

Certification Report

Identity Applet v4.0/QSCD on NXP JCOP 4.5 P71

Sponsor:	<i>NXP Semiconductors Germany GmbH</i> Beiersdorfstrasse 12 22529 Hamburg Germany
Developer:	<i>ID&Trust Kft.</i> Versec sor 18. 1021 Budapest Hungary
Evaluation facility:	<i>Keysight Technologies Netherlands Riscure B.V.</i> Delftechpark 49 2628 XJ Delft The Netherlands
Report number:	NSCIB-CC-2400103-01-CR
Report version:	1
Project number:	NSCIB-2400103-01
Author(s):	Kjartan Jæger Kvassnes
Date:	13 February 2026
Number of pages:	12
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	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	6
2.3.1 Assumptions	6
2.3.2 Clarification of scope	6
2.4 Architectural Information	7
2.5 Documentation	7
2.6 IT Product Testing	7
2.6.1 Testing approach and depth	7
2.6.2 Independent penetration testing	8
2.6.3 Test configuration	8
2.6.4 Test results	8
2.7 Reused Evaluation Results	8
2.8 Evaluated Configuration	8
2.9 Evaluation Results	9
2.10 Comments/Recommendations	9
3 Security Target	10
4 Definitions	10
5 Bibliography	11

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 IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71. The developer of the IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71 is ID&Trust Kft. located in Budapest, Hungary and NXP Semiconductors Germany GmbH was 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 addressed by the current ST is a Qualified Signature Creation Device (QSCD) representing a contact or contactless smart card which is able to generate signature creation data (SCD) and create qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized signatory can use it.

The TOE has been evaluated by Keysight Technologies Netherlands Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 13 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 scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the IDentity Applet v4.0/QSCD on NXP 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 IDentity Applet v4.0/QSCD on NXP 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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.

The TOE is stated as a Qualified Signature Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by Keysight Technologies Netherlands Riscure B.V. included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 7 0.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature Creation Devices.

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 IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71 from ID&Trust Kft. located in Budapest, Hungary.

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) registered under the reference BSI-DSZ-CC-1149-V4-2025	A1
OS	JCOP 4.5 OS registered under the reference NSCIB-CC-2300127-02	Platform ID: J3R6000373181200 ROM ID: B3375FE9B5508BC4 Build ID: 6D20B6197D635E7C Core ID: 55606FD4BEECF3CD Patch ID: 0000000000000000
Applet	IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71	v4.0.9219

To ensure secure usage a set of guidance documents is provided, together with the IDentity Applet v4.0/QSCD on NXP 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 1.4.4.

2.2 Security Policy

The TOE is a Qualified Signature Creation Device (QSCD) representing a contact or contactless smart card which is able to generate signature creation data (SCD) and create qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized signatory can use it.

The TOE support the following security features:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control;
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The TOE supports and implements cryptographic mechanisms that are compliant with Electronic Signatures and Trust Infrastructures (ESI) Cryptographic Suites, ETSI TS 119 312 V1.5.1.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

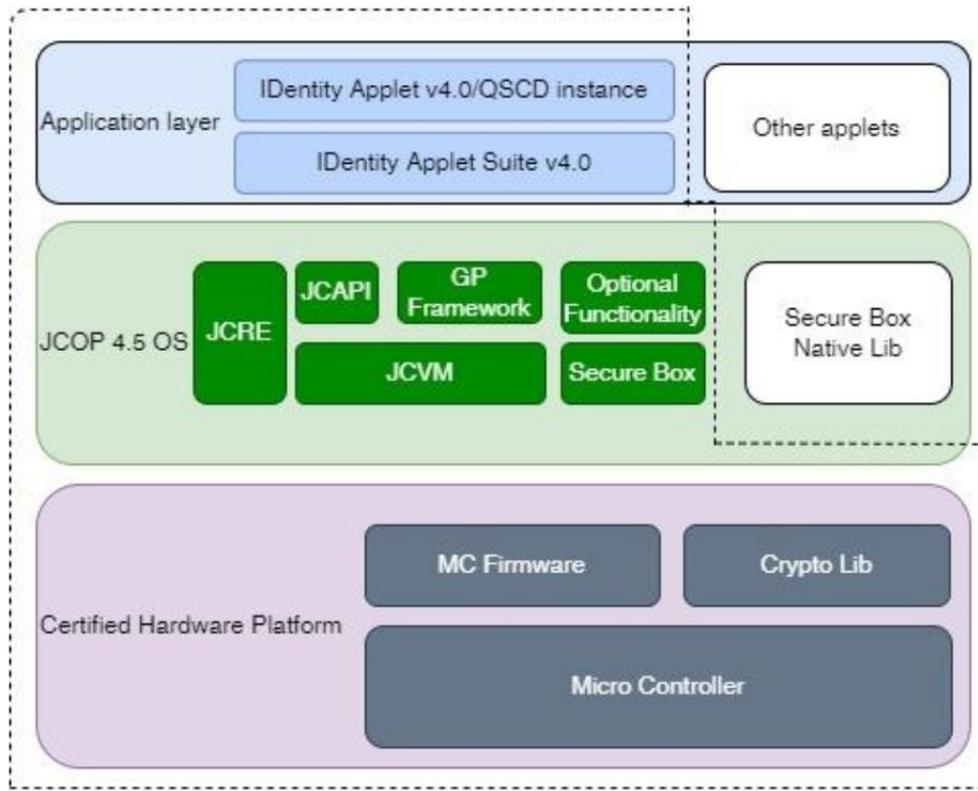
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the [ST].

