

Certification Report

NXP JCOP 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1

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

Evaluation facility: **SGS Brightsight B.V.**
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0428888-CR2**

Report version: **1**

Project number: **0428888_2**

Author(s): **Wim Ton**

Date: **06 December 2022**

Number of pages: **19**

Number of appendices: **0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	7
2.1 Identification of Target of Evaluation	7
2.2 Security Policy	9
2.3 Assumptions and Clarification of Scope	10
2.3.1 Assumptions	10
2.3.2 Clarification of scope	10
2.4 Architectural Information	10
2.5 Documentation	11
2.6 IT Product Testing	12
2.6.1 Testing approach and depth	12
2.6.2 Repeated Developer Tests	Error! Bookmark not defined.
2.6.3 Evaluator-defined Tests	Error! Bookmark not defined.
2.6.4 Independent penetration testing	13
2.6.5 Test configuration	13
2.6.6 Test results	13
2.7 Reused Evaluation Results	14
2.8 Evaluated Configuration	14
2.9 Evaluation Results	16
2.10 Comments/Recommendations	16
3 Security Target	17
4 Definitions	17
5 Bibliography	19

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 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, 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, 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 authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

The 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 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1. The developer of the NXP JCOP 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1 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 type is software deployed on a certified hardware platform (including hardware, firmware and crypto library), called the micro-controller. The TOE software stack, JCOP 6.2, is a patchable 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 software stack creates 2 separate domains, providing a familiar Java Card Secure Element domain (eSE) and an eUICC domain providing eUICC functionality in accordance with the GSMA Specification.

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 the currently enabled MNO profile. The CSP part is a Cryptographic Service Provider.

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 02 November 2021. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 29 November 2022 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:

- Inclusion of the new version, JCOP 6.2 R2.01.1, in which the eUICC plugin is fully integrated into the TOE and a number of augmentation packages (which are optional in Java Card 3.1) are added namely: Sensitive Result, Monotonic Counters, Cryptographic Certificate Management, Key Derivation Functions and System Time. In addition, support of the hardware SN220 B0.1 C37[HW-CERT] was included for JCOP 6.2 R2.01.1
- Inclusion of versions R1.02.1 and R1.02.1-1, which contain bug-fixes of the eUICC
- For all TOE versions the claimed PP version is changed from JC 3.05 [BSI-CC-PP-0099-2017] to JC 3.1 [BSI-CC-PP-0099-V2-2020].
- Addition of a new wafer fab (SMIC) and transfer of the NXP IT infrastructure site from Hamburg to Eindhoven

The security evaluation reused 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 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1, 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 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1 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) 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).

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

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).

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. Note that the certification results apply only 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 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

	Name	Version
Hardware (platform)	IC Hardware	B0.1
Data Configuration (C13 platform)	Factory Page	21043
	System Page Common	21031
	BootOS Patch	9.0.3 PL1 v1
Software (C13 platform)	Factory OS	9.0.4
	Boot OS	9.0.3
	Flash Driver Software:	9.0.2
	Services Software	9.17.4
	Crypto Library	2.2.0
Software	JCOP 6.2 on SN220.C13 R1.01.1 with plugin version 1.6.016	
	JCOP6.2 OS, native applications, OS Update Component, eUICC component and CSP component	R1.01.1
	eUICC plug-in	1.6.016

Table 1 R1.01.1 components

	Name	Version
Hardware (platform)	IC Hardware	B0.1
Data Configuration (C13 platform)	Factory Page	21043
	System Page Common	21031
	BootOS Patch	9.0.3 PL1 v1
Software (C13 platform)	Factory OS	9.0.4
	Boot OS	9.0.3
	Flash Driver Software:	9.0.2
	Services Software	9.17.4
	Crypto Library	2.2.0

Software	JCOP 6.2 on SN220.C13 R1.02.1 with plugin version 1.6.019	
	JCOP6.2 OS, native applications, OS Update Component, eUICC component and CSP component	R1.02.1
	eUICC plug-in	1.6.019

Table 2 R1.02.1 components

	Name	Version
Hardware (platform)	IC Hardware	B0.1
Data Configuration (C13 platform)	Factory Page	21043
	System Page Common	21031
	BootOS Patch	9.0.3 PL1 v1
Software (C13 platform)	Factory OS	9.0.4
	Boot OS	9.0.3
	Flash Driver Software:	9.0.2
	Services Software	9.17.4
	Crypto Library	2.2.0
Software	JCOP 6.2 on SN220.C13 R1.01.1 with plugin version 1.6.019	
	JCOP6.2 OS, native applications, OS Update Component, eUICC component and CSP component	R1.01.1
	eUICC plug-in	1.6.019
	Patch ID	01.00

