Certification Report

JCOP 4 SE050M

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-0075446-CR2**
Report version:	**1**
Project number:	**0075446_2**
Author(s):	**Denise Cater**
Date:	**23 January 2022**
Number of pages:	**15**
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

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 SE050M. The developer of the JCOP 4 SE050M 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 SE050M, 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 *[ST]* section 1.3.2.

It is noted that this TOE is a modification of an already certified product “JCOP 4 P71” (CC-22-180212/2, reported in *[P71_CR]*), which included the configurations “JCOP 4 SE050 v4.7 R2.00.11” and “R2.03.11”. This TOE, JCOP 4 SE050M (v4.7 R3.00.11), includes a number of local changes from JCOP 4 SE050 v4.7 R2.00.11 and JCOP 4 SE050 v4.7 “R2.03.11”.

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 03 March 2020. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 23 January 2023 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

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

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-1136-V3-2022 (previously certified with the identifier BSI-DSZ-CC-1040), which resulted in a new logical configuration R4. It should be noted that the new configuration R4 of the hardware platform is not be used by this TOE, JCOP 4 on SE050M.

In addition, the DRG.4 claim was clarified in *[ST]* and the guidance documents, and the list of sites related to the JCOP development was refreshed along with the associated site audit results.

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 SE050M, 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 SE050M 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 SE050M from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	**Version**
IC Hardware (Hard macro instantiated with a wafer, module or package)	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library *(The SE050 hardware is an instantiation of the N7121 hard macro with I2C sidecar.)*	B1
IC Dedicated Test Software	Test Software	9.2.3
IC Dedicated Support Software	Boot Software	9.2.3
	Firmware	9.2.3
	Flashloader OS	1.2.5
	Library Interface	9.2.3
	○ Communication Library	6.0.0
	○ CRC Library	1.1.8
	○ Memory Library	1.2.3
	○ Flash Loader Library	3.6.0
	System Mode OS	13.2.3
	Crypto Library	0.7.6
	○ RNG Lib	0.7.6
	○ RNG HealthTest Lib	0.7.6
	○ Sym. Cipher Lib	0.7.6
	○ KeyStoreMgr Lib	0.7.6
	○ Sym. Utilities Lib	0.7.6
	○ RSA Lib	0.7.6
	○ RSA Key Generation Lib	0.7.6
	○ ECC Lib	0.7.6
	○ SHA Library & Hash Library	0.7.6
	○ Asym. Utilities Lib	0.7.6
IC Embedded Software	JCOP OS + Modules Patch ID = “0000000000000001” Platform Build ID = “9EE6CC6E53D85899” Revision = “156997” ROM ID = “2E5AD88409C9BADB” Platform ID = “J3R3510265451100”	svn 156997 Configuration “JCOP 4 SE050M v4.7 R3.00.11”

To ensure secure usage a set of guidance documents is provided, together with the JCOP 4 SE050M. 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 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:

- 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

2.3 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:

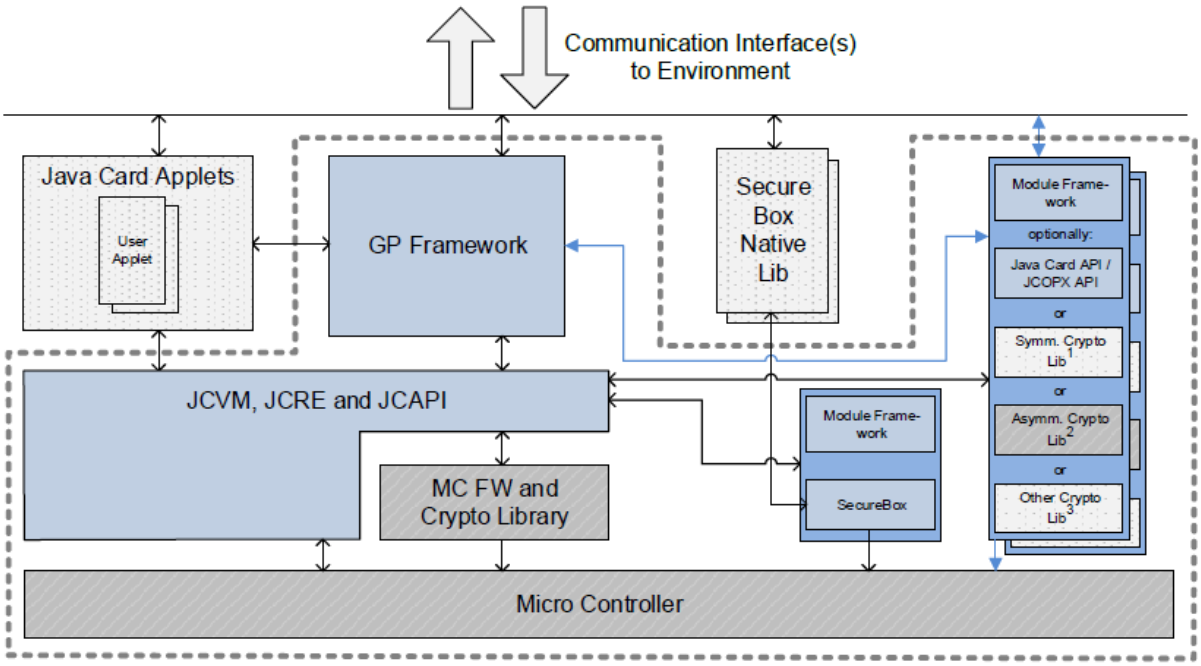

Figure 1 Logical architecture of the TOE

In the above figure, the 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.

