Certification Report

NXP JCOP 5.2 on SN100.C58 Secure Element

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

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

Report number:	**NSCIB-CC-0023577-CR2**
Report version:	**1**
Project number:	**0023577_2**
Author(s):	**Denise Cater**
Date:	**09 July 2020**
Number of pages:	**14**
Number of appendices:	**0**

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

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

TÜVRheinland®
Precisely Right.

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.

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

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.

TÜVRheinland®
Precisely Right.

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 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 originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 10 December 2019. The re-evaluation also took place by Brightsight B.V. and was completed on 08 July 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 second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are the introduction of two new configurations in addition to that certified as per NSCIB-CC-0023577-CR and maintained as per NSCIB –CC-0023577-MA.

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 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 provides sufficient evidence that the TOE meets the EAL5 augmented with ASE_TSS.2, ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5 (+)) 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]*.

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 NXP JCOP 5.2 on SN100.C58 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 (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
	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 TOE	**JCOP5.2**	**R1.01.1**
	Platform ID: N5C2M00261A70600	
	Platform Build ID: 0261A7	
	eUICC plug-in	1.5.129
	JCOP5.2	**R2.01.1**
	Platform ID: N5C2M0029E7D0600	
	Platform Build ID: 029E7D	
	eUICC plug-in	1.5.146
	JCOP5.2	**R2.02.1**
	Platform ID: N5C2M002A62D0600	
	Platform Build ID: 02A62D	
	eUICC plug-in	1.5.148

To ensure secure usage a set of guidance documents is provided together with the NXP JCOP 5.2 on SN100.C58 Secure Element. Details can be found in section “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to 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-key3DES, 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.
- Functionality introduced in R2, for which there are no specific additional security claims:
    - CAT-TP, with limitations as described in the [AGD_UGM] Section 8.1.
    - 5G features as per SIM Alliance 2.3, as in [AGD_UGM] Section 2.4.4 and 8.1.
    - Extension to Global Platform Amendment H, as in [AGD_UGM] Section 3.5.7.
    - CPLC data made available through SystemInfo, as in [AGD_UGM] Section 2.1.3.22.

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 application functionality has not been assessed, only the self-protection of the TSF.

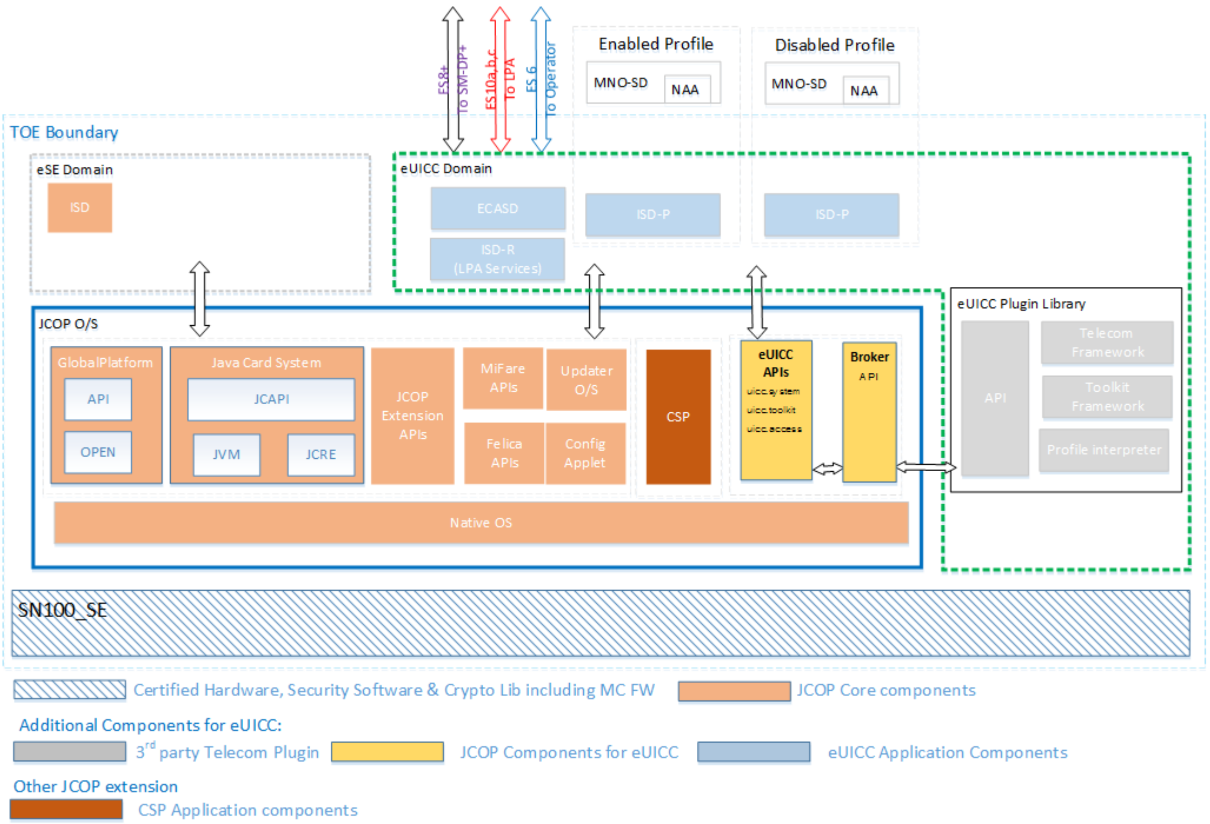
2.4 Architectural Information

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 O/S 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 O/S 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:

JCOP Version	Identifier	Version
JCOP 5.2 R1	[AGD_UGM52R1] JCOP 5.2 R1.01.1 User Guidance Manual	1.8, 2019-10-30
	[AGD_UGMSEMS52R1] JCOP 5.2 R1.01.1 User Guidance Manual Addendum for SEMS API	1.1, 2019-10-17
	[AGD_CSP52R1] JCOP 5.2 R1.01.1 User Guidance Manual Addendum for CSPAPI	1.6, 2019-10-15
JCOP 5.2 R2	[AGD_UGM52R2] JCOP 5.2 R2, User Guidance Manual, doc. no. 608813	1.3, 2020-06-08
	[AGD_UGMSEMS52R2] JCOP 5.2 R2, User Guidance Addendum SEMS, doc. no. 614012	1.2, 2020-06-08
	[AGD_CSP52R2] JCOP 5.2, User Guidance Manual Addendum for CSP API, doc. no. 614112	1.2, 2020-06-08

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 module level. All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. 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.

TOE is 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 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.

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 developer functional testing is 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 were used originate from the JCOP 5.0 R1.11.0 and JCOP 6.0 R1.13.0 certified under *[CR2-195714]*.

The total test effort expended by the evaluators was 14 weeks. During that test time 50% of the total time was spend on Perturbation attacks, 36% on side channel testing and 14% on logical tests.

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]*.

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 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.

It is noted that although the original evaluation NSCIB-CC-0023577 was a "Full-evaluation" of the TOE (not a re-certification), Code review results and test results of the preceding and succeeding versions of the TOE were re-used.

The JCOP5.2 base and JC are a delta from JCOP5.1 on SN100.C48 (*[CR2-221699]*), which is in turn also a delta from the JCOP5.0 on SN100.C25 (*[CR2-195714]*). Test results where applicable are re-used from the earlier certifications. For those test cases where the test results were more than 6 months old, the test results have been revalidated through re-execution of the test case or a representative test case.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE. Site Re-use Reports (STARs) resulting from other evaluations have been utilized).Sites involved in the development and production of the hardware platform were re-used by composition. 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 [AGD_UGM]. The term 'Platform' is being used for the entire TOE. In particular this means that the DF20 tag as returned shall have the value in ASCII format:

JCOP 5.2 Revision	Identifier
R1.01.1	N5C2M00261A70600
R2.01.1	N5C2M0029E7D0600
R2.02.1	N5C2M002A62D0600

.

The identifier of the Plugin, can be verified with the EF10 tag, it shall have the format:

Tag	Len	Description			Value
EF10	3E	Tag	Len	Value Description	
		81	1D	Plugin label	("IDEMIA.eSIM_MERCURY_V2.2+_APP")
					"4944454D49412E6553494D5F4D4552435552595F56322E322B5F415050"
		82	07	eUICC plugin version	R1.01.1 ("1.5.129") "312E352E313239"
					R2.01.1 ("1.5.146") "312E352E313436"
					R2.02.1 ("1.5.148") "312E352E313438"
		83	0F	JCOPX API label	("JCOPX eUICC API") "4A434F50582065554943432041504"
		84	03	JCOPX API version	R1.01.1: ("5.2") "352E32" R2.01.1 and R2.02.1:

					("5.3") "352E33"

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 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 augmented with 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 Profiles *[PP0099]*, *[PP0100]* and *[PP0104]*.

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.

3 Security Target

The NXP JCOP 5.2 on SN100.C58 Secure Element Security Target, v2.2, 11 June 2020 *[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:

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

TÜVRheinland®
Precisely Right.

5 Bibliography

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

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
[CR2-195714]	Certification Report NXP JCOP 5.0 on SN100.C25 Secure Element, NSCIB-CC-195714-CR, version 2.0, 6 December 2019.
[CR2-221699]	Certification Report SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48/C58, NSCIB-CC-221699-CR2, 25 November 2019.
[ETR]	Evaluation Technical Report NXP JCOP 5.2 on SN100.C58 Secure Element on SN100.C58" – EAL5+, 19-RPT-537, Version 10.0, 07 July 2020.
[ETRfC]	ETR for Composition "JCOP 5.2 Javacard with eUICC and CSP extension" – EAL5+, 19-RPT-939, Version 9.0, 06 July 2020.
[HW-CERT]	Certification Report SN100 Series - Secure Element with Crypto Library SN100_SE B2.1 C25/C48/C58, NSCIB-CC-174263-CR2, version 1.0, 18-09-2019.
[HW-ETRfC]	ETR for Composition SN100 Series – Secure Element with crypto library B2.1 C25, C48 and C58, 19-RPT-596, v7.0, 09-09-2019.
[HW-ST]	Security Target, SN100 Series – Secure Element with Crypto Library, Rev. 3.3.
[JIL-AM]	JIL, Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.3, April 2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[NSI-11]	NSCIB Scheme Instruction 11 Remaining strength of cryptographic implementations, version 1.1, 1 October 2017.
[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, GMSA Association, Version 1.0 05-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).
[ST]	NXP JCOP 5.2 on SN100.C58 Secure Element Security Target, v2.2, 11 June 2020.
[ST-lite]	NXP JCOP 5.2 on SN100.C58 Secure Element Security Target Lite, v2.0, 12 June 2020.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).