TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Version 2021-06

Certification Report

JCOP 4.7 SE051

Sponsor and developer:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20** **22529 Hamburg** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0095534-CR2**
Report version:	**1**
Project number:	**0095534_2**
Author(s):	**Denise Cater**
Date:	**25 November 2021**
Number of pages:	**14**
Number of appendices:	**0**

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

Head Office:
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 Netherlands Chamber of Commerce (KVK), 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 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 JCOP 4.7 SE051. The developer of the JCOP 4.7 SE051 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, which is referred to as JCOP 4.7 SE051, is a Java Card with a GP Framework. The TOE is a composite product on top of a CC certified Hardware (Micro Controller component) with IC Dedicated Software and Crypto Library (MC FW and Crypto Library component).

The software stack, which is stored on the Micro Controller and executed by the Micro Controller, can be further split into the following components:

- Firmware for booting and low level functionality of the Micro Controller (MC FW) like writing to flash memory. This includes software for implementing cryptographic operations, called Crypto Library.
- Software for implementing a Java Card Virtual Machine [JCVM], a Java Card Runtime Environment [JCRE] and a Java Card Application Programming Interface [JCAPI], called JCVM, JCRE and JCAPI.
- Software for implementing content management according to GlobalPlatform [GP], called GlobalPlatform (GP) Framework.
- Software for executing native libraries, called Secure Box.

The TOE has some dedicated functionality that can be removed depending upon customer needs. These items are listed in [STLite] section 1.3.2

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 07 July 2020. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 23 November 2021 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 minor changes”.

The modified TOE did not change from physical perspective. The change lies in the underlying platform, which also physically did not change but only received a different certification identifier. This resulted in reference updates in the ST of the modified TOE. Furthermore, the guidance documents received minor updates related to clarifications and references.

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 JCOP 4.7 SE051, 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 JCOP 4.7 SE051 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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with 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).

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

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 JCOP 4.7 SE051 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Hardware	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) (The SE051 hardware is an instantiation of the N7121 hard macro with I2C sidecar)	B1
IC Dedicated Test Software (On-chip software)	Test Software	9.2.3
IC Dedicated Support Software (On-chip software)	Boot Software	9.2.3
	Firmware	9.2.3
	Flashloader OS	1.2.5
	Library Interface • Communication Library • CRC Library • Memory Library • Flash Loader Library	9.2.3 • 6.0.0 • 1.1.8 • 1.2.3 • 3.6.0
	System Mode OS	13.2.3
	Crypto Library • RNG Lib • RNG HealthTest Lib • Sym. Cipher Lib • KeyStoreMgr Lib • Sym. Utilities Lib • RSA Lib • RSA Key Generation Lib • ECC Lib • SHA Library & Hash Library • Asym. Utilities Lib	0.7.6 • 0.7.6 • 0.7.6 • 0.7.6 • 0.7.6 • 0.7.6 • 0.7.6 • 0.7.6 • 0.7.6 • 0.7.6 • 0.7.6
IC Embedded Software	JCOP OS + Modules Patch ID = “0000000000000001” Platform Build ID • IOT Full = “4C0954E73E773C6E” • IOT Reduced = “1A08FA5067B5F256” Revision = “170817” ROM ID = “2E5AD88409C9BADB” Platform ID = “J3R351029B411100”	revision 170817

To ensure secure usage a set of guidance documents is provided, together with the JCOP 4.7 SE051. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.4.

2.2 Security Policy

The following cryptographic primitives are supported and included within the TSF:

- 3DES for encryption/decryption (CBC and ECB) and MAC generation and verification (Retail-MAC, CMAC and CBC-MAC)
- AES for encryption/decryption (CBC, ECB and Counter Mode) and MAC generation and verification (CMAC, CBC-MAC)
- RSA and RSA-CRT for encryption/decryption and signature generation/verification and key generation
- ECC over GF(p) for signature generation/verification (ECDSA) and key generation
- RNG according to DRG.3 or DRG.4 of AIS 20 [AIS20]
- Diffie-Hellman with ECDH and modular exponentiation
- Hash algorithms SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

The following (non-TSF) cryptographic primitives are supported:

- AES in Counter with CBC-MAC mode (AES CCM)
- Keyed-Hash Message Authentication Code (HMAC)
- HMAC-based Key Derivation Function (HKDF) [RFC-5869]
- Elliptic Curve Direct Anonymous Attestation (ECDAA) [TPM]
- ECC based on Edwards and Montgomery curves

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 a GP Framework. It can be used to load and execute off-card verified Java Card applets. It is a composite product on top of a CC certified Hardware (Micro Controller component) with IC Dedicated Software and Crypto Library (MC FW and Crypto Library component).

