

## Certification Report

### Identity Applet v4.0/BAC on NXP JCOP 4.5 P71

Sponsor:	<b><i>NXP Semiconductors Germany GmbH</i></b> Beiersdorfstrasse 12 22529 Hamburg Germany
Developer:	<b><i>ID&amp;Trust Kft.</i></b> Versec sor 18. 1021 Budapest Hungary
Evaluation facility:	<b><i>Keysight Technologies Netherlands Riscure B.V.</i></b> Delftechpark 49 2628 XJ Delft The Netherlands
Report number:	<b>NSCIB-CC-2400101-01-CR</b>
Report version:	<b>1</b>
Project number:	<b>NSCIB-2400101-01</b>
Author(s):	<b>Kjartan Jæger Kvassnes</b>
Date:	<b>13 February 2026</b>
Number of pages:	<b>12</b>
Number of appendices:	<b>0</b>

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

# CONTENTS

<b>Foreword</b>	<b>3</b>
<b>Recognition of the Certificate</b>	<b>4</b>
International recognition	4
European recognition	4
<b>1 Executive Summary</b>	<b>5</b>
<b>2 Certification Results</b>	<b>6</b>
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	7
2.3.1 Assumptions	7
2.3.2 Clarification of scope	7
2.4 Architectural Information	7
2.5 Documentation	7
2.6 IT Product Testing	8
2.6.1 Testing approach and depth	8
2.6.2 Independent penetration testing	8
2.6.3 Test configuration	8
2.6.4 Test results	9
2.7 Reused Evaluation Results	9
2.8 Evaluated Configuration	9
2.9 Evaluation Results	9
2.10 Comments/Recommendations	9
<b>3 Security Target</b>	<b>10</b>
<b>4 Definitions</b>	<b>10</b>
<b>5 Bibliography</b>	<b>12</b>

## 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/BAC on NXP JCOP 4.5 P71. The developer of the IDentity Applet v4.0/BAC 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 is a contactless integrated circuit chip with IC Dedicated Software (Micro Controller Firmware, Crypto Library), Embedded Software (JCOP 4.5) and IDentity Applet v4.0/BAC, containing components for a machine readable travel document (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control.

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/BAC 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/BAC 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]<sup>1</sup> for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC\_DVS.2 (Sufficiency of security measures).

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.

---

<sup>1</sup> 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/BAC 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/BAC 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/BAC 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 support the following security features:

The following TOE ensured security functions are the most significant for its operational use:

- Only entities (e.g. terminals) possessing authorisation can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,
  - Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the entity connected
  - Averting of inconspicuous tracing of the travel document,
  - Self-protection of the TOE security functionality and the data stored inside.

The API exposed by IDentity Applet v4.0/BAC allows fast development of cryptographic supported applications for National ID, ePassport, Enterprise ID, Healthcare, Transportation, and Payment applications. IDentity Applet v4.0/BAC is designed for the Java Card family of smart card platforms and specifically for the NXP JCOP IC which is certified according to the CC EAL 6+ both the microprocessor and the JCOP OS as well. The Platform provides:

- Cryptographic algorithms and functionality (3DES, AES, RSA, SHA, ECDSA, RNG, DH, ECDH, etc.);
- GlobalPlatform 2.3 functionality;
- Three different communication protocol (ISO 7816 T=0, T=1, ISO 14443 T=CL (contact-less));
- Java Card 3.0.5 functionality (secure memory management, garbage collection, extended Length APDUs, etc.)

The combination of the internal security mechanisms in combination with the fulfilment of the mandatory guidance requirements ensures that the provided security services and features achieve a high attack resistance.

