Certification Report

NXP JCOP6.x on SN200.C04 Secure Element

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

Evaluation facility: ***Riscure***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-235773-CR2**

Report version: **1**

Project number: **235773_2**

Author(s): **Hans-Gerd Albertsen**

Date: **13 October 2020**

Number of pages: **15**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

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. The developer of the NXP JCOP6.x on SN200.C04 Secure Element is NXP Semiconductors Germany GmbH located in Hamburg, Germany and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE consists of an embedded Secure Element SN200.C04 with Crypto Library loaded with a Java Card operating system image JCOP 6.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 update 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 has been originally evaluated by Riscure B.V. located in Delft, The Netherlands and was certified on 08. July 2019. The re-evaluation also took place by Riscure B.V. and was completed on 09 October 2020 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

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

The major changes are the addition of JCOP 6.1 (R1.04.0) on hardware configuration SN200 (UART Interface) and SN210 (SPMI Interface), comprising the following improvements compared to JCOP 6.0:

- Security hardening.

- Minor functional changes, not security relevant.

- Bugfixes and implementation improvements, not security relevant.

A further minor change was a typo correction in the JCOP 6.0 UGM (v1.13 -> v1.14) with no security impact.

The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the NXP JCOP6.x on SN200.C04 Secure Element, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the NXP JCOP6.x on SN200.C04 Secure Element are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provides sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with 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]*.

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

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP6.x on SN200.C04 Secure Element from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SN200 Secure Element (as part of the base certification)	B1.1 C04
Configuration Data	Factory Page (as part of base certification) System Page Common (as part of the base certification) BootOS Patch (as part of the base certification)	19554 20103 7.0.5 PL3 v9
Software	Crypto Library (as part of the base certification) Services Software (as part of the base certification) Java Card OS with proprietary extensions, implements Java Card 3.0.4 Classic	V1.0.0 4.13.3.0 6.0 R1.13.0 6.1 R1.04.0

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. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to 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. Detailed information on these

security objectives that must be fulfilled by the TOE environment can be found in section 5.2 of the *[ST]*.

2.3.2 Clarification of scope

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

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 and 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.

