**TrustCB B.V.**

# Certification Report

## NXP JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210"

| | |
|---|---|
| Sponsor and developer: | **NXP Semiconductors**<br>**High Tech Campus 60**<br>**5656 AG Eindhoven**<br>**the Netherlands** |
| Evaluation facility: | **Riscure B.V.**<br>**Delftechpark 49**<br>**2628 XJ Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-2300044-02-CR** |
| Report version: | **1** |
| Project number: | NSCIB-**2300044-02** |
| Author(s): | **Haico Haak** |
| Date: | **16-October 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 JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210". The developer of the NXP JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210" is NXP Semiconductors located in Eindhoven, the Netherlands 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 consists of an embedded Secure Element SN200 SE with Crypto Library loaded with a Java Card operating system image JCOP6.x. The embedded secure element is based on a Flash-based secure microcontroller platform, based on an ARM SC300 core along with cryptographic hardware coprocessors. The eSE includes Security Software, composed of Services Software and a Crypto Library, that is used by the Security IC Embedded Software (the Java Card operating system).

The operating system is a Java Card operating system supporting GlobalPlatform specifications for card management. This operating system image is loaded in the flash memory of the embedded SE, together with an updated OS image. The update OS is a component which facilitates the secure update of the TOE.

The Java Card operating system provides a runtime environment with APIs for Java Card applications. These applications are not part of the TOE.

The usage of the TOE is focused on security critical applications in small form factors. One main usage scenario is the use in mobile phones, which can use the TOE to enable mobile payment or mobile ticketing with the phone based on the security of the TOE.

The hardware of the Micro Controller already protects against physical attacks by applying various sensors to detect manipulations and by processing data in ways which protect against leakage of data by side channel analysis. With the software stack the TOE provides many cryptographic primitives for encryption, decryption, signature generation, signature verification, key generation, secure management of PINs and secure storage of confidential data (e.g. keys, PINs). Also the software stack implements several countermeasures to protect the TOE against attacks.

The TOE was evaluated initially by Riscure B.V. located in Delft, The Netherlands and was certified on 09-10-2023. The re-evaluation of the TOE has also been conducted by Riscure B.V, and was completed on 16 October 2024 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:

• Two new JCOP variants are added:

- JCOP 6.6 R1.06.0 "SN200"

- JCOP 6.6 R1.06.0 "SN210"

• Minor functionality additions and deprecations

• Improve security hardening

• Minor bugfixes

• Updated user guidance

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 JCOP6.x on SN200.C04 Secure

Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210", 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 JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210" 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. ALC_DVS.2 (Sufficiency of security measures), AVA_VAN.5 (Advanced methodical vulnerability analysis), ASE_TSS.2 (TOE summary specification with architectural design summary), and ALC_FLR.1 (Basic flaw remediation).

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

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

---

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

# 2 Certification Results

## 2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210" from NXP Semiconductors located in Eindhoven, the Netherlands.

The TOE is comprised of the following main components:

| Delivery item type | Identifier |
|---|---|
| Product | NXP SN200.C04 Secure Element in "SN200" and "SN210" configuration with Crypto Library and including software (JCOP6x OS, native applications and OS Update Component) that is identified by Platform ID and Device Type. |

The TOE has 9 versions:

- JCOP6.0 R1.13.0 "SN200" (UART as NFC interface)
- JCOP6.1 R1.04.0 "SN200" (UART as NFC interface)
- JCOP6.1 R1.04.0 "SN210" (SPMI as NFC interface)
- JCOP6.4 R1.06.0 "SN200" (UART as NFC interface)
- JCOP6.4 R1.06.0 "SN210" (SPMI as NFC interface)
- JCOP6.5 R1.04.0 "SN200" (UART as NFC interface)
- JCOP6.5 R1.04.0 "SN210" (SPMI as NFC interface)
- JCOP6.6 R1.06.0 "SN200" (UART as NFC interface)
- JCOP6.6 R1.06.0 "SN210" (SPMI as NFC interface)

Note: "SN200" and "SN210" both identify the same hardware platform with one unique certificate.

