Certification Report

JCOP 4 P71

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-180212-CR5**

Report version: **1**

Project number: **180212_5**

Author(s): **Denise Cater**

Date: **26 September 2022**

Number of pages: **14**

Number of appendices: **0**

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 **3**

Recognition of the Certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **7**

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 8
2.3 Assumptions and Clarification of Scope 8
2.3.1 Assumptions 8
2.3.2 Clarification of scope 8
2.4 Architectural Information 8
2.5 Documentation 9
2.6 IT Product Testing 9
2.6.1 Testing approach and depth 10
2.6.2 Independent penetration testing 10
2.6.3 Test configuration 11
2.6.4 Test results 11
2.7 Reused Evaluation Results 11
2.8 Evaluated Configuration 11
2.9 Evaluation Results 12
2.10 Comments/Recommendations 12

3 Security Target **13**

4 Definitions **13**

5 Bibliography **14**

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.

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 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 is available in following configurations, of which both configurations have two versions:

- Configuration Banking & Secure ID (version JCOP 4 P71 v4.7 R1.00.4, JCOP 4 P71 v4.7 R1.01.4 and JCOP 4 P71 v4.7 R1.02.4)
- Configuration Secure Authentication (version JCOP 4 SE050 v4.7 R2.00.11 and JCOP 4 SE050 v4.7 R2.03.11)

The TOE was evaluated initially by Brightsight B.V. located in Delft, The Netherlands and was certified on 23 July 2019. A re-evaluation also took place by Brightsight B.V. and was completed on 20 March 2020 with the approval of the ETR. A second re-evaluation took place by SGS Brightsight B.V. and was completed on 26 February 2021. The third re-evaluation of the TOE was conducted by SGS Brightsight B.V. and completed on 04 July 2022 with the approval of the ETR. This fourth re-evaluation of the TOE was conducted by SGS Brightsight B.V. and completed on 19 September 2022 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]*.

The second issue of the Certification Report is a result of a “recertification with minor changes”.

The minor changes are additional version of the Security Authentication configuration with improved FIPS 140-2 compliance and bug fixes, and updates for site certifications.

The security evaluation re-used the evaluation results of previously performed evaluations.

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

Although there are no changes to the JCOP 4 operating system, the changes were characterised as ‘major’ due to certification of the underlying hardware platform.

The underlying hardware platform, certified by BSI under reference BSI-DSZ-CC-1040 (BSI-DSZ-CC-1040-2019-MA-01), was re-evaluated by a different ITSEF while remaining under the same scheme but given a new reference, i.e. BSI-DSZ-CC-1136. There were no changes to the physical TOE part of the hardware platform TOE. The only hardware platform TOE changes lay in the Security Target and the N7121 guidance, reflecting references to the renewed components. In addition, site certifications for the hardware platform were renewed and added as relevant.

The security evaluation re-used the evaluation results of previously performed evaluations. However the vulnerability analysis was renewed and penetration testing was performed during this re-certification.

The fourth issue of the Certification Report is a result of a “recertification with major changes”.

Although there were no changes to the JCOP 4 operating system, the changes were characterised as ‘major’ due to re-certification of the underlying hardware platform and update of *[ST]*:

- The underlying hardware platform, certified by BSI under reference BSI-DSZ-CC-1136-V2-2022, was re-evaluated to include a new production site.

- The requirement FCS_COP.1.1[ECDHPACEKeyAgreement] was amended in *[ST]* and *[ST-Lite]* to limit the key lengths used for PACE-PIN to 256, 384 and 512 bits, and the associated user guidance documents (see section 2.5 Documentation) were updated to reflect these changes.

The security evaluation reused the evaluation results of previously performed evaluations. The vulnerability analysis was not refreshed in its entirety and there was no renewed testing as part of the re-certification.

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

The major changes are due to re-certification of the underlying hardware platform and update of *[ST]:*

- The underlying hardware components were re-certified by BSI, including a new version of the Crypto Library, under reference BSI-DSZ-CC-1136-V3-2022.

- A new JCOP configuration (JCOP 4 P71 v4.7 R1.02.4) was added based on this updated Crypto Library, with no other code changes (the JCOP implementation is the same between versions R1.01.4 and R1.02.4).

- The user guidance documents and ST were updated with clarifications on the scope and references to the underlying hardware certificate.

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 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]* (Parts I, II and III).

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.