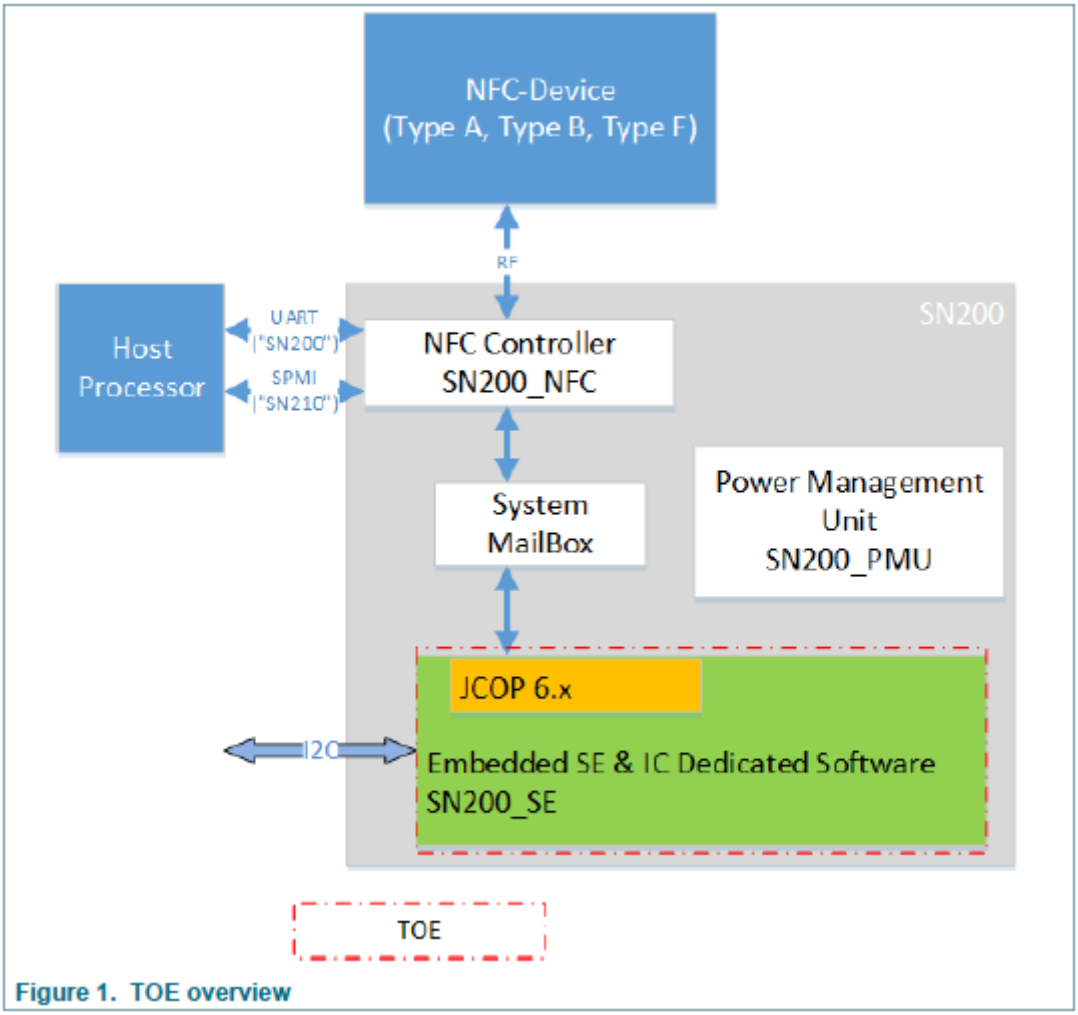

Figure 1. TOE overview

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, provides up to 4 gates for external users to communicate with the TOE supporting Card Emulation Mode Type A, Type B and Type F as well as a wired Interface using APDUCard Gate. 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 JCOP6.0/6.1 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).

The components of the TOE are depicted in Figure 2.

