Certification Report

JCOP 4.5 P71

Sponsor and developer: ***NXP Semiconductors Germany GmbH***
Beiersdorfstrasse 12
22529 Hamburg
Germany

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-2300127-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300127-01**
Author(s):	**Jordi Mujal**
Date:	**16 January 2024**
Number of pages:	**14**
Number of appendices:	**0**

CONTENTS

Foreword

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

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

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

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

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

Recognition of the Certificate

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

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the JCOP 4.5 P71. The developer of the JCOP 4.5 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 is a Java Card with a GP Framework, it is a composite product consisting of a certified Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. The TOE uses one or more communication interfaces to communicate with its environment. The TOE includes the JCVM, JCRE, JCAPI and the GP Framework. Also included is optional functionality and the Secure Box mechanism. Secure Box Native Libraries provide native functions for untrusted third parties and are not part of the TOE.

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 02 August 2022 (CC-22-0313985). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 16 January 2024 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 major changes from previous evaluations are:

- The underlying HW platform was recertified.

- The Security Target of the certified TOE has been updated to include the updated HW platform and some SFRs are rephrased.

- Guidance is updated.

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 4.5 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 4.5 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).

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

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the JCOP 4.5 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 N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) Customer Option: NOS-ROM See *[HW-CERT]* for more details.	A1
	IC Dedicated Test Software – Test Software	11.6.5
	IC Dedicated Support Software - Boot Software - Firmware - Library Interface	11.6.5 11.6.5 11.6.5
	IC Dedicated Support Software - Crypto Library	1.1.2
	Library - Communication Library - CRC Library - Memory Library	7.10.2 1.1.8 1.2.3.1
Software	JCOP 4.5 OS OS Updater Modules	JCOP 4.5 OS Platform ID = J3R6000373181200 ROM ID = B3375FE9B5508BC4 Patch ID = 0000000000000000 (svn = 226072)
	Variant 1	Platform Build ID = 6D20B6197D635E7C OS Core ID = 55606FD4BEECF3CD
	Variant 2	Platform Build ID = 5314F0A7BAE6B138 OS Core ID = 318CCEEB284A3AF9

To ensure secure usage a set of guidance documents is provided, together with the JCOP 4.5 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 following cryptographic algorithms are supported:

- Data Encryption Standard with 3 keys (3DES) for en-/decryption (CBC and ECB) and MAC generation and verification (Retail-MAC, CMAC and CBC-MAC).
- Advanced Encryption Standard (AES) for en-/decryption (CBC, ECB and counter mode) and MAC generation and verification (CMAC, CBC-MAC).
- Rivest Shamir Adleman asymmetric algorithm (RSA) and RSA CRT for en-/ decryption and signature generation and verification.
- Modular and ECC point arithmetic functions not provided by the standard Java Card API
- RSA and RSA Chinese Remainder Theorem (CRT) key generation.
- Elliptic Curve Cryptography (ECC) over GF(p) for signature generation and verification (ECDSA).

- ECC over GF(p) key generation.
- Random number generation according to class DRG.3 or DRG.4 of AIS 20.
- Diffie-Hellman with ECDH and modular exponentiation.
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithm.

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

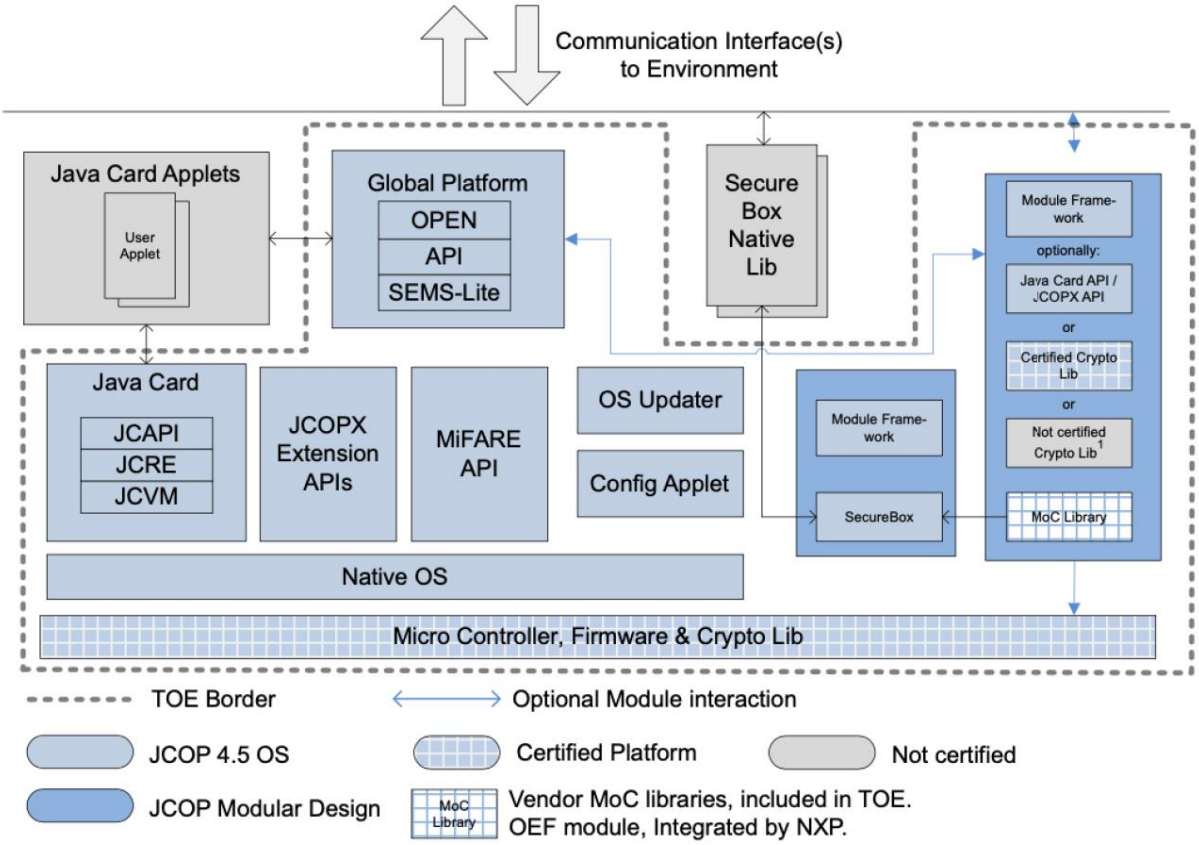
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The following (non-TSF) cryptographic primitives are supported but no there is no security claim on them:

- KoreanSEED
- 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

2.4 Architectural Information

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



2.5 Documentation

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

Identifier	Version
JCOP 4.5 P71, User manual for JCOP 4.5 P71, User Guidance and Administrator Manual	Rev. 1.8 – 2023-04-03.

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 performed extensive testing on functional specification, subsystem and module level, covering all security functions and aspects of the TSF. The developer uses a set of industry standard and proprietary test suites and tools. The TOE is tested both in its physical implementation and using simulator and emulator platforms in order to cover all relevant aspects. During testing, the TOE is identified by its SVN number.

The developer uses a distributed and fully automated test environment to allow the execution of a vast number of parallel tests. All results are logged and any unexpected results are flagged for analysis.

The overall completeness is being monitored using code coverage tools. For each tool, the developer has investigated and documented inherent limitations that can lead to coverage being reported as less than 100%. For all such cases, the developer provided a "gap" analysis with rationales.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

The evaluators witnessed a selection of the developer tests covering various aspects of the TOE, as well as areas where the code coverage approach has limitations.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluator independent testing was focused on verifying the TOE identification mechanisms to ensure that the preparative guidance procedures are sufficient, and on the adherence of the TOE implementation to the Java Card and GlobalPlatform specifications for selected corner cases.

2.6.2 Independent penetration testing

The independent vulnerability analysis was performed according to *[CC]* and *[JIL-AM]*. The ratings have been calculated according to *[JIL-AAPS]*. Overall, it was conducted along the following steps:

- When evaluating the evidence in classes ASE, ADV and AGD, the evaluator considered whether potential vulnerabilities could already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- 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 evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis used the attack methods in *[JIL-AM]* and rating calculations in *[JIL-AAPS]*.
- 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. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that were deemed appropriate.

The total test effort expended by the evaluators in the original evaluation was 17 weeks. During that test campaign, 47% of the total time was spent on Perturbation attacks, 41% on side-channel testing, and 12% on logical tests. During this evaluation, the total test effort expended by the evaluators was 4 weeks. During that test campaign, 50% of the total time was spent on Perturbation attacks, 25% on side-channel testing, and 25% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". 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).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

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

2.7 Reused Evaluation Results

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 development and production of the TOE, by use of five Site Technical Audit Reports. In addition, 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 JCOP 4.5 P71.
The TOE can be identified by means of the IDENTIFY command as described *[ST]* section 1.3.4 and *[UG]* chapter 2. The IDENTIFY command also returns information about modules present in the TOE.

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 4.5 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_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 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)
- Elliptic Curve Direct Anonymous Attestation (ECDAA)
- ECC based on Edwards and Montgomery curves

Which are out of scope as there are no security claims relating to these.

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 4.5 P71 Security Target, Rev. 2.6, 11 December 2023 *[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
CFB	Cipher Feedback
CTR	Counter
DES	Data Encryption Standard
CPLC	Card Production Life Cycle
CRT	Chinese Remainder Theorem
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DRG	Deterministic Random Generator
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDAA	Elliptic Curve Direct Anonymous Attestation
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
EDC	Error Detection Code
EdDSA	Elliptic Curve Edwards-curve Digital Signature Algorithm
eUICC	embedded Universal Integrated Circuit Card
GCM	Galois/Counter Mode
GF	Galois Field
GP	Global Platform
GCM	Galois/Counter Mode
GSMA	Groupe Speciale Mobile Association
IM4	Image4
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MNO	Mobile Network Operators
NFC	Near-Field Communication
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile

RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SMB	Secure Mailbox
TOE	Target of Evaluation
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
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 “NXP JCOP 4.5 P71” – EAL6+, 23-RPT-1351, version 2.0, 20 December 2023
[ETRfC]	Evaluation Technical Report for Composition “NXP JCOP 4.5 P71” – EAL6+, 23-RPT-1350, version 2.0, 20 December 2023
[HW-CERT]	Certification Report, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-1149-V3-2023
[HW-ETRfC]	Evaluation Technical Report for Composite Evaluation (ETR COMP) for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Version 2, 01 December 2023
[HW-ST]	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) Security Target Lite, Rev. 1.8, 1 December 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	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 2.6, 02 August 2022
[PP_0099]	Java Card System - Open Configuration Protection Profile, December 2017, Version 3.0.5, registered under the reference BSI-CC-PP-0099-2017
[ST]	JCOP 4.5 P71 Security Target, Rev. 2.6, 11 December 2023
[ST-lite]	JCOP 4.5 P71 Security Target Lite, Rev. 2.6, 11 December 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)