Table 3 R1.02.1-1 components

	Name	Version
Hardware (platform)	IC Hardware	B0.1
Data Configuration (C37 platform)	Factory Page	21043
	System Page Common	21031
	BootOS Patch	10.0.2 PL1 v1
Software (C37 platform)	Factory OS	10.0.2
	Boot OS	10.0.2
	Flash Driver Software:	10.0.0

	Services Software	10.17.6
	Crypto Library	2.3.1
Software	JCOP 6.2 on SN220.C37 R2.01.1	
	JCOP6.2 OS, native applications, OS Update Component, eUICC component, and CSP component	R2.01.1

Table 4 R2.01.1 components

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1. 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, XTS, 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
- Versions R1.01.1, R1.02.1, and R1.02.1-1 support Java Card 3.0.5 functionality
- Version R2.01.1 Supports Java Card 3.1 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' version 2.2.1 [29] and v2.2.2 [30]
- 5G features as per SIM Alliance 2.3 – no security functionality is claimed
- 5th Logical Channel
- 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: JCOP6.2 OS includes a Config Applet that can be used for configuration of the TOE.

- OS Update Component: Proprietary functionality that can update JCOP6.2 OS or UpdaterOS: UAI update component: Proprietary functionality that can update the JCOP6.2 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

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.

2.4 Architectural Information

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 logical architecture, originating from the Security Target [ST] for the JCOP 6.2 R1.x configurations of the TOE can be depicted as follows:

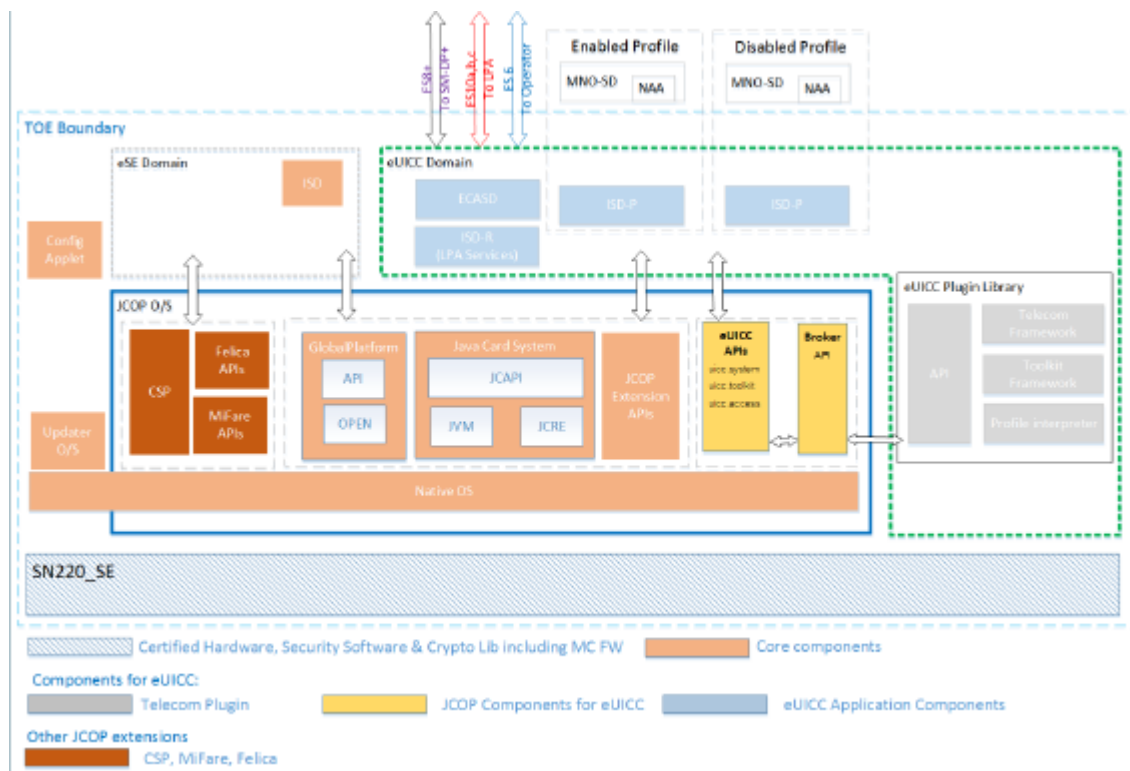


Figure 1. Logical architecture of the TOE JCOP 6.2 R1.X

The logical architecture, originating from the Security Target [ST] for the JCOP 6.2 R2.x configuration of the TOE can be depicted as follows:

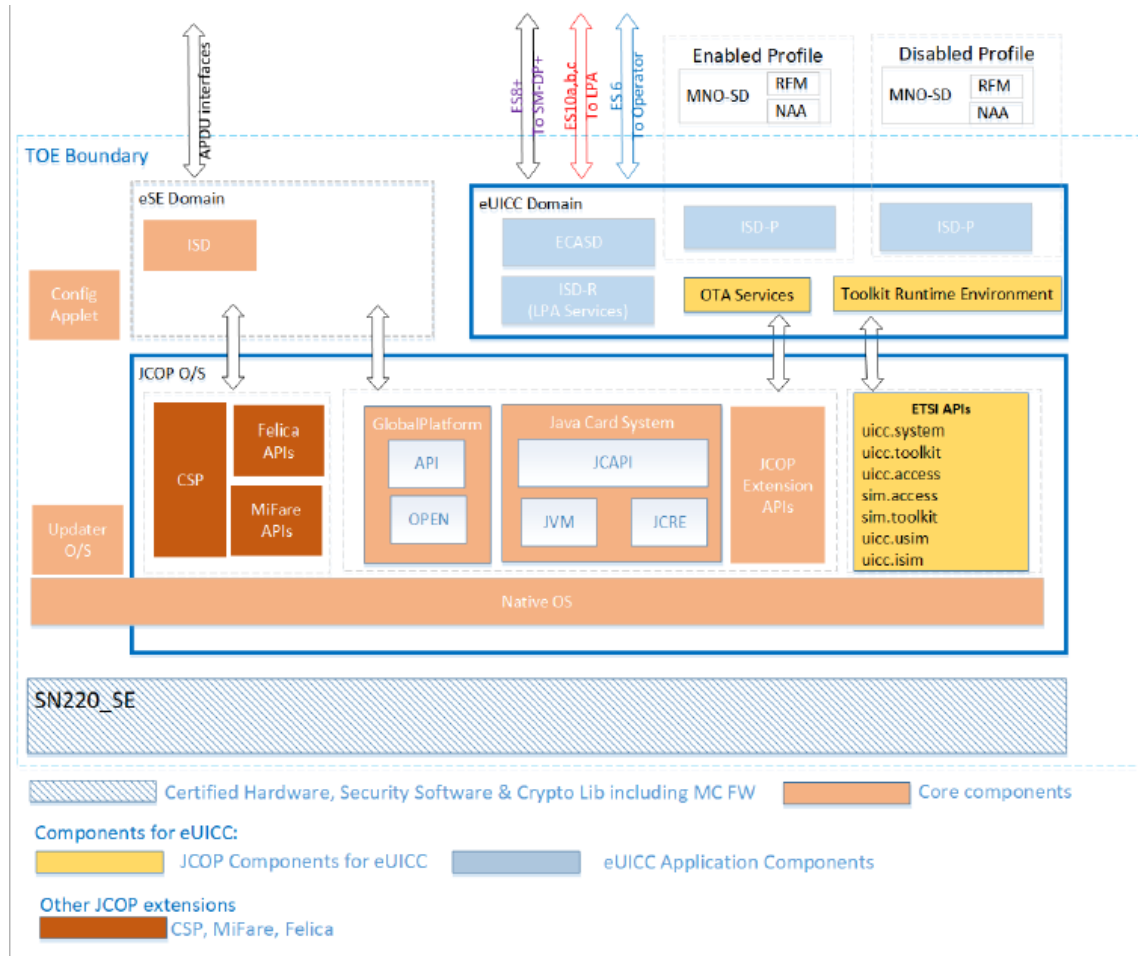


Figure 2. Logical architecture of the TOE JCOP 6.2 R2.X

2.5 Documentation

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

Identifier	Version
JCOP 6.2 R1.01.1, User Guidance Manual	Rev. 1.7
JCOP 6.2 R1.01.1, AMD I SEMS Application User Manual Addendum	Rev 1.0
JCOP 6.2 R1.01.1, CSP User Manual Addendum	Rev. 1.0
JCOP 6.2 R1.01.1, eUICC Profile Package Interpreter Guide, Addendum	Rev. 1.1