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210". For details, see section 2.5 "Documentation" of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.

## 2.2 Security Policy

The usage of the TOE is focused on security critical applications in small form factors where an attacker potentially has direct physical access to the TOE. One main usage scenario is the use in mobile phones, which can use the TOE to enable mobile payment or mobile ticketing with the phone based on the security of the TOE.

The TOE provides a variety of security features. The hardware of the Micro Controller already protects against physical attacks by applying various sensors to detect manipulations and by processing data in ways which protect against leakage of data by side channel analysis.

With the software stack the TOE provides many cryptographic primitives for encryption, decryption, signature generation, signature verification, key generation, secure management of PINs and secure storage of confidential data (e.g. keys, PINs). Also, the software stack implements several countermeasures to protect the TOE against attacks.

For a detailed description of the collaboration of the base TOE components and JCOP operating system refer to the TOE summary specification in the security target and the security target of the base TOE.

## 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 Operating System embedded on an NXP SN200 Series Secure Element. The SN200 Series Secure Element is a product which integrates an NFC Controller and a Secure micro-controller, comparable to a smart card controller, on a single die. It also provides Power Management and IC specific software services.

The component of the SN200 on which the TOE executes is the embedded Secure Element (eSE), abbreviated to SN200_SE. The eSE and associated IC Dedicated Software is Common Criteria certified to EAL6. The IC dedicated software includes IC Dedicated Support Software (Boot O/S, Factory O/S, Flash Driver Software) and Security Software (Crypto Library and Services Software, providing Flash memory support functionality such as wear-levelling and anti-tear protection). Figure 1 provides an overview of the TOE and the communication Interfaces.