## 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.

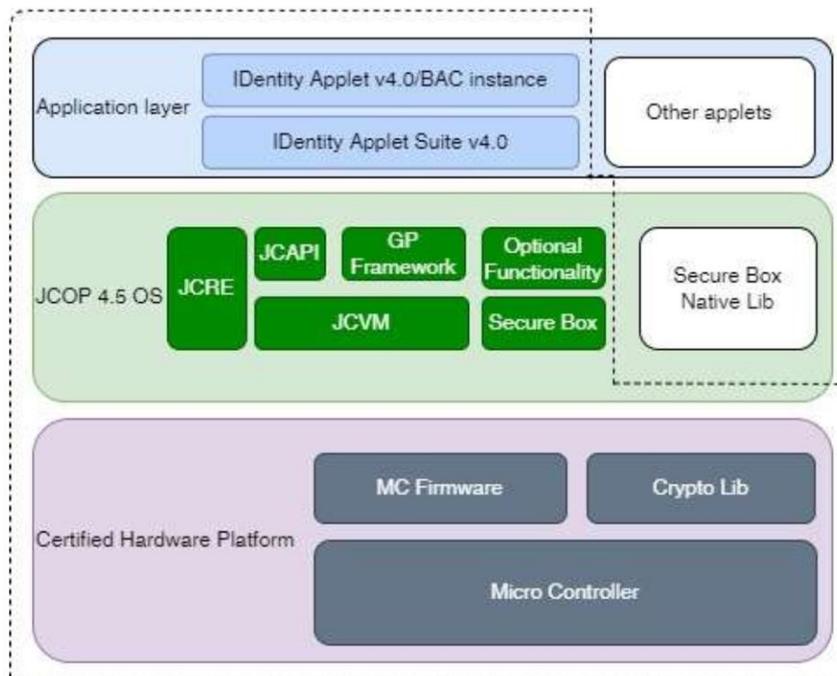
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalised must perform proper and safe personalisation according to the guidance and referred ICAO guidelines.

The environment in which the TOE is used must ensure that the inspection system protects the confidentiality and integrity of the data send and read from the TOE.

## 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, we determine whether an attack method is 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/BAC 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/BAC 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/BAC on NXP JCOP 4.5 P71, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC\_DVS.2**. This implies that the product satisfies the security requirements specified in Security Target [ST].

The Security Target claims 'strict' conformance to the Protection Profile [PP\_0055].

## 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>.

### 3 Security Target

The Security Target IDentity Applet v4.0/BAC/AA - ePassport with BAC and Active Authentication, v1.0, 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:

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
ACL	Access Control List
AES	Advanced Encryption Standard
BAC	Basic Access Control
CA	Chip Authentication
CAM	Chip Authentication Mapping
CGA	Certificate Generation Application
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
CVCA	Country Verifying Certification Authority
DCAP	eIDAS Dutch Conformity Assessment Process
DFA	Differential Fault Analysis
EAC	Extended Access Control
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
eMRTD	electronic MRTD
IC	Integrated Circuit
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems I
JIL	Joint Interpretation Library
LAN	Local Area Network
MAC	Message Authentication Code
MITM	Man-in-the-Middle

MRTD	Machine Readable Travel Document
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key
QSCD	Qualified Signature/Seal Creation Device
RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SCD	Signature Creation Data Select this or the next entry, depending on context.
SCD	Signature Creation Device
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
SM	Secure Messaging
SPA/DPA	Simple/Differential Power Analysis
SSH	Secure Shell
SSL	Secure Sockets Layer
SVD	Signature Verification Data Select this or the next entry, depending on context.
SVD	Signature Verification Device
TA	Terminal Authentication
TCP	Transmission Control Protocol
TRNG	True Random Number Generator
VLAN	Virtual LAN

## 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]	ID&Trust Ltd. IDentity Applet v4.0/BAC on NXP JCOP 4.5 P71 v4.0.9219 Evaluation Technical Report, version 2.0, dated 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 05 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)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP_0055]	Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0055-2009
[ST]	Security Target IDentity Applet v4.0/BAC/AA - ePassport with BAC and Active Authentication, v1.0, 12 January 2026

(This is the end of this report.)