Table 5 R1.01.1 Guidance

Identifier	Version
JCOP 6.2 R1.02.1, User Guidance Manual	Rev. 1.2

JCOP 6.2 R1.02.1, AMD I SEMS Application User Manual Addendum	Rev 1.1
JCOP 6.2 R1.02.1, CSP User Manual Addendum	Rev. 1.1
JCOP 6.2 R1, eUICC Profile Package Interpreter Guide, Addendum	Rev. 1.2

Table 6 R1.02.1 and R1.02.1-1 Guidance

Identifier	Version
JCOP 6.2 R2.01.1, User Guidance Manual	Rev. 1.2
JCOP 6.2 R2.01.1, AMD I SEMS Application User Manual Addendum	Rev 1.0
JCOP 6.2 R2.01.1, CSP User Manual Addendum	Rev. 1.0

Table 7 R2.01.1 Guidance (The eUICC is integrated in the UGM)

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 TOE is tested thoroughly by the developer, covering all security functions and aspects of the TSF. The developer uses a set of industry standard and proprietary test suites and tools. The TOE is tested both in its physical implementation and using simulator and emulator platforms in order to cover all relevant aspects

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 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, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

During the baseline evaluation 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 tests were executed in the test environment of the developer. 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 tests performed on earlier and intermediate versions also hold on this TOE.

During the renewal, the evaluator analysis showed that the test approach has not been changed between the base evaluation and the renewal evaluation. It is noted that the ITSEF has already seen

large numbers of similar TOEs that have been testing using this approach. It ITSEF expects that by renewing this part of the ATE_IND will result in new insights or a different conclusion from the base-evaluation.

2.6.2 Independent penetration testing

A methodical analysis performed was conducted along the following steps:

When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities could 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 was performed on the TOE. During this attack oriented analysis the protection of the TOE 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 methods in [JIL-AM]. An important source for assurance in this step was the technical report [ETRfC_HW] of the underlying platform.

All potential vulnerabilities were 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 were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate

In the baseline evaluation the total test effort expended by the evaluators for the original evaluation was 25 weeks. During that test campaign, 36% of the total time was spent on Perturbation attacks, 22% on side-channel testing, and 41% on logical tests.

During this renewal evaluation the potential vulnerabilities were re-assessed and new potential vulnerabilities were added. The total test effort consists of 31% of the total time spent on Perturbation attacks, 36% on side channel testing and 33% on logical tests. An effort of 9 weeks was spent on testing for the renewal.

2.6.3 Test configuration

The evaluator tested the TOE in the configuration as stated in the [ST] using the following interfaces:

- SMB-Mail box Wired Mode, Card Emulation mode, SPI-REE and I2C interfaces of SN220 to test the eSE domain of Secure Element
- ISO7816 T=0/T=1 of SN220 to test the eUICC domain of Secure Element

This is the same configuration as used by the developer.

It is noted that for the baseline evaluation the evaluator assessed the test results on the JCOP 6.2 R1.01.1. For this renewal the evaluator assessed the test results on the JCOP 6.2 R2.01.1.

No sample preparation was required for the perturbation tests.

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).

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 and penetration testing has been renewed.

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition. The list of site security certificates was updated to reflect moving the NXP IT from Hamburg to Eindhoven.

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 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1.

The TOE can be identified using the Platform Identifier, the Identifier of the PlugIn and the Identifier of the patch as explained in Section 1.4 of [ST] and 1.3 of the [UGM]. The term 'Platform' is being used for the entire TOE as it has been developed by NXP. In particular this means that the DF20 tag as returned shall have the value in ASCII format as outlined in the following table:

TOE Version	Tag DF20 Platform Build ID
JCOP 6.2 R1.01.1	N5D2M003245A0600
JCOP 6.2 R1.02.1 and JCOP 6.2 R1.02.1-1	N5D2M00372520600
JCOP 6.2 R2.01.1	N5D2M003D0430600

Table 8 TOE version tag

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	NXP_eSIM_APP "4E58505F6553494D5F415050"
		82	07	eUICC plugin version	"1.6.016" "312E362E303136"
		83	0F	JCOPX API label	"JCOPX eUICC API" "4A434F505820655549434320415049"
		84	03	JCOPX API version	"6.0" "362E30"

