Certification Report

NXP JCOP 6.2 on SN220 Secure Element, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1

Sponsor and developer:	***NXP Semiconductors GmbH*** **Beiersdorfstraße 12** **22529 Hamburg** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300174-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300174-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**17 June 2024**
Number of pages:	**15**
Number of appendices:	**0**

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

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.

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

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 6.2 on SN220 Secure Element, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1. The developer of the NXP JCOP 6.2 on SN220 Secure Element, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1 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 was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 29 November 2022 (CC-22-0428888). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 17 June 2024 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]*.

This third issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are was the addition of JCOP 6.2 R5.01.1.

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, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1, 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, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1 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), ASE_TSS.2 (TOE summary specification with architectural design summary), AVA_VAN.5 (Advanced methodical vulnerability analysis) and ALC_FLR.1 (Basic flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP 6.2 on SN220 Secure Element, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1 from NXP Semiconductors GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components (on C13 certified HW configuration):

Delivery item type	Identifier	Version
Hardware	IC Hardware	B0.1
Data Configuration (platform C13)	Factory Page	21043
	System Page Common	21031
	BootOS Patch	9.0.3 PL1 v1
Software (platform C13)	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 R1.01.1 on SN220.C13 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
	JCOP 6.2 R1.02.1 on SN220.C13 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
	JCOP 6.2 R1.02.1-1 on SN220.C13 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
	Patch ID	01.00
	JCOP 6.2 R1.02.1-2 on SN220.C13 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
	Patch ID	01.00, 01.01, 01.02

The TOE is comprised of the following main components (on C37 certified HW configuration):

Delivery item type	Identifier	Version
Hardware	IC Hardware	B0.1
Data Configuration (platform C37)	Factory Page	21043
	System Page Common	21031
	BootOS Patch	10.0.2 PL1 v1
Software (platform C37)	Factory OS	10.0.2
	Boot OS	10.0.2
	Flash Driver Software	10.0.2
	Services Software	10.17.6
	Crypto Library	2.3.1
Software	**JCOP 6.2 R2.01.1 on SN220.C37 with plugin version N.A**	
	JCOP6.2 OS, native applications, OS Update Component, eUICC component and CSP component	R2.01.1
	eUICC plug-in	Plugin fully integrated
	JCOP 6.2 R5.01.1 on SN220.C37 with plugin version N.A	
	JCOP6.2 OS, native applications, OS Update Component, eUICC component and CSP component	R5.01.1
	eUICC plug-in	Plugin fully integrated

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP 6.2 on SN220 Secure Element, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1. 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 provides the following security functionality:

- 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.
- GlobalPlatform 2.3 functionality including Amendments A,B,C,D,E,F,H and I and is;
    - compliant with the Common Implementation Configuration;

- 5th Logical Channel;
- Cryptographic Service Provider (CSP) features;
- NXP Proprietary 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 JCOP 6.2 OS or Updater OS;
    - 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.
- JCOP 6.2 R1.01.1, JCOP 6.2 R1.02.1, JCOP 6.2 R1.02.1-1 and JCOP 6.2 R1.02.1-2 support:
    - Java Card 3.0.5 functionality;
    - GSMA ’Remote SIM Provisioning Architecture for consumer Devices’ version 2.2.1 and v2.2.2.
- JCOP 6.2 R2.01.1 Supports:
    - Java Card 3.1 functionality;
    - GSMA ’Remote SIM Provisioning Architecture for consumer Devices’ v2.2.2.
- JCOP 6.2 R5.01.1 Supports:
    - Java Card 3.1 functionality;
    - GSMA ’Remote SIM Provisioning Architecture for consumer Devices’ v2.3;
    - Cryptographic algorithms and functionality:
        - SHA-3 hash algorithm;
    - Java Card functionality:
        - Korean Seed FPAD support for Java Card;
        - AC Reset on eUICC domain via signed APDU;
        - Allow support of dual package load scenario via JCRE loader to handle multiple CAP downloads in parallel;
    - NXP Proprietary Functionality:
        - SN220 supports CL over eUICC;
        - SWP feature support - JCOP allows the Manage LSI Assign SWP command;
        - AID routing table is updated based on CLPP on the active profile in eUICC;
        - NFC identifies current active eSIM profile through CL parameters from JCOP;
        - Patching support over UART T0.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