"SN200" and "SN210" both identify the same hardware platform with one unique certificate but in two different configurations. "SN210" denomination is used to distinguish from "SN200" in the way the NFC controller communicates with the Host Processor. On the "SN200", the NFC Controller communicates with the Host Processor though an UART interface. On the "SN210", the NFC Controller communicates with the Host Processor through a SPMI interface. This distinction does not affect the TOE (see Figure 1) since the UART/SPMI interfaces are outside the scope of the TOE. Please note, only SN200 denomination will be used in the rest of this certification report.
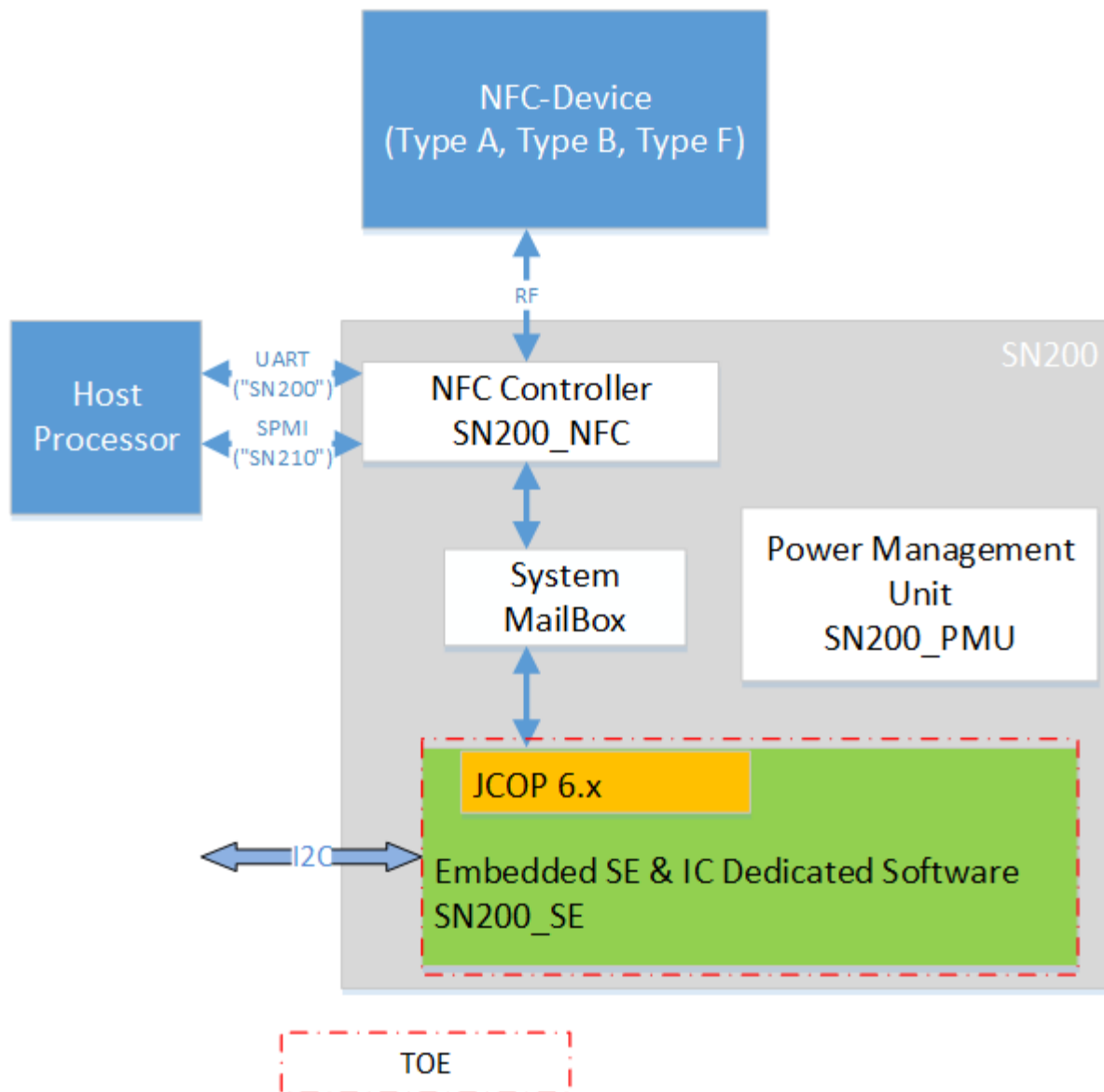
The TOE directly supports an I2C communication interface and communicates with the integrated NFC controller via the System Mailbox. The integrated NFC controller is not in scope of this evaluation, however it provides gates for external users to communicate with the TOE. Supported gates are Card Emulation Mode Type A/B/F, wired Interface using APDUCard over UART("SN200") or SPMI("SN210"), and Reader mode Type A/B (JCOP6.4, JCOP 6.5 and JCOP6.6). Extended length APDU communication is supported for Card Emulation and wired mode, up to 32kBytes.

The TOE can be further split into the following components:

- Software that implements the Java Card Virtual Machine and a Java Card Runtime Environment, called JCVM and JCRE.

- Software that implements the Java Card Application Programming Interface called JCAPI.

- Software for implementing content management according to GlobalPlatform, called GP.

- Software that implements a proprietary programming interface, called Extension API.

- Software that implements low level functionality, called Native OS.

- Software for implementing third party functionality, called Native Applications – including support for MiFARE and Felica applications.

- Software that handles personalization and configuration, called Config Applet.

- Software to update JCOP6 OS or updatable components of the IC Dedicated Software called OS Update. This component ensures that only NXP Authorized updates may be applied.
- •Software to transfer personalization applet data from an old to a new version of an applet on applet update time, called Applet Migration (AMD).
- Software that provides customer control on the Applet Migration and OS Update processes and ensures that only customer authorized OS updates can be performed in predefined states of the TOE. This software feature is called Image4 (IM4).