Table 9 JCOP 6.2 R1.01.1 Plugin version

Tag	Len	Description			Value
EF10	3E	Tag	Len	Value Description	

		81	1 D	Plugin label	NXP_eSIM_APP" "4E58505F6553494D5F415050
		82	0 7	eUICC plugin version	"1.6.019" "312E362E303139"
		83	0 F	JCOPX API label	"JCOPX eUICC API" "4A434F505820655549434320415049"
		84	0 3	JCOPX API version	"6.0" "362E30"

Table 10 JCOP 6.2 R1.02.1 and JCOP 6.2 R1.02.1-1 Plugin version

The identifier of the Patch, to make a distinction between JCOP 6.2 R1.02.1 and JCOP R1.02.1 can be verified with patch version query as explained in section 4.7 of the TOE User Guidance Manuals, as specified in the *Documentation* section above. .

Product	Value	Description
R1.02.1	FE	Tag 0xFE
	0A	Length
	DF 4C	Tag DF 4C
	07	Length 0x07
	90 00	Tag 0x90, Length 0x00
	92 03	Tag 0x92, Length 0x03
	04 01 02	MIFARE Version
R1.02.1-1	FE	Tag 0xFE
	11	Length 0x11
	DF 4C	Tag DF 4C
	0E	Length 0x0E
	90 07	Tag 0x90, Length 0x07
	A0	Sub Tag - Patch Version
	05	Length 0x05
	01 00	Patch ID V01.00
	01	Java Patch Status - STATEINFO_ACTIVE (see also Table 4.39)
	A5	Native Patch Status - STATEINFO_NOT_AVAILABLE
	A5	ROM Patch Status - STATEINFO_NOT_AVAILABLE
	92 03	Tag 0x92, Length 0x03
	04 01 02	MIFARE Version

Table 11 JCOP 6.2 R1.02.1 and JCOP 6.2 R1.02.1-1 Patch version

The authenticity of the TOE is checked by following the procedure explained in Section 1.3 of the TOE User Guidance Manuals, as specified in the *Documentation* section above, along with the challenge-response authenticity check as explained in Section 1.3.1.1 of TOE User Guidance Manuals.

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 [ETRF] 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 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 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 Java Card Protection Profile [PP_JC] and eUICC for Consumer Devices Protection Profile (Base-PP only) [PP_eUICC]. The Security Target also claims strict conformance to the Cryptographic Service Provider Protection Profile [PP_CSP].

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: OSCCA, MIFARE, and Felica, which are out of scope as there are no security claims relating to these.

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).

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.

3 Security Target

The NXP JCOP 6.2 on SN220 Secure Element, Security target, 1.8, 24 November 2022 [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
API	Application Programme Interface
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CRT	Chinese Remainder Theorem
CSP	Cryptographic Service Provider
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
eUICC	Embedded Universal Integrated Circuit Card
GCM	Galois Counter Mode
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MITM	Man-in-the-Middle
MNO	Mobile Network Operator
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm

SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
SM	Secure Messaging
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
[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 6.2 on SN220 Secure Element” – EAL5+, 22-RPT-1262, 2.0, 24 November 2022
[ETRFc]	Evaluation Technical Report for Composition “NXP JCOP 6.2 on SN220 Secure Element” – EAL5+, 22-RPT-1263, 2.0, 24 November 2022
[HW-CERT]	Secure Element with Crypto Library B0.1 C13/C37, CC-22-0258298, 1.0, 21 Oct 2021
[HW-ETRFc]	ETR for composite evaluation SN220 Series - Secure Element with Crypto Library B0.1 C13/C37, 20210539-D4, 1.6, 6 October 2022
[HW-ST]	SN220 Series - Secure Element with Crypto Library, v1.5, 29 September 2022
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 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 2.5, 28 March 2019
[PP_CSP]	Common Criteria Protection Profile Cryptographic Service Provider, 19 February 2019, version 0.9.8, BSI-CC-PP-0104-2019
[PP_eUICC]	GSMA. Embedded UICC for Consumer Devices, version 1.0, 05, June 2018, BSI-CC-PP-0100-2018
[PP_JC]	Java card protection profile - open configuration, version 3.1, April 2020, BSI-CC-PP-0099-v2-2020
[ST]	NXP JCOP 6.2 on SN220 Secure Element, Security target, 1.8, 24 November 2022
[ST-lite]	NXP JCOP 6.2 on SN220 Secure Element, Security target Lite, 1.8, 24 November 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)