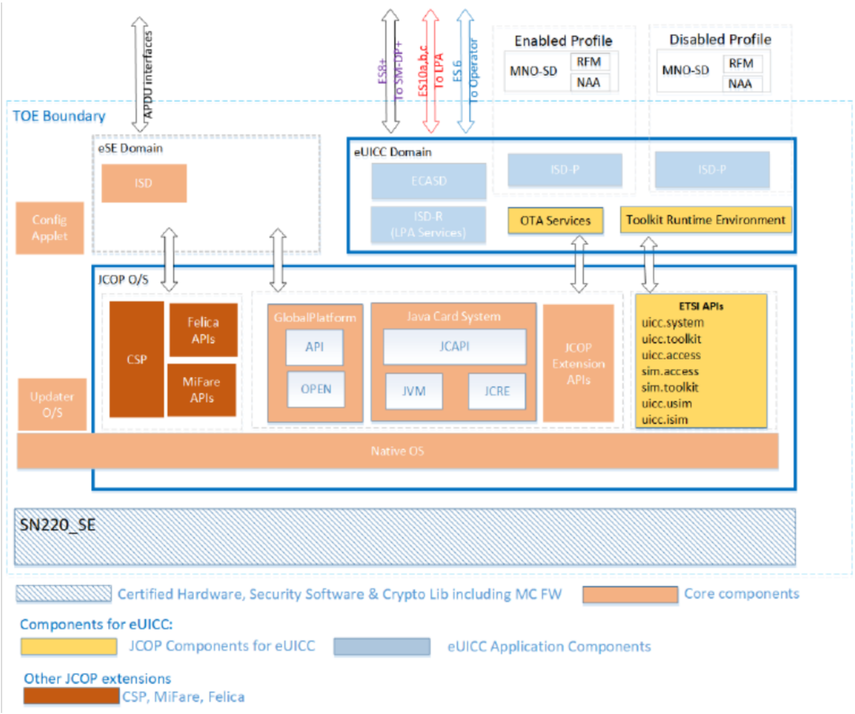
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 2.4.3 of the *[ST]*.

2.3.2 Clarification of scope

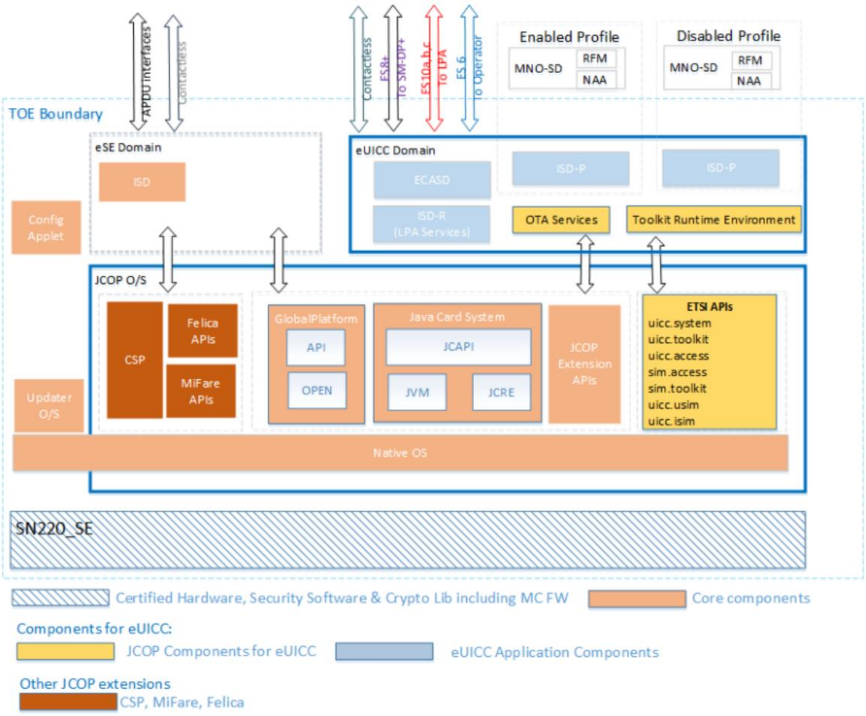
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

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



The logical architecture, originating from the Security Target [ST] for the JCOP 6.2 R5.x configuration of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer for JCOP 6.2 R1.01.1:

Identifier	Version
JCOP 6.2 R1.01.1, User Guidance Manual, User documentation, dated 30 September 2022	Rev. 1.7
JCOP 6.2 R1.01.1, AMD I SEMS Application User Manual Addendum, User documentation, dated 16 June 2021	Rev 1.0
JCOP 6.2 R1.01.1, CSP User Manual Addendum, dated 16 June 2021	Rev 1.0
JCOP 6.2 R1.01.1, eUICC Profile Package Interpreter Guide, Addendum, dated 30 July 2021	Rev 1.1

