

Certification Report

JCOP 4.7 SE051

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-2500026-01-CR**

Report version: **1**

Project number: **NSCIB-2500026-01**

Author(s): **Haico Haak**

Date: **18 February 2026**

Number of pages: **15**

Number of appendices: **0**

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

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	9
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	10
2.6.4 Test results	11
2.7 Reused Evaluation Results	11
2.8 Evaluated Configuration	11
2.9 Evaluation Results	11
2.10 Comments/Recommendations	11
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, 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.

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

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 4.7 SE051. The developer of the JCOP 4.7 SE051 is NXP Semiconductors Germany GmbH located in Hamburg, Germany and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE, which is referred to as JCOP 4.7 SE051, is a Java Card with a GP Framework. The TOE is a composite product on top of a CC certified Hardware (Micro Controller component) with IC Dedicated Software and Crypto Library (MC FW and Crypto Library component). The software stack, which is stored on the Micro Controller and executed by the Micro Controller, can be further split into the following components:

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

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

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 27 March 2023 (CC-23-0095534). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 18 February 2026 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:

- Recertification of underlying platform resulting in user guidance updates
- Life cycle changes resulting in TOE user guidance updates

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the JCOP 4.7 SE051, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the JCOP 4.7 SE051 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report [ETR]¹ for this product provide sufficient evidence that the TOE meets the EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE summary specification with architectural design summary) and ALC_FLR.1 (Basic flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 [CEM] for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [CC] (Parts I, II and III).

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



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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the JCOP 4.7 SE051 from NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version	
IC Hardware	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) (The SE051 hardware is an instantiation of the N7121 hard macro with I2C side-car.)	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	0.7.7
	RNG Lib	0.7.6	0.7.7
	RNG HealthTest Lib	0.7.6	0.7.7
	Sym. Cipher Lib	0.7.6	0.7.7
	KeyStoreMgr Lib	0.7.6	0.7.7
	Sym. Utilities Lib	0.7.6	0.7.7
	RSA Lib	0.7.6	0.7.7
	RSA Key Generation Lib	0.7.6	0.7.7
	ECC Lib	0.7.6	0.7.7
SHA Library & Hash Library	0.7.6	0.7.7	
Asym. Utilities Lib	0.7.6	0.7.7	
IC Embedded Software	JCOP OS + Modules Configuration " JCOP 4 SE051 v4.7 R3.01.11 " Platform ID = "J3R351029B411100" Platform Build ID (IOT Full)= "4C0954E73E773C6E" Platform Build ID (IOT Reduced)= "1A08FA5067B5F256" Patch ID = "0000000000000001" ROM ID = "2E5AD88409C9BADB"	svn 170817	
	JCOP OS + Modules Configuration " JCOP 4 SE051 v4.7 R3.02.11 " Platform ID = "J3R35103B4821100" Platform Build ID (IOT Full)= "2C756560A10E9893" Platform Build ID (IOT Reduced)= "E051774C8DBE2C33" Patch ID = "0000000000000001" ROM ID = "2E5AD88409C9BADB"	svn 242818	

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

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

2.2 Security Policy

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

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

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

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

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the [ST].

2.3.2 Clarification of scope

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

2.4 Architectural Information

The TOE is a Java Card with a GP Framework. It can be used to load and execute off-card verified Java Card applets. It is a composite product on top of a CC certified Hardware (Micro Controller component) with IC Dedicated Software and Crypto Library (MC FW and Crypto Library component). The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:

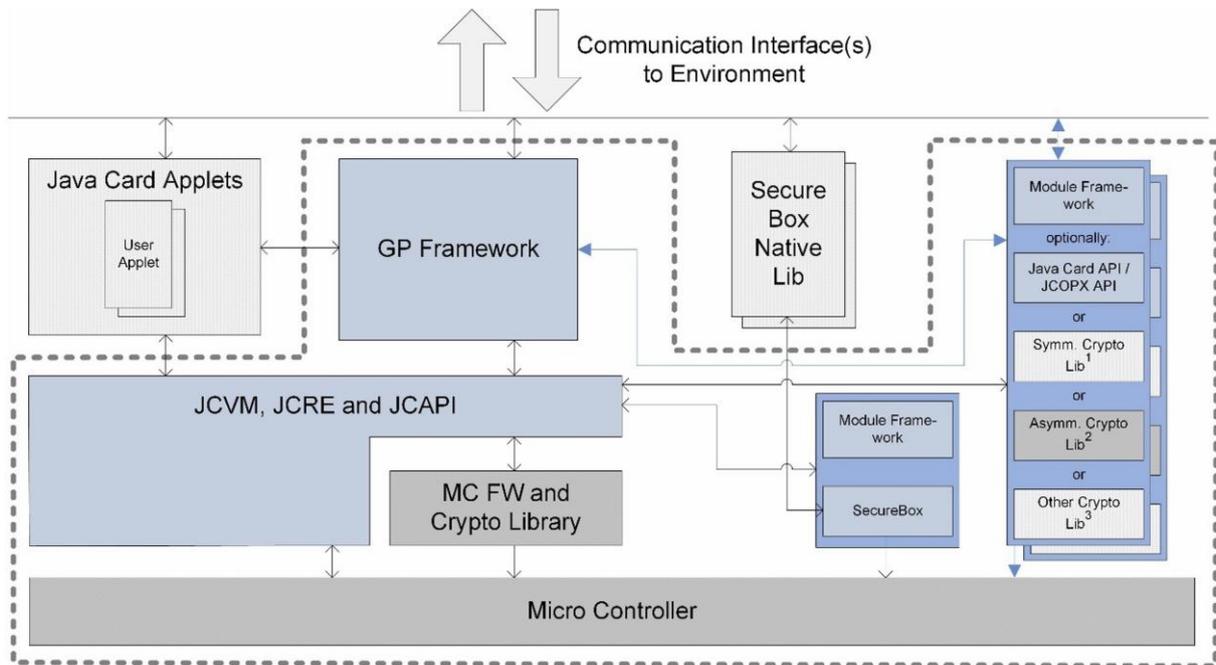


Figure 1 Logical architecture of the TOE

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

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

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

2.5 Documentation

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

Identifier	Version
JCOP 4.7 SE051, User manual for JCOP 4.7 SE051, User Guidance and Administrator Manual	Rev.2.5 24 June 2025
SE051, Plug & Trust Secure Element, Product data sheet	Rev. 1.6 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 performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

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.

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

2.6.2 Independent penetration testing

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

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in 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 vulnerability analysis has been refreshed during this re-evaluation.

During the baseline evaluation a total of 4 weeks and 1 day of penetration testing was performed for the TOE. The test cases were split 24% perturbation testing, 71% side channel attacks and 5% software logical attacks.

During the first re-evaluation, a further 5.5 weeks test effort was expended by the evaluators, of which 18.2% of the total time was spent on Perturbation attacks, 72.7% on side channel testing, and 9.1% on logical tests.

During the second re-evaluation, a further 5 weeks test effort was expended by the evaluators, of which 40% of the total time was spent on Perturbation attacks, 40% on side-channel testing, and 20% on logical tests.

The total test effort expended in this re-evaluation by the evaluators was 4 weeks. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 25% perturbation attacks, 0% retrieving keys with FA, 50% side-channel attacks, 0% attacks on RNG, 25% of the total time was spent on logical attacks, 0% on fuzzing attacks, and 0% application isolation penetration tests.

2.6.3 Test configuration

Testing was performed on the configuration JCOP 4 P71 v4.7 R1.01.4 and JCOP 4 P71 R1.00.4. Due to the minor differences between these configurations, the results equally apply to other configurations 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.

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

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

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition.

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 4.7 SE051, together with the configuration identifiers:

- JCOP 4 SE051 v4.7 R3.01.11
- JCOP 4 SE051 v4.7 R3.02.11

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

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the [EAR], which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to [COMP] a derived document [ETRFc] was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "Pass".

Based on the above evaluation results the evaluation lab concluded the JCOP 4.7 SE051, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ASE_TSS.2 and ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target [ST].

The Security Target claims 'demonstrable' conformance to the Protection Profile [PP].

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:

- 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
- PACE key agreement and PACE CAM

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

3 Security Target

The JCOP 4.7 SE051 Security Target Rev. 2.12 — 18 December 2025 [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
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SSM	Scalable Security Module
SPA/DPA	Simple/Differential Power Analysis
SSH	Secure Shell
TOE	Target of Evaluation

5 Bibliography

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

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report “JCOP 4.7 SE051” – EAL6+, Version 2.0, 17 February 2026
[ETRFc]	Evaluation Technical Report for Composition “JCOP 4.7 SE051” – EAL6+, Version 2.0, 17 February 2026
[HW-CERT]	Deutsches IT-Sicherheitszertifikat BSI-DSZ-CC-1136-V5-2026 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, 30 January 2026, BSI
HW-CR]	BSI-DSZ-CC-1136-V5-2026 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, 30 January 2026, BSI
[HW-ETRFc]	Evaluation Technical Report for Composite Evaluation (ETR COMP) NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) B1, version 4, 10 December 2025
[HW-ST]	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target, Rev.3.4, 9 December 2025
[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 3.2.1, February 2024
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[GP]	Global Platform Inc., GlobalPlatform Card Specification, Version 2.3.1, March 2018
[PP_0099]	Java Card System - Open Configuration Protection Profile, Version 3.0.5, December 2017, registered under the reference BSI-CC-PP-0099-2017
[ST]	JCOP 4.7 SE051 Security Target Rev. 2.12 — 18 December 2025
[ST-lite]	JCOP 4.7 SE051 Security Target Lite Rev. 2.12 — 18 December 2025

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

(This is the end of this report.)