The TOE is a composite product on top of CC certified Hardware, Firmware and Crypto Library. Part of the TOE are the JCVM, JCRE, JCAPI and the GP Framework. Also included is optional functionality and the Secure Box mechanism. The Secure Box Native Library provide 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 SE050M v4.7 R3.00.11, User Manual for JCOP 4 SE050M	Rev.1.8 28 October 2022
SE050M Embedded Secure Element, Preliminary Data Sheet	Rev. 3.2 27 October 2022

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 FSP, 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.

The ordering dependencies were analysed. The developer performed random order testing to identify any ordering dependencies. This was done for Unit Tests, System Tests and Acceptance Tests. For

most (commercial) test suites there are no claims on ordering dependencies. For these situations tests were executed both in random order as in alphabetical order and the results were compared.

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 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.

During the baseline evaluation 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 witnessing sessions were used to sample and check the actual test results. The following three categories were selected for test witnessing:

- Demonstrate how TOE is identified during functional testing
- Spot checks on coverage and set-up
- Testing of the Global Platform secure messaging protocol

For the testing performed by the evaluators, the developer has provided samples and a test environment.

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 this re-evaluation, the TOE implementation was not changed and no additional developer tests were performed.

2.6.2 Independent penetration testing

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-AAPS]*.
- 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.

During the baseline evaluation a total of 14 penetration tests were identified and a total of 17.5 weeks of penetration testing was performed.

The vulnerability analysis was refreshed as part of this re-evaluation and the total test effort expended by the evaluators during this re-evaluation was 8.5 weeks. During that test campaign, 23% of the total time was spent on Perturbation attacks, 65% on side-channel testing, and 12% on logical tests.

2.6.3 Test configuration

During the baseline evaluation the TOE was tested (Unit Tests, Integration Tests and 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 (ISO1443)

Testing has been performed on the TOE (J3R3510265451100) as well as earlier revisions (previously certified by NSCIB with certificate CC-20-180212), such as:

- J3R35101FA9E0400 “JCOP 4 P71” – v4.7 R1.00.4
- J3R3510236310400 “JCOP 4 P71” – v4.7 R1.01.4

During this re-evaluation, assurance from penetration testing was obtained from penetration tests performed on the related product “JCOP 4 P71” – v4.7 R1.02.4 (J3R35103B01B0400,) as part of the evaluation of JCOP 4 on P71, as report in *[P71_CR]*. The evaluator assessed the differences between the related product and the TOE and determined the assurance gained from testing the related product is valid for the TOE due to the minor differences between the versions.

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 by use of 5 site certificates and Site Technical Audit Reports. Sites involved in the development and production of the hardware platform were reused by composition.

No sites have been visited as part of this re-evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number JCOP 4 SE050M, together with the configuration identifier “JCOP 4 SE050M v4.7 R3.00.11” which can be identified through the modules and versions listed when issuing the IDENTIFY command as described in the *User Guidance and Administration Manual*.

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 SE050M, 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 proprietary or non-standard algorithms, protocols and implementations was not rated in the course of this evaluation:

- 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.

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 SE050M Security Target for JCOP 4 SE050M, Rev. 2.2, 03 January 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
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
MITM	Man-in-the-Middle
MRTD	Machine Readable Travel Document
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
SMM	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
[ETR]	Evaluation Technical Report “JCOP 4 SE050M” – EAL6+, 20-RPT-108, Version 8.0, 19 January 2023
[ETRfC]	Evaluation Technical Report for Composition NXP “JCOP 4 SE050M” – EAL6+, 20-RPT-163, Version 8.0, 19 January 2023
[HW-CERT]	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
[HW-ETRfC]	ETR for composite evaluation according to AIS 36 for the Product 7121, BSI-DSZ-CC-1136-2021, Version 2, 25 August 2022
[HW-ST]	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, Rev 2.6, 13 June 2022
[GP]	GlobalPlatform Card Specification, v2.3.1, GPC_SPE_034, GlobalPlatform Inc., March 2018
[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, Version 3.0.5, December 2017, registered under the reference BSI-CC-PP-0099-2017)
[P71_CR]	Certification Report JCOP 4 P71, NSCIB-CC-180212-CR5, version 1, 26 September 2022 With maintenance addendum applied: Assurance Continuity Maintenance Report JCOP 4 P71, NSCIB-CC-180212-5MA1, version 1, 23 January 2023
[ST]	JCOP 4 SE050M Security Target for JCOP 4 SE050M, Rev. 2.2, 03 January 2023
[ST-lite]	JCOP 4 SE050M Security Target Lite for JCOP 4 SE050M, Rev 2.2, 03 January 2023
[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.)