Certification Report

JCOP 4 P71

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

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-180212-CR**

Report version: **1**

Project number: **180212**

Author(s): **Wouter Slegers and Denise Cater**

Date: **23 July 2019**

Number of pages: **13**

Number of appendices: **0**

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-180212**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors Germany GmbH** **Troplowitzstrasse 20, 22529 Hamburg, Germany**
Product and assurance level	**JCOP 4 P71** Assurance Package: ▪ EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 Protection Profile Conformance (if appropriate): ▪ Java Card System - Open Configuration Protection Profile, BSI-CC-PP-0099-2017, December 2017, Version 3.0.5
Project number	**180212**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity	Date of 1st issue : **25-07-2019** Certificate expiry : **25-07-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword **4**

Recognition of the certificate **5**

International recognition 5
European recognition 5

1 Executive Summary **6**

2 Certification Results **7**

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 7
2.3 Assumptions and Clarification of Scope 8
2.4 Architectural Information 8
2.5 Documentation 8
2.6 IT Product Testing 9
2.7 Re-used evaluation results 10
2.8 Evaluated Configuration 10
2.9 Results of the Evaluation 11
2.10 Comments/Recommendations 11

3 Security Target **12**

4 Definitions **12**

5 Bibliography **13**

TÜVRheinland®
Precisely Right.

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 JCOP 4 P71. The developer of the JCOP 4 P71 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 the Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. The software stack 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 Framework
- Software for executing native libraries, called Secure Box.

The TOE is referred to as JCOP 4 P71. The JCOP 4 Operating System (JCOP 4 OS) consists of the software stack without the Crypto Library (Crypto Lib) and without the Micro Controller Firmware (MC FW). The TOE uses one or more communication interfaces to communicate with its environment.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 23 July 2019 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]*.

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 P71, 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 P71 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]*.

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 JCOP 4 P71 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 (as part of [CR-N7121] certificate)	B1
Software	IC Dedicated Test Software (as part of [CR-N7121] certificate)	9.2.3
	Boot Software (as part of [CR-N7121] certificate)	9.2.3
	Firmware (as part of [CR-N7121] certificate)	9.2.3
	FlashLoader OS (as part of [CR-N7121] certificate)	1.2.5
	Library Interface (as part of [CR-N7121] certificate)	9.2.3
	System Mode OS (as part of [CR-N7121] certificate)	13.2.3
	Crypto Library (as part of [CR-N7121] certificate)	0.7.6
	IC Embedded Software (for “Configuration Banking & Secure ID”)	svn129694 svn144945
	IC Embedded Software (for “Configuration Secure Authentication”)	svn138990

To ensure secure usage a set of guidance documents is provided together with the JCOP 4 P71. Details can be found in section ”Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.3.3.

2.2 Security Policy

The TOE is a composite product on top of CC certified Hardware, Firmware and Crypto Library. Part of the TOE are the JCVM, JCRE and JCAPI features and the GP Framework.

The TOE features a Modular Design which allows features to be present or removed upon customer needs. Each module is part of the JCOP OS and implements specific use-case features and can be accessed through APDUs or APIs. A module can only be removed but not added. Modules included in the TOE are detailed in *[ST]* section 1.3.2.

The SecureBox Module (securebox) provides a feature allowing execution of non-certified native software within the TOE.

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

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 4.4 of the *[ST]*.

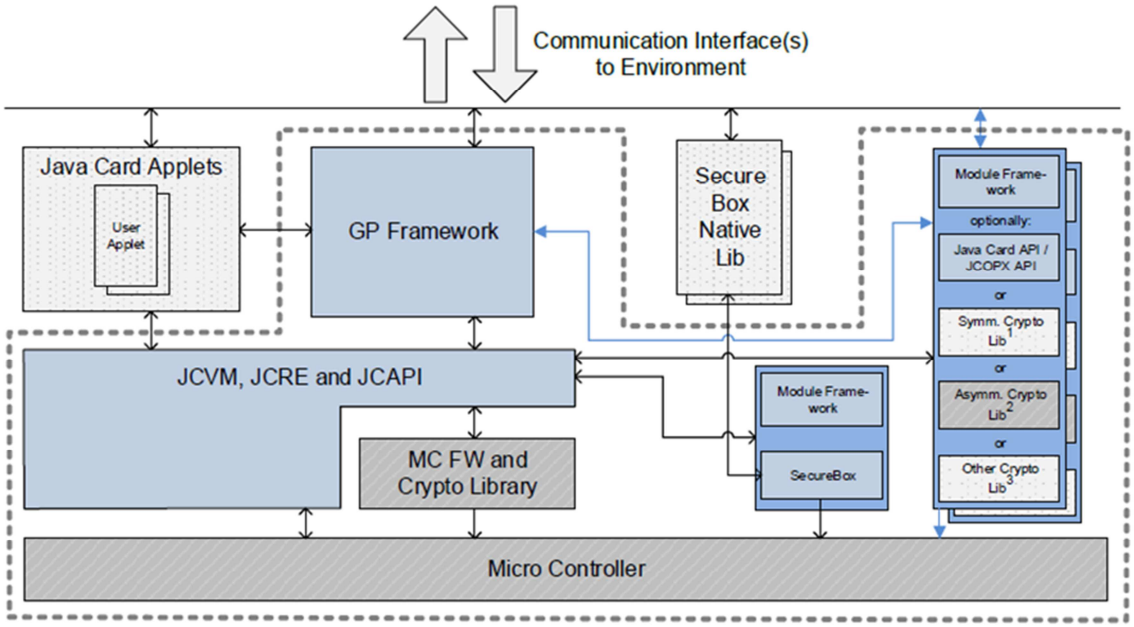
2.3.2 Clarification of scope

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:



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

2.5 Documentation

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

	Identifier	Version
Configuration Banking & Secure ID	JCOP 4 P71, User manual for JCOP 4 P71	Rev 3.7, 2019-05-28
	NXP Secure Smart Card Controller N7121, Preliminary data sheet	Rev 2.0, 2018-08-31,
Configuration Secure Authentication	JCOP 4 SE050, User manual for JCOP 4 SE050	Rev 1.2, 2019-05-31
	SE050 Family, Data Sheet	Rev 0.1, 2018-04-03

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 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. security measures not hit due to redundancy checks).

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.

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

The evaluator witnessed execution of a sample of tests cases from the test suite. This was done due to the distributed and remote testing equipment necessary to perform tests, which would not be feasible to perform this at the ITSEF premises. The following seven categories were selected for test witnessing:

- Spot checks on coverage and set-up
- Demonstrate how TOE is identified during functional testing
- Attempt to execute an illegal access from within native code running in the SecureBox
- Spot checks on various crypto functions (during both sessions)
- Perform test of anti-tearing mechanism for GP command Store Data
- Testing of the Global Platform secure messaging protocol
- Testing of the I2C protocol

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in classes ASE, ADV and AGD, potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
- For ADV_IMP a thorough implementation representation review was performed on the TOE. During this attack oriented analysis, the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was performed taking into account the attack

methods in *[JIL-AM]* and attack potential in [JIL-AP]. An important source for assurance in this step is the technical report *[N7121-ETRfC]* of the underlying platform.

- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable by using *[JIL-AP]*. 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 penetration tests that were defined are presented below in the subsections.

Test performed have been described in 11 test cases.

2.6.3 Test Configuration

Penetration testing started targeting configuration “Configuration Banking & Secure ID” svn129694 followed by “Configuration Secure Authentication” svn138990. Most of the testing was performed on an earlier revision of the product, i.e. indicated as “svn125196” (J3R35101E90C0400) while the TOE “Configuration Banking & Secure ID” is indicated as “svn129694” (J3R35101FA9E0400) and “svn144945” (J3R3510236310400). The changes from the earlier revision and the TOE revisions have been assessed and showed that the results obtained are not impacted by the changes.

Finally, specific testing has been performed for further assurance for “Configuration Secure Authentication” indicated as “svn138990” (J3R351021EEE0400). The assurance gained from penetration testing on the svn129694 configuration has been assessed to be valid for svn138990 due to the similarities of both configurations. Nevertheless, one test was repeated on the second configuration for added assurance on the main security action.

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.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Re-used evaluation results

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 5 site certificates.

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 JCOP 4 P71.

The TOE is available in two configurations, of which the first configuration has two versions:

Configuration	JCOP Version
Configuration Banking & Secure ID	JCOP 4 P71 v4.7 R1.00.4 JCOP 4 P71 v4.7 R1.01.4
Configuration Secure Authentication	JCOP 4 SE050 v4.7 R2.00.11

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] 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 JCOP 4 P71, 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]*.

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:

- KoreanSEED
- 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

To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

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

3 Security Target

The JCOP 4 P71, Security Target for JCOP 4 P71 / SE050, Rev. 3.4, 06-06-2019 *[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
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
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.

[CR-N7121] BSI-DSZ-CC-1040-2019, NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library from NXP Semiconductors Germany GmbH, v1.0, BSI

[N7121-ETRfC] ETR for Composition, NXP Secure Smart Card Controller P7121 with IC Dedicated Software and Crypto Library (N7121) according to AIS36, 18-RPT-788 v8.0, 31 May 2019, Brightsight

[N7121-ST] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library Security Target, Rev. 1.5, 31 May 2019

[ETR] Evaluation Technical Report JCOP 4 P71, 19-RPT-542, Version 1.0, Issue 08 July 2019.

[ETRfC] Evaluation Technical Report for Composition NXP JCOP 4 P71 – EAL6+, 19-RPT-177, Version 1.0, Issue 27 June 2019.

[GP] GlobalPlatform Card Specification, v2.3, GlobalPlatform Inc., October 2015

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

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

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

[JIL-AM] JIL, Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.2, January 2013

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019

[PP] Java Card System - Open Configuration Protection Profile, December 2017, Version 3.0.5, certified by Bundesamt für Sicherheit in der Informationstechnik (BSI, BSI-CC-PP-0099-2017)

[RFC-5869] RFC 5869, HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010.

[ST] JCOP 4 P71, Security Target for JCOP 4 P71 / SE050, Rev. 3.4, 06-06-2019.

[ST-lite] JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050, Rev. 3.4, 06-06-2019

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

[TPM] TPM Rev. 2.0: Trusted Platform Module Library Specification, Family "2.0", Level 00, Revision 01.07- March 2014.

(This is the end of this report).