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 architecture can be depicted as follows:



2.5 Documentation

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

Identifier	Version
ID&Trust, Identity Applet Suite v4.0 Administrator's Guide, dated 08 December 2025	v4.0.9
ID&Trust, Identity Applet Suite v4.0 Users' Guide, 08 December 2025	v4.0.11

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 SFR-enforcing 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

The vulnerability analysis focused on the functionality implemented by the applet TOE, but considers the entire composite TOE where needed. Any potential vulnerabilities that may arise from the usage of the underlying platform are considered and assessed. The assessment is structured based on the JHAS attack methods for smartcards and similar devices [JIL-AMS].

For each attack method, we describe how the attack method applies to the TOE. The following is considered for each attack method:

- The design and implementation of the features relevant for the attack method
- Specific attack techniques from the evaluator's attack repository
- Implemented countermeasures
- Observations from the platform evaluation
- Platform user guidance

Based on these items, the lab determined whether an attack method was applicable to the TOE and should be tested during the penetration testing phase. During the assessment, the evaluator also examined the results of the evaluation of the underlying platform, and confirmed that any obligations or guidance from the platform have been correctly covered and followed.

The total test effort expended by the evaluators was 3 weeks. During that test campaign, 0% of the total time was spent on Perturbation attacks, 0% was on physical attacks, 0% was on overcoming sensors and filters, 67% was on perturbation attacks, 0% was on retrieving keys with FA, 0% was on side-channel attacks, 0% was on exploitation of test features, 0% was on attacks on RNG, 0% was on ill-formed Java Card applications, 33% was on software attacks, and 0% was on application isolation penetration tests.

2.6.3 Test configuration

The TOE is only available in one security configuration, IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71.

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.

2.7 Reused Evaluation Results

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.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the [ETR], which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is “Pass”.

Based on the above evaluation results the evaluation lab concluded the IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target [ST].

The Security Target claims 'strict' conformance to the Protection Profile [EN419211-2], [EN419211-4] and [EN419211-5].

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 Security Target IDentity Applet v4.0/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS, Version 1.0, Dated 12 January 2026 [ST] is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

DCAP	eIDAS Dutch Conformity Assessment Process
eMRTD	electronic MRTD
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
TOE	Target of Evaluation
QSCD	Qualified Signature/Seal Creation Device

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
[EU-REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation(EU) No 910/2014 as regards establishing the European Digital Identity Framework
[eIDAS-REP]	eIDAS Conformity Assessment Report for IDentity Applet v4.0, Version 2.0, Dated 13 February 2025
[EN419211-2]	EN 419 211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation, 2013, registered under the reference BSI-CC-PP-0059-2009-MA-02
[EN419211-4]	EN 419 211-4:2013, Protection profiles for Secure signature creation device — Part 4: Extension for devices with key generation and trusted channel to certificate generation application, 2013, registered under the reference BSI-CC-PP-0071-2012-MA-01
[EN419211-5]	EN 419211-5:2013 Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, 2013, registered under the reference BSI-CC-PP-0072-2012-MA-01
[ETR]	ID&Trust Ltd. IDentity Applet v4.0/QSCD on NXP JCOP 4.5 P71 v4.0.9219 Evaluation Technical Report, Version 2.0, Date 13 February 2026
[HW-CERT]	Certification Report BSI-DSZ-CC-1149-V4-2025 for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), dated 5 September 2025
[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 4, 2025-08-07, TÜV Informationstechnik GmbH. (confidential document)
[HW-ST]	Security Target Lite BSI-DSZ-CC-1149-V4-2025, NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Version 2.0, 2025-08-04, NXP Semiconductors
[OS-CERT]	Certification report JCOP 4.5 P71. NSCIB-CC-2300127-02-CR, Version 1, dated 15 December 2025

[OS-ETRFc]	Evaluation Technical Report for Composition “NXP JCOP 4.5 P71” – EAL6+, 25-RPT-132, version 5.0, 11 December 2025
[OS-ST]	JCOP 4.5 P71 Security Target Lite, Rev. 2.9, 05 September 2025
[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)
[JIL_QSCD]	Security Evaluation and Certification of Qualified, Electronic Signature/Seal Creation Devices, JIL Interpretations for Security Certification according to eIDAS Regulation 910/2014, Version 1.0, July 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Security Target IDentity Applet v4.0/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS, Version 1.0, Dated 12 January 2026

(This is the end of this report.)