**Components of the TOE**
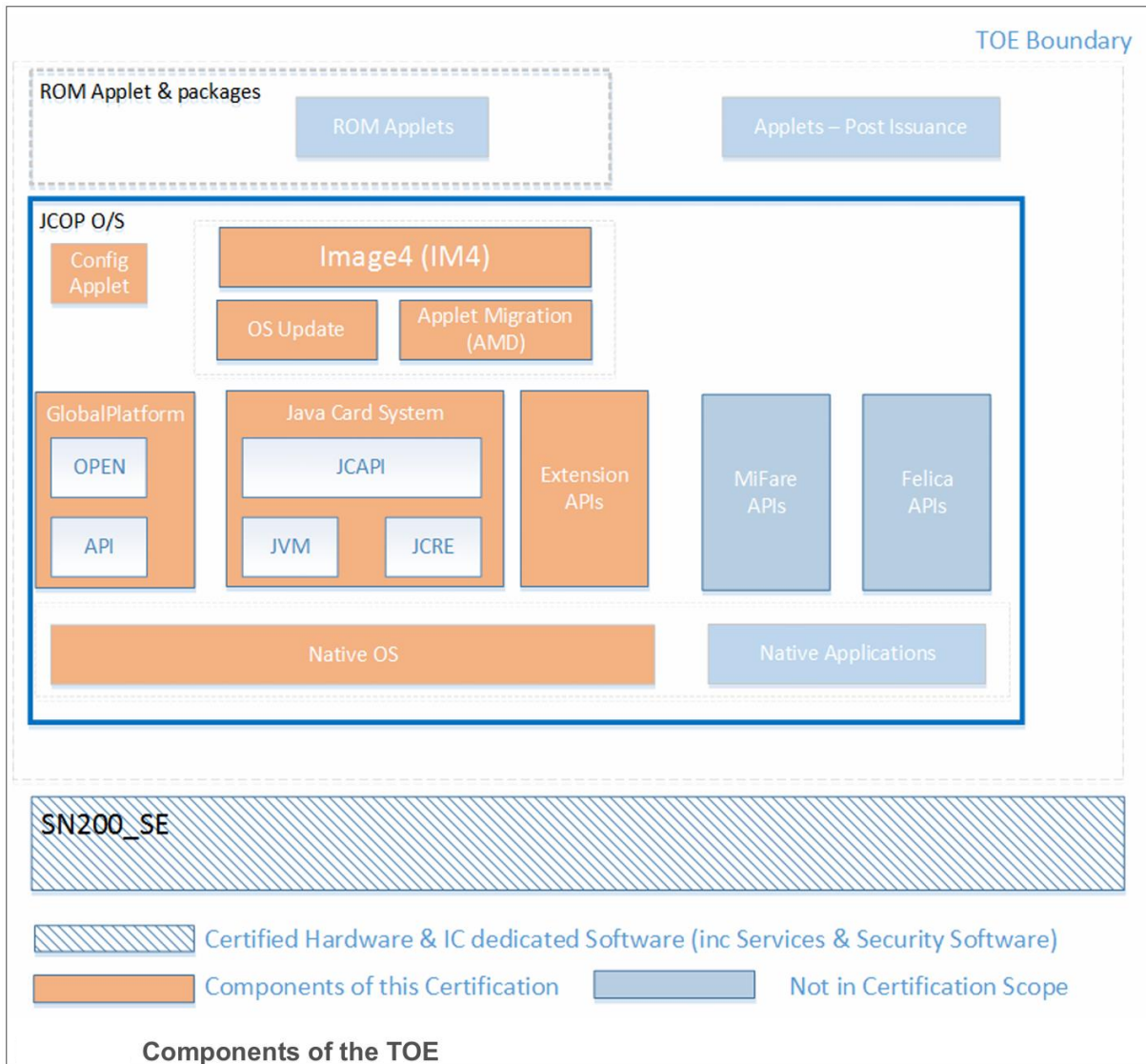
The figure above also shows applets. The applets are small Java programs which can be executed by the TOE, but are not part of the TOE. The Config Applet has special privileges and is used to personalise and configure the TOE. Customer applets are not part of the TOE. The Config Applet is part of the TOE.

