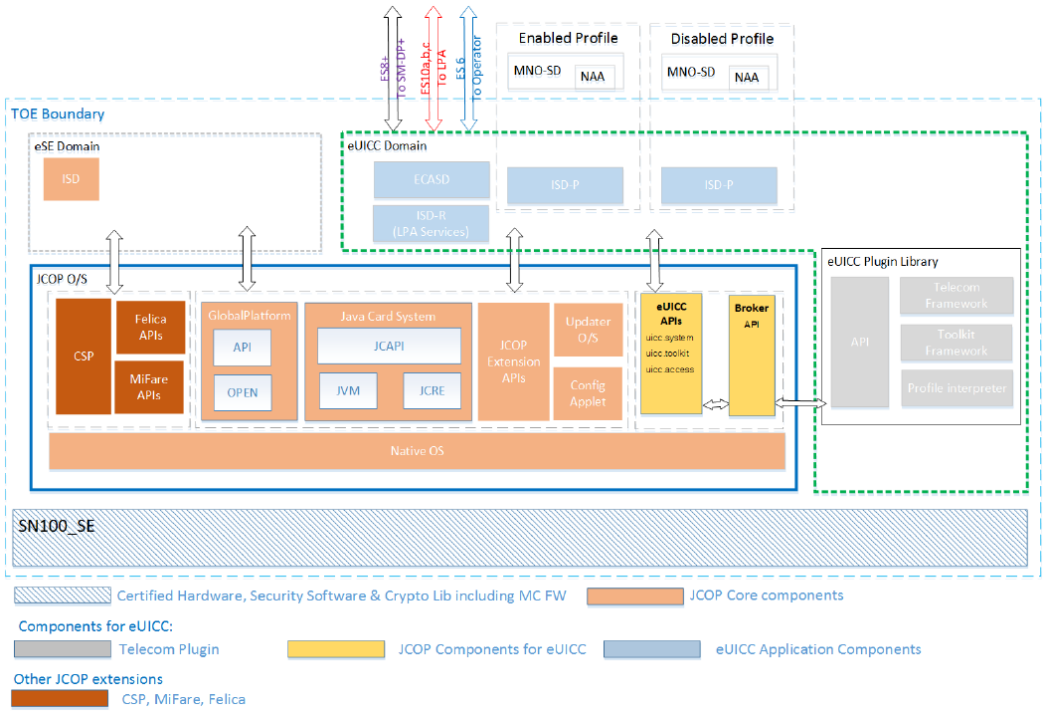
2.4 Architectural Information

The TOE consists of a certified Hardware IC, with Micro Controller Firmware (Boot OS, Factory OS and Flash driver software) and certified security software library consisting of a crypto library and services software. All these parts are depicted in the figure below with the shaded box marked SE100_SE. Since, this TOE is a composite on top of this certified platform, this block is not depicted in more detail.

The Software stack consists of the JCOP Core parts marked with salmon coloured blocks implementing the Native OS, Global platform functionality and the Java Card 3.05 functionality. The TOE also implements a Cryptographic Service Provider marked with an orange coloured block. It implements a number of NXP proprietary features like the JCOP extension APIs for MiFare, Felica, Updater OS and Config applet (note there are no security claims relating to MiFare and Felica).

Furthermore the TOE implements GSMA 'Remote SIM Provisioning Architecture for consumer Devices', referred to as eUICC. The JCOP OS supports the eUICC APIs and uses the Broker API to forward to the eSIM/SIM/UICC/ISIM commands to the eUICC Plugin Library.

The TOE supports two domains, the eSE for the Java Card Secure Element domain and an eUICC domain providing UICC functionality in accordance with the GSMA Specification.



2.5 Documentation

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

Identifier	Version
Guidance components delivered to the customer for JCOP 5.2 R1.01.1	
JCOP 5.2 R1.01.1 User Guidance Manual	2.3
JCOP 5.2 R1.01.1 User Guidance Manual Addendum for SEMS API	1.1
JCOP 5.2 R1.01.1 User Guidance Manual Addendum for CSP API	1.6
Guidance components delivered to the customer for JCOP 5.2 R2.01.1 and JCOP 5.2 R2.02.1	
JCOP 5.2 R2 User Guidance Manual	1.6
JCOP 5.2 R2 User Guidance Manual Addendum for SEMS API	1.2
JCOP 5.2 R2 User Guidance Manual Addendum for CSPAPI	1.2
Guidance components delivered to the customer for JCOP 5.2 R2.03.1	
JCOP 5.2 R2.03.1 User Guidance Manual	1.3
JCOP 5.2 R2.03.1 User Guidance Manual Addendum for SEMS API	1.0
JCOP 5.2 R2.03.1 User Guidance Manual Addendum for CSP API	1.0
Guidance components delivered to the customer for JCOP 5.2 R3.01.1 with plugin 195 and plugin 196	
JCOP 5.2 R3.01.1.User Guidance Manual	1.4
JCOP 5.2 R3.01.1 User Guidance Manual Addendum for SEMS API	1.2

JCOP 5.2 R3.01.1 User Guidance Manual Addendum for CSP API	1.0
Guidance documents (JCOP 5.2 R3.01.1-1 with plugin 197)	
JCOP 5.2 R3.01.1-1 User Guidance Manual	1.2
JCOP 5.2 R3.01.1-1 User Guidance Manual Addendum for SEMS API	1.0
JCOP 5.2 R3.01.1-1 User Guidance Manual Addendum for CSP API	1.0
Guidance documents (JCOP 5.2 R3.01.1-2 with plugin 196)	
JCOP 5.2 R3.01.1-2 User Guidance Manual	1.3
JCOP 5.2 R3.01.1-2 User Guidance Manual Addendum for SEMS API	1.1
JCOP 5.2 R3.01.1-2 User Guidance Manual Addendum for CSP API	1.0

2.6 IT Product Testing

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

2.6.1 Testing approach and depth

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

The TOE was tested both in its physical implementation and using simulator and emulator platforms in order to cover all relevant aspects. During testing, the TOE is identified by its SVN number.