[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 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 (R1/R2/R3/R4), as part of *[CR-N7121]*	B1
Software	IC Dedicated Test Software (as part of *[CR-N7121]*)	9.2.3.0
	Boot Software (as part of *[CR-N7121]*)	9.2.3.0
	Firmware (as part of *[CR-N7121]*)	9.2.3.0
	FlashLoader OS (as part of *[CR-N7121]*)	1.2.5
	Library Interface (as part of *[CR-N7121]*)	9.2.3.0
	System Mode OS (as part of *[CR-N7121]*)	13.2.3.0
	Crypto Library (as part of *[CR-N7121]*)	0.7.6 / 0.7.7[2]
	IC Embedded Software (for “Configuration Banking & Secure ID”)	JCOP4 P71v4.7 R1.00.4 Platform ID containing in ASCII “J3R35101FA9E0400” svn129694
		JCOP4 P71v4.7 R1.01.4 Platform ID containing in ASCII “J3R3510236310400” svn144945
		JCOP4 P71v4.7 R1.02.4 Platform ID containing in ASCII “J3R35103B01B0400” svn241691
	IC Embedded Software (for “Configuration Secure Authentication”)	JCOP4 SE050 v4.7 R2.00.11 Platform ID containing in ASCII “J3R351021EEE0400” svn138990
		JCOP4 SE050 v4.7 R2.03.11 Platform ID containing in ASCII

[2] The Crypto Library version used for JCOP 4 P71 v4.7 R1.02.4 is 0.7.7, whereas for other configurations it is 0.7.6.

		“J3R3510264571100” svn156759

To ensure secure usage a set of guidance documents is provided, together with the JCOP 4 P71. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.3.

2.2 Security Policy

The TOE 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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see 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.

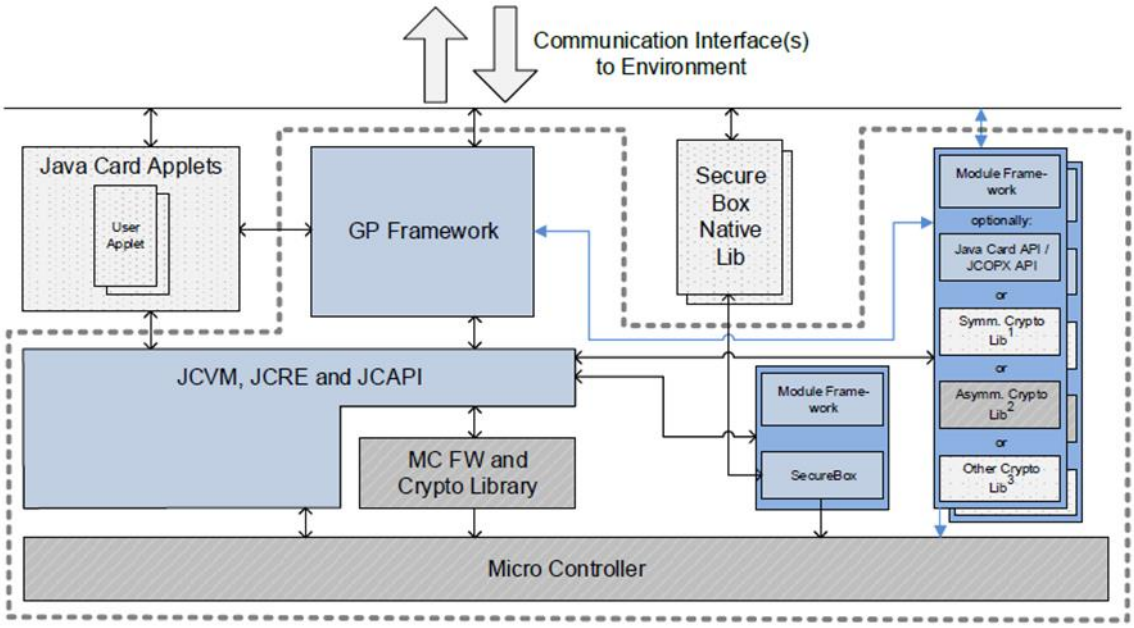
There are no security claims relating to the following cryptographic algorithms:

- 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

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:

Configuration	Identifier	Version
Configuration Banking & Secure ID (TOE versions svn129694, svn144945 & svn241691)	JCOP 4 P71, User manual for JCOP 4 P71	Rev 4.2 05 August 2022
	NXP Secure Smart Card Controller N7121, Product data sheet	Rev 3.3, 15 April 2020
Configuration Secure Authentication (TOE version svn138990)	JCOP 4 SE050 v4.7 R2.00.11, User manual for JCOP 4 SE050 v4.7 R2.00.11, User Guidance and Administrator Manual	Rev 1.9 05 August 2022
	SE050 Family, Data Sheet	Rev 0.1, 3 April 2018
Configuration Secure Authentication (TOE version svn156759)	JCOP 4 SE050 v4.7 R2.03.11, User manual for JCOP 4 SE050 4.7 R2.03.11, User Guidance and Administrator Manual	Rev 2.2 05 August 2022
	SE050 Family, Data Sheet	Rev 0.1, 3 April 2018

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.