## 2.5   Documentation

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

| Identifier | Version |
|---|---|
| JCOP 6.0 R1.13.0 (JCOP 6.0 11.3.13) – User Guidance Manual | 1.17 |
| JCOP 6.0 R1.13.0 – User Guidance Manual Addendum | 1.13 |

| | |
|---|---|
| JCOP 6.0 R1.13.0 – Anomaly Sheet | 1.14 |
| | |
| JCOP 6.1 R1.04.0 (JCOP 6.1 13.3.04) – User Guidance Manual | 3.6 |
| JCOP 6.1 R1.04.0 – User Guidance Manual Addendum | 3.3 |
| JCOP 6.1 R1.04.0 – Anomaly Sheet | 3.4 |
| | |
| JCOP 6.4 R1.06.0 (JCOP 6.4 17.3.06) – User Guidance Manual | 5.9.1 |
| JCOP 6.4 R1.06.0 (JCOP 6.4 17.3.06) – User Guidance Manual Addendum | 5.8 |
| JCOP 6.4 R1.06.0 (JCOP 6.4 17.3.06) – Anomaly Sheet | 5.8 |
| | |
| JCOP 6.5 R1.04.0 (JCOP 6.5 19.3.04) – User Guidance Manual | 7.6 |
| JCOP 6.5 R1.04.0 (JCOP 6.5 19.3.04) – User Guidance Manual Addendum | 7.5 |
| JCOP 6.5 R1.04.0 (JCOP 6.5 19.3.04) – Anomaly Sheet | 7.5 |
| | |
| JCOP 6.6 R1.06.0 (JCOP 6.6 20.3.06) – User Guidance Manual | 8.5.2 |
| JCOP 6.6 R1.06.0 (JCOP 6.6 20.3.06)– User Guidance Manual Addendum | 8.5 |
| JCOP 6.6 R1.06.0 (JCOP 6.6 20.3.06) – Anomaly Sheet | 8.5 |

## 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 SFR-enforcing 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.

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.

Amount of developer testing performed:

- The tests are performed on security mechanisms and on subsystem and module level with a total amount of several thousand test scenarios.
- As demonstrated by ATE_COV.2 the developer has tested all security mechanisms and TSFIs.
- As demonstrated by ATE_DPT.3 the developer has tested all the TSF subsystems and modules against the TOE design and against the security architecture description.

For the testing performed by the evaluators, the developer has provided samples and a test environment. During the baseline evaluation the evaluators verified the execution of a selection of the developer tests and conducted a number of test cases designed by the evaluator.

### 2.6.2 Independent penetration testing

The evaluator independent penetration tests were conducted according to the following testing approach:

- During evaluation of the ADV, ATE and ALC classes the evaluators hypothesized possible vulnerabilities. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained in particular from the source code analysis in IMP. This resulted in a shortlist of potential vulnerabilities to be tested.
- Next the evaluators analyzed the TOE design and implementation for resistance against the JIL attacks. This resulted in further potential vulnerabilities to be tested.
- The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ARC has assessed all information.
- The evaluators concluded that a number of areas could be potentially vulnerable for attackers possessing a high attack potential. Consequently, practical penetration testing was performed for absolute assurance.

The total test effort expended by the evaluators during this re-evaluation was 17 weeks. During that test campaign, 53% of the total time was spent on Perturbation attacks, and 47% on side-channel testing.

For the fourth certification the total test effort expended by the evaluators was 10 weeks. During that test campaign, 40% of the total time was spent on Perturbation attacks, 20% on retrieving keys with FA, 20% on side-channel testing, and 20% on logical tests.

For the third certification the total test effort expended by the evaluators was 10 weeks. During that test campaign, 40% of the total time was spent on Perturbation attacks, 20% on retrieving keys with FA, 20% on side-channel testing, and 20% on logical tests.