Code coverage analysis was used by NXP to verify overall test completeness. Test benches for the various TOE parts were 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 were analysed. For each tool, the developer has investigated and documented inherent limitations that could 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 were extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

The developer tests witnessed by the evaluators were selected to cover various aspects of the TOE, as well as areas where the code coverage approach has limitations. The selection was designed to focus on TOE parts that differ from previous releases (e.g. eUICC and CSP). The tests were executed in the test environment of the developer.

As the developer functional testing was quite rigorous, the selection was chosen to primarily target eUICC and CSP aspects. For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluator tested on the TOE version to be certified but also on intermediate versions and re-used test results of earlier versions of the TOE. The evaluator provided an analysis to demonstrate that the results of the test cases performed on earlier versions and intermediate versions also hold for this TOE.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.

For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack oriented analysis the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. This analysis was performed according to the attack methods in *[JIL-AM]*. An important source for assurance in this step is the technical report *[HW-ETRfC]* of the underlying platform. The Code Review on this TOE was performed as a delta code review on the predecessor of this TOE JCOP5.1 R1.00.1 certified under *[CR2-221699]*. For each identified Potential Vulnerability identified the evaluator analysed whether the code implementing this potential vulnerability is also part of this TOE version and still exists.

All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate. For the potential vulnerabilities that were identified during JCOP 5.1 R1.00.1 certified under *[CR2-221699]*, the assurance and the test result, providing it was not outdated, was re-used. In cases where the test evidence is outdated, the test was in the meantime redone or a representative test was performed and used to validate the test and provide the assurance. The additional test results, to renew outdated tests or to validate outdated tests originate from the JCOP 5.0 R1.11.0 and JCOP 6.0 R1.13.0 evaluation, certified under *[CR2-195714-CR2]*.

During the most recent, previous re-certification, the vulnerability analysis was refreshed. As a result some representative tests were performed to provide ongoing assurance of penetration testing performed in earlier evaluation of the TOE.

The total test effort expended by the evaluators during the previous re-certification was 12 weeks. During that test campaign, 34% of the total time was spent on Perturbation attacks, 46% on side-channel testing, and 20% on logical tests.

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 developer and evaluator tested the TOE in the following configuration:

- SMB-Mail box Wired Mode, Card Emulation mode, SPI of SN100 to test eSE domain of Secure Element
- ISO7816 T=0/T=1 of SN100 to test eUICC domain of Secure Element

The developer and evaluator tested on the TOE version to be certified but also on intermediate versions of the TOE. The evaluator provided an analysis to demonstrate that the results of the test cases performed on earlier versions and intermediate versions also hold for this TOE. Hence, the test configurations used were deemed to be consistent with those documented in *[ST]*.

During the previous re-certification where the JCOP 5.2 R3 configuration was added, the tests were performed on JCOP 5.2 R3.01.1 and JCOP 5.2 R1.01.1, as well as a predecessor (intermediate) version. Again, the evaluator provided an analysis to demonstrate that the results of the test cases performed on the intermediate versions also hold for the TOE.

For this current recertification representative samples were chosen to assure that the changes being evaluated had not impacted the TOE build nor its configuration

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. 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 extensively reviewed and reused in this certification activity, 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 5.2 on SN100.C58 Secure Element.

The TOE can be identified using the Platform Identifier as explained in Section 1.3 of all the User Guidance Manuals referenced in section 2.5. The term “Platform” is used for the entire TOE.

2.9 Evaluation Results

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

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

Based on the above evaluation results the evaluation lab concluded the NXP JCOP 5.2 on SN100.C58 Secure Element, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 ASE_TSS.2, ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims ’strict’ conformance to the Protection Profile *[PP0104]*, and demonstrable conformance to the Protection Profiles [*PP0099]* and *[PP0100]*.

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 customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

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 5.2 on SN100.C58 Secure Element Security Target, Rev. 3.13, 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
CRT	Chinese Remainder Theorem
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
eUICC	embedded Universal Integrated Circuit Card
GP	Global Platform
GCM	Galois/Counter Mode
GSMA	Groupe Speciale Mobile Association
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MNO	Mobile Network Operators
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
TOE	Target of Evaluation

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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report “NXP JCOP 5.2 SN100.C58 Secure Element” – EAL5+, 23-RPT-056, 2.0, 31 March 2023
[ETRfC]	Evaluation Technical Report for Composition "NXP JCOP 5.2 SN100.C58 Secure Element"– EAL5+, 23-RPT-054, 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 Must be retained for all smartcard-related TOEs
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution) Must be retained for all smartcard-related TOEs
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 22 August 2022
[ST]	NXP JCOP 5.2 on SN100.C58 Secure Element Security Target, Rev. 3.13, 17 March 2023
[ST-lite]	NXP JCOP 5.2 on SN100.C58 Secure Element Security Target Lite, Rev. 3.9, 17 March 2023
[PP0099]	Java Card Protection Profile - Open Configuration, version 3.0.5 (December 2017), published by Oracle, Inc. (BSI-CC-PP-0099-2017)
[PP0100]	Embedded UICC for Consumer Devices, GSMA Association, Version 1.0 0, 5-June-2018, 05 June 2018 (BSI-CC-PP-0100-2018)
[PP0104]	Common Criteria Protection Profile Cryptographic Service Provider version 0.9.8 (BSI-CC-PP-0104-2019)

(This is the end of this report.)