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 during the initial evaluation of the TOE:

- 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

For the testing performed by the evaluators, the developer has provided samples and a test environment. During the first re-certification of the TOE the evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator. During this second re-certification activity the evaluator performed a limited number of test cases designed by the evaluator. There has been no additional evaluator testing performed in the third re-evaluation. No additional evaluator testing was performed this fourth re-evaluation due to the fact that the additional JCOP variant added differs only from the previous variant in a small part of its underlying Crypto Library, and the developer already sufficiently tested for the purposes of non-regression. The test results of the independent evaluator tests are not affected by the change and the previously obtained assurance is valid for the TOE.

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-AAPS]*. An important source for assurance in this step was 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-AAPS]*. 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.

The tests performed during the initial evaluation were described in 11 test cases. An additional two test cases were identified during the second re-evaluation. The total test effort expended by the

evaluators during the second re-evaluation was 5 weeks. During that test campaign 25.5% of the total time was spend on Perturbation attacks, 49% on side channel testing and 25.5% on logical tests. There was no additional testing performed in the third re-evaluation. During this fourth re-evaluation the total test effort expended by the evaluators was two weeks. During that test campaign, 50% of the total time was spent on perturbation attacks, and 50% on side-channel attacks.

The validity of tests results from earlier (re-)evaluations have been confirmed by gaining assurance from similar penetration tests during subsequent re-evaluations, and as a result, all test results are still valid for the current TOE.

2.6.3 Test configuration

Evaluator testing performed during the initial evaluation started targeting configuration “Configuration Banking & Secure ID” svn129694 followed by “Configuration Secure Authentication” svn138990. The evaluator’s independent tests performed during this second re-evaluation of the TOE were executed on JCOP 4 P71 v4.7 R1.00.4, namely “Configuration Banking & Secure ID” svn129694. The evaluator assessed the differences between the TOE variants and concluded the results from the testing of JCOP 4 P71 v4.7 R1.00.4 were equally applicable to the other 3 variants of the TOE.

The testing performed during this fourth re-evaluation was executed on the new configuration JCOP 4 P71 v4.7 R1.02.4. As the JCOP implementation is the same between versions R1.01.4 and R1.02.4, the test results are considered to be equally applicable to the other four (4) variants 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 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 Reused Evaluation Results

This is a re-certification. Evaluation results of the earlier version of the TOE have been reused, including vulnerability analysis and testing results.

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE, by use of five (5) site certificates and associated Site Technical Audit Reports. 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 P71 together with the configuration identifiers:

Configuration	JCOP Version
Configuration Banking & Secure ID	JCOP 4 P71 v4.7 R1.00.4 JCOP 4 P71 v4.7 R1.01.4 JCOP 4 P71 v4.7 R1.02.4
Configuration Secure Authentication	JCOP 4 SE050 v4.7 R2.00.11 JCOP 4 SE050 v4.7 R2.03.11

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

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

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

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The JCOP 4 P71, Security Target for JCOP 4 P71 / SE050, Rev. 4.8, 08 August 2022 *[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
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

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[AIS20] Bundesamt fuer Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitaetsklassen und Evaluationsmethodologie fuer deterministische Zufallszahlen-generatoren, Version 2.1, 02 December 2011

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[ETR] Evaluation Technical Report NXP "JCOP 4 P71" – EAL6+, 19-RPT-542, v11.0, 14 September 2022

[ETRfC] Evaluation Technical Report for Composition NXP "JCOP 4 P71" – EAL6+, 19-RPT-177, v14.0, 14 September 2022

[GP] GlobalPlatform Card Specification, GPC_SPE_034, v2.3, October 2015

[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)

[N7121-CR] BSI-DSZ-CC-1136-V3-2022 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, 07 September 2022

[N7121-ETRfC] Evaluation Technical Report for Composite Evaluation (ETR COMP) NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) B1, version 2.0, 25 August 2022

[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, registered under the reference BSI, BSI-CC-PP-0099-2017).

[ST] JCOP 4 P71, Security Target for JCOP 4 P71 / SE050, Rev. 4.8, 08 August 2022

[ST-lite] JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050, Rev. 4.8, 08 August 2022

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

(This is the end of this report.)