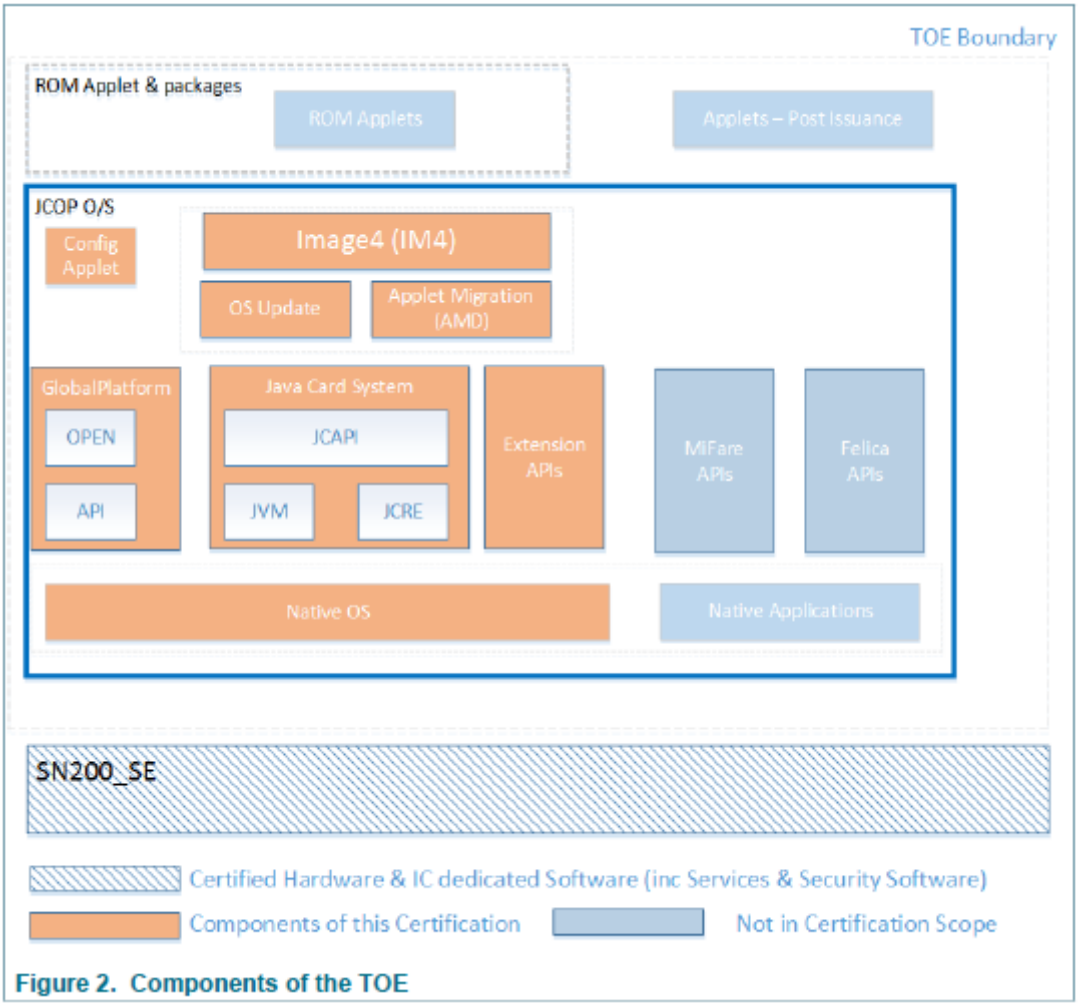

Figure 2. Components of the TOE

2.5 Documentation

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

Identifier	Version	Form of Delivery
JCOP6.0 R1.13.0 User Guidance Manual	1.14	Electronic Document
JCOP6.0 R1.13.0 UGM Manual Addendum	1.13	Electronic Document
JCOP6.0 R1.13.0 UGM Anomaly Sheet	1.13	Electronic Document
JCOP6.1 R1.04.0 User Guidance Manual	3.3	Electronic Document
JCOP6.1 R1.04.0 UGM Addendum	3.3	Electronic Document
JCOP6.1 R1.04.0 UGM Anomaly Sheet	3.3	Electronic Document

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. The evaluators have 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.

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.

2.6.3 Test Configuration

Testing was performed on the TOE (JCOP6.0 R1.13.0 and JCOP6.1 R1.04.0 (SN200 & SN210 configuration). Details can be found in *[ETRfC]*.

2.6.4 Testing Results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

The 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 Re-used evaluation results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 11 site certificates (NXP Hamburg, NXP Gratkorn, NXP Bangalore, NXP HTC60, NXP San Jose, NXP San Diego 2, NXP Phoenix, NXP Caen, NXP Mougins, NXP ATKH Kaohsiung, and ASEK Kaohsiung).

Sites involved in the development and production of the hardware platform were re-used by composition. No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP JCOP6.x on SN200.C04 Secure Element. The user can identify the TOE by requesting the platform ID. The platform ID is obtained by the GET PLATFORM IDENTIFIER command. Details are described in the guidance documentation.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the NXP JCOP6.x on SN200.C04 Secure Element, to be **CC Part 2 extended, CC Part 3** conformant, (check ST compliance claim) 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]*.

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

2.10 Comments/Recommendations

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

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

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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)

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. In order 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 Security Target NXP JCOP6.x on SN200.C04 Secure Element, Version 2.3, 10. September 2020 *[ST]* is included here by reference.

Please note that for the need of publication a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
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
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NSCIB	Netherlands Scheme for Certification in the area of IT security
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
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.
[ETR]	Evaluation Technical Report NXP JCOP6.x on SN200.C04 Secure Element, Doc ID 20190620-D3, Version 1.1, 25. September 2020.
[ETRfC]	ETR for Composite Evaluation NXP JCOP6.x on SN200.C04 Secure Element, Doc ID 20190620-D4 Version 1.1, 25. September 2020.
[HW-CERT]	Certification Report SN200 Series - Secure Element with Crypto Library SN200_SE B1.1 C04, NSCIB-CC-217812-CR, Version 1.0, 04.07.2019.
[HW-ETRfC]	ETR for Composite Evaluation ETR for composite evaluation SN200 Series – Secure Element with Crypto Library B1.1 C04, NSCIB_217812-ETR-COMP_v1.0.pdf, v1.0, 01.07.2019
[HW-ST]	SN200 Series - Secure Element with Crypto Library Security Target, st_SN200_SE_1_1.pdf, 24.06.2019
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Java Card Protection Profile – Open Configuration, registered under the reference BSI-CC-PP-0099-2017, Version 3.0.5, 21. December 2017
[ST]	Security Target NXP JCOP6.x on SN200.C04 Secure Element, Version 2.3, 10. September 2020.
[ST-lite]	Security Target Lite NXP JCOP6.x on SN200.C04 Secure Element, Version 2.1, 10. September 2020
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).