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:

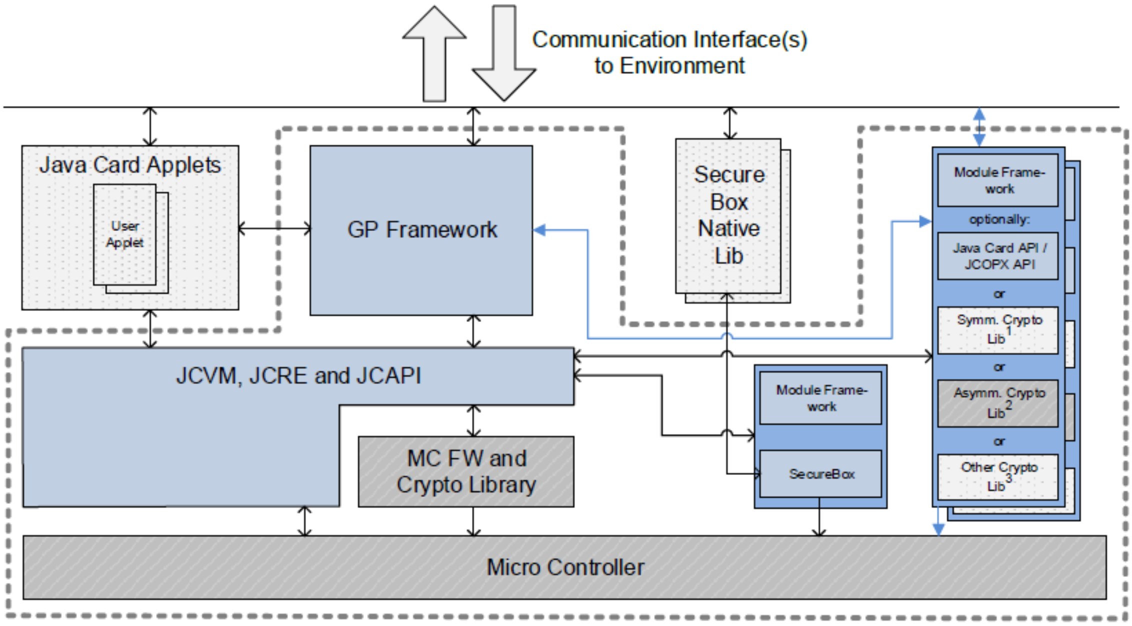

Figure 1 Logical architecture of the TOE

In the above figure, the solid blue parts are in scope of the TOE, with the items in hatched blue being provided by the composite (certified hardware and crypto library). The items in grey are out of scope.

The TOE is a composite product on top of CC certified Hardware, Firmware and Crypto Library. Parts of the TOE are the JCVM, JCRE, JCAPI and the GP Framework. Also included are optional functionality and the Secure Box mechanism. The Secure Box Native Library provides native functions for untrusted third parties and are not part of the TOE.

The I2C protocol is supported. For this, the hardware contains a so-called sidecar.

2.5 Documentation

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

Identifier	**Version**
JCOP 4.7 SE051, User manual for JCOP 4.7 SE051, User Guidance and Administration Manual	Rev. 1.3, 27 September 2021
SE051, Plug & Trust Secure Element, Product Data Sheet	Rev. 1.3, 15 April 2021

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 module and module interface level. The tests are performed by NXP through execution of the test scripts using an automated and distributed system. Test tools and scripts are extensively used to verify that the tests return expected values.

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 evaluator performed the ATE activities based on code coverage analysis. The evaluator also used an acceptable alternative approach (as described in the application notes, Section 14.2.2 in [CEM]) and used analysis of the implementation representation (i.e. inspection of source code) to validate the rationales provided by the developer.

During the baseline evaluation the evaluator witnessed the execution of developer tests. Test cases were selected that cover various aspects of the TOE, as well as areas where the code coverage approach has limitations.

The developer tests are extensive and as such testing would lead to tests that are only superficially different from testing performed by the developer. As a result, the evaluator judged that tests should be defined that are supplementing the developer’s tests and should be based on how adequate the TOE security functions are implemented rather than on how well the various industry standards are met. Further focus was put on logical testing.

