Version 2024-12

# Certification Report

# IDentity Applet v4.0/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) on NXP JCOP 4.5 P71

| | |
|---|---|
| Sponsor: | ***NXP Semiconductors Germany GmbH***<br>**Beiersdorfstrasse 12**<br>**22529 Hamburg**<br>**Germany** |
| Developer: | ***ID&Trust Kft.***<br>**Versec sor 18.**<br>**1021 Budapest**<br>**Hungary** |
| Evaluation facility: | ***Keysight Technologies Netherlands Riscure B.V.***<br>**Delftechpark 49**<br>**2628 XJ Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-2400102-01-CR** |
| Report version: | **1** |
| Project number: | NSCIB-**2400102-01** |
| 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.*

® TrustCB is a registered trademark. Any use or application requires prior approval.

# CONTENTS



® TrustCB is a registered trademark. Any use or application requires prior approval.

# 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.

® TrustCB is a registered trademark. Any use or application requires prior approval.

# 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.

® TrustCB is a registered trademark. Any use or application requires prior approval.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the IDentity Applet v4.0/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) on NXP JCOP 4.5 P71. The developer of the IDentity Applet v4.0/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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 contact or contactless smart card with the IDentity Applet Suite v4.0 configured as IDentity Applet/PACE-EAC1/EAC2. The TOE is applicable as an electronic document (with two applications: ePassport or eID), which compliance to relevant eIDAS standards.

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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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.

® TrustCB is a registered trademark. Any use or application requires prior approval.

[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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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<br>ROM ID: B3375FE9B5508BC4<br>Build ID: 6D20B6197D635E7C<br>Core ID: 55606FD4BEECF3CD<br>Patch ID: 0000000000000000 |
| Applet | IDentity Applet v4.0/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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:

- Only authenticated terminals can get access to the User Data stored on the TOE and use security functionality of the electronic document according to the access rights of the terminal,
- the Electronic Document Holder can control access by consciously presenting his electronic document and/or by entering his secret PIN
- authenticity and integrity of user data can be verified
- confidentiality of user data in the communication channel between the TOE and the connected terminal is provided
- inconspicuous tracing of the electronic document is averted
- its security functionality and the data stored inside are self-protected
- Optionally support the Active Authentication and Chip Authentication mapping.

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.

® TrustCB is a registered trademark. Any use or application requires prior approval.

## 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.

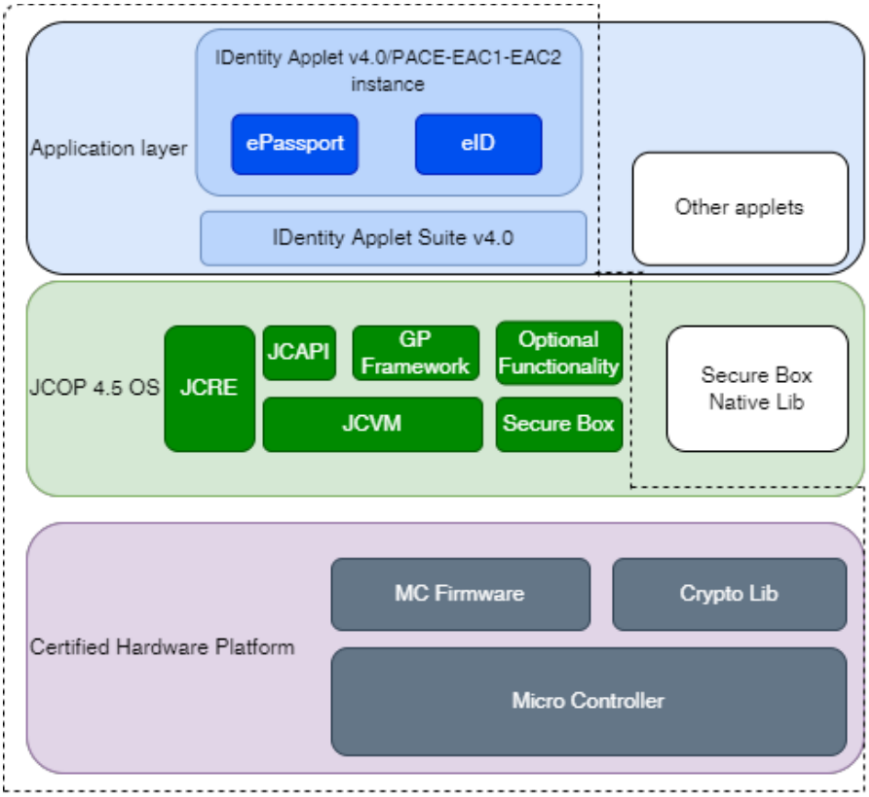
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

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:

® TrustCB is a registered trademark. Any use or application requires prior approval.

| 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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) on NXP JCOP 4.5 P71

® TrustCB is a registered trademark. Any use or application requires prior approval.

### 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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) 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 *[PP_0056], [PP_0068]* and *[PP_0086]*.

## *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).

® TrustCB is a registered trademark. Any use or application requires prior approval.

# 3 Security Target

The Security Target ID&Trust IDentity Applet v4.0/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) - Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification 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:

| | |
|---|---|
| ACL | Access Control List |
| eMRTD | electronic MRTD |
| IC | Integrated Circuit |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| JIL | Joint Interpretation Library |
| JIL | Joint Interpretation Library |
| NSCIB | Netherlands Scheme for Certification in the area of IT Security |
| PACE | Password Authenticated Connection Establishment |
| PP | Protection Profile |
| QSCD | Qualified Signature/Seal Creation Device |
| TOE | Target of Evaluation |

® TrustCB is a registered trademark