The following documentation is provided with the product by the developer to the customer for JCOP 6.2 R1.02.1, JCOP 6.2 R1.02.1-1 and JCOP 6.2 R1.02.1-2:

Identifier	Version
JCOP 6.2 R1.02.1, User Guidance Manual, User documentation, dated 13 March 2022	Rev. 1.3
JCOP 6.2 R1.02.1, AMD I SEMS Application User Manual Addendum, User documentation, dated 03 March 2022	Rev. 1.1
JCOP 6.2 R1.02.1, CSP User Manual Addendum, dated 03 March 2022	Rev. 1.1
JCOP 6.2 R1.02.1, eUICC Profile Package Interpreter Guide, Addendum, dated 03 February 2022	Rev. 1.2

The following documentation is provided with the product by the developer to the customer for JCOP 6.2 R2.01.1:

Identifier	Version
JCOP 6.2 R2.01.1, User Guidance Manual, User documentation, dated 30 September 2022	Rev. 1.2
JCOP 6.2 R2.01.1, AMD I SEMS Application User Manual Addendum, User documentation, dated 05 August 2022	Rev. 1.0
JCOP 6.2 R2.01.1, CSP User Manual Addendum, dated 05 August 2022	Rev. 1.0

The following documentation is provided with the product by the developer to the customer for JCOP 6.2 R5.01.1:

Identifier	Version
NXP JCOP 6.2 R5.01.1, User Guidance Manual, dated 16 February 2024	Rev. 1.3
NXP JCOP 6.2 R5.01.1, AMD I SEMS Application User Manual Addendum, dated 30 January 2024	Rev. 1.1
NXP JCOP 6.2 R5.01.1, CSP User Manual Addendum, dated 30 January 2024	Rev. 1.1

2.6 IT Product Testing

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

2.6.1 Testing approach and depth

The 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 underlying hardware test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

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. For this analysis will be performed according to the attack methods in [JIL-AM]. An important source for assurance in this step is the technical report [ETRfC_HW] of the underlying platform.
- 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.

The total test effort expended by the evaluators was six weeks. During that test campaign, 33% of the total time was spent on Perturbation attacks, 17% on side-channel testing, and 50% on logical tests.

2.6.3 Test configuration

The following TOE configuration was used for testing:

- JCOP 6.2 R5.01.1

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.

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.

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, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1.

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 6.2 on SN220 Secure Element, versions R1.01.1, R1.02.1, R1.02.1-1, R1.02.1-2, R2.01.1, R5.01.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2, ASE_TSS.2, AVA_VAN.5 and ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

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

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 6.2 on SN220 Secure Element Security Target, Rev. 2.0.7, Dated 14 June 2024 *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
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 6.2 on SN220 Secure Element" - EAL5+, 24-RPT-448, Version 4.0, Dated 14 June 2024

[ETRfC] Evaluation Technical Report for Composition NXP JCOP 6.2 on SN220 Secure Element – EAL5+, 24-RPT-447, Version 5.0, Dated 17 June 2024

[HW-CERT] Certification Report SN220 Series - Secure Element with Crypto Library B0.1 C13/C37, version 1, dated 10 May 2024, registered under the reference NSCIB-CC-2300181-01-CR

[HW-ETRfC] ETR for composite evaluation SN220 Series - Secure Element with Crypto Library B0.1 C13/C37, 20230432_V-D4, Version 1.1, Dated 18 April 2024

[HW-ST] SN220 Series - Secure Element with Crypto Library Security Target, Rev 1.6, Dated 12 April 2024

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[PP0099] Protection Profile Java Card System – Open Configuration Protection Profile, Version 3.1, April 2020, registered under the reference BSI-CC-PP-0099-v2-2020

[PP0100] Embedded UICC for Consumer Devices Protection Profile, GSMA Association, version 1.0 05 June 2018 registered under the reference BSI-CC-PP-0100-2018

[PP0104] Common Criteria Protection Profile Cryptographic Service Provider version 0.9.8 registered under the reference BSI-CC- PP-0104-2019

[ST] NXP JCOP 6.2 on SN220 Secure Element Security Target, Rev. 2.0.7, Dated 14 June 2024

[ST-lite] NXP JCOP 6.2 on SN220 Secure Element Security Target Lite, Rev.2.0.7., dated 14 June 2024

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

(This is the end of this report.)