During the re-evaluation, no specific functional testing has been performed and functional testing was reused from the baseline evaluation.

2.6.2 Independent penetration testing

This section contains information with regard to the evaluator testing effort, mandated to be included in the ETR by AVA_VAN.5-5, AVA_VAN.5-10 and AVA_VAN.5-12.

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ADV and AGD potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour. From the ASE class, no potential vulnerabilities were identified.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack-oriented analysis, the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was supported by the attack list in [JIL-AM] and application of attack potential in [JIL-AAP].
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For most of the potential vulnerabilities a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

The vulnerability analysis has been refreshed during this re-evaluation.

During the baseline evaluation a total of 4 weeks and 1 day of penetration testing was performed for the TOE. The test cases were split 24% perturbation testing, 71% side channel attacks and 5% software logical attacks. During this re-evaluation, a further 5.5 weeks test effort was expended by the evaluators, of which 18.2% of the total time was spent on Perturbation attacks, 72.7% on side-channel testing, and 9.1% on logical tests.

2.6.3 Test configuration

The TOE was tested (System Tests) in the following configurations:

- FPGA Emulator and PC Platform
- TOE (SO28 package and SMD package)
- Using T=0, T=1 (ISO7816) and T=CL (ISO14443)

As part of this re-evaluation, penetration testing has been performed on the “JCOP 4 P71” product (J3R35101FA9E0400). The evaluator notes that the TOE is closely related to the “JCOP 4 P71” product (certified with the identifier CC-21-180212). They share the underlying platform as well as same code base (albeit different feature set) and do not differ substantially from a conceptual point of view. As such, assurance from the “JCOP 4 P71” is also applicable for the TOE.

The Penetration testing for this re-evaluation was performed on the IOT Full feature set of the TOE.

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 strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. The remaining security level still exceeds 80 bits, so this is considered sufficient. Therefore, no exploitable vulnerabilities were found with the independent penetration tests.

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.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number JCOP 4.7 SE051.

The TOE can be used in Full IOT configuration or Reduced IOT configuration, as indicated by the Platform Build ID.

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 JCOP 4.7 SE051, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with 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 Protection Profile *[PP_0099]*.

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 following algorithms, protocols and implementations was not rated in the course of this evaluation:

- AES in Counter with CBC-MAC mode (AES CCM)
- Keyed-Hash Message Authentication Code (HMAC)
- HMAC-based Key Derivation Function (HKDF)
- Elliptic Curve Direct Anonymous Attestation (ECDAA)
- ECC based on Edwards and Montgomery curves

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 JCOP 4.7 SE051, Security Target, Rev. 1.6, 18 November 2021 *[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
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CMAC	Chaining Message Authentication Code
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC (over GF)	Elliptic Curve Cryptography (over Galois Fields)
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JCAPI	Java Card Application Programming Interface
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SSM	Scalable Security Module
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 “JCOP 4.7 SE051” – EAL6+, 21-RPT-1131, Version 2.0, 22 November 2021

[ETRfC] Evaluation Technical Report for Composition “JCOP 4.7 SE051” – EAL6+, 21-RPT-1132, Version 2.0, 22 November 2021

[GP] GlobalPlatform Card Specification, v2.3.0, GPC_SPE_034, GlobalPlatform Inc., October 2015

[HW-CR] Certification Report, BSI-DSZ-CC-1136-2021 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) from NXP Semiconductors Germany GmbH, version 1.0, 10 February 2021

[HW-ETRfC] Evaluation Technical Report for Composite Evaluation (ETR COMP) NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) B1, version 3.0, 05 February 2021

[HW-ST] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2), Security Target, Revision 2.2, 19 January 2021

[HW-ST-lite] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2), Security Target Lite, Revision 1.8, 19 January 2021

[JCAPI] Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5, May 2015

[JCRE] Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5, May 2015

[JCVM] Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5, May 2015

[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_0099] Java Card System - Open Configuration Protection Profile, registered under the reference BSI-CC-PP-0099-2017, December 2017, Version 3.0.5

[ST] JCOP 4.7 SE051, Security Target, Rev. 1.6, 18 November 2021

[ST-lite] JCOP 4.7 SE051, Security Target Lite, Rev. 1.6, 18 November 2021

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

(This is the end of this report.)