For the second certification (2020) in total 6 tests have been performed, 2 fault injection attacks, 2 side channel attacks, 1 combined attack and 1 logical security test. The overall time spent for penetration testing was approx. 14 weeks.

For the first certification (2019) in total 9 test have been performed, 7 fault injection attacks, 2 side channel attacks. The overall time spent for penetration testing was approx. 14 weeks.

### 2.6.3 Test configuration

The tests for this re-certification are performed on the TOE version JCOP 6.6 R1.06.0, while the original tests were performed on JCOP 6.0 R1.13.0 and JCOP 6.5 R1.04.0. Details can be found in [ETRfC].

### 2.6.4 Test results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

The 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 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.

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 JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210".

## 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 JCOP6.x on SN200.C04 Secure Element, versions JCOP6.0 R1.13.0 "SN200", JCOP6.1 R1.04.0 "SN200", JCOP6.1 R1.04.0 "SN210", JCOP6.4 R1.06.0 "SN200", JCOP6.4 R1.06.0 "SN210", JCOP6.5 R1.04.0 "SN200", JCOP6.5 R1.04.0 "SN210", JCOP6.6 R1.06.0 "SN200", JCOP6.6 R1.06.0 "SN210", to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2, ALC_FLR.1, AVA_VAN.5, and ASE_TSS.2.** This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP]*.

## 2.10  Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the 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:

- FELICA (out of scope as there are no security claims).

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 JCOP6.x on SN200.C04 Secure Element Security Target, Rev. 4.5, 21 August 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:

| | |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| CAP file | File in Converted APplet format |
| DES | Data Encryption Standard |
| DFA | Differential Fault Analysis |
| ECC | Elliptic Curve Cryptography |
| EMA | Electromagnetic Analysis |
| GUI | Graphical User Interface |
| IC | Integrated Circuit |
| IT | Information Technology |
| JIL | Joint Interpretation Library |
| MAC | Message Authentication Code |
| NSCIB | Netherlands Scheme for Certification in the area of IT Security |
| OS | Operating System |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| RAM | Random Access Memory |
| RNG | Random Number Generator |
| RSA | Rivest-Shamir-Adleman Algorithm |
| SHA | Secure Hash Algorithm |
| SPA/DPA | Simple/Differential Power Analysis |
| TRNG | True Random Number Generator |

TRUSTCB®
TRUST AND VERIFY

# 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 Must be retained for all composite smartcard TOEs |
| [ETR] | Evaluation Technical Report for NXP JCOP 6.x on SN200 Series Secure Element with Crypto Library B1.1 C04, v1.1, 15 October 2024 |
| [ETRfC] | ETR for Composite Evaluation for NXP JCOP 6.x on SN200 Series Secure Element with Crypto Library B1.1 C04, v1.1, 15 October 2024 |
| [HW-CERT] | Certification Report SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04, NSCIB-CC-2200037-02-CR, 15-08-2024 |
| [HW-ETRfC] | Riscure, ETR for Composite evaluation for SN200 Series Secure Element with Crypto Library B1.1 C04, v1.2, 20230432_C-D4, 2024-08-14 |
| [HW-ST] | NXP Semiconductors, SN200 Series Secure Element with Crypto Library Security Target, Rev1.5, 2024-04-29 |
| [JIL-AAPS] | Joint Interpretation Library, Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, 2024-02 |
| [JIL-AMS] | Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution) |
| [NSCIB] | Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022 |
| [PP] | Java Card Protection Profile – Open Configuration, registered under the reference BSI-CC-PP-0099-2017, Version 3.0.5, 21. December 2017 |
| [ST] | NXP JCOP6.x on SN200.C04 Secure Element Security Target, Rev. 4.5, 21 August 2024 |
| [ST-lite] | NXP JCOP6.x on SN200.C04 Secure Element Security Target Lite, Rev. 4.5, 21 August 2024 |
| [ST-SAN] | ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006 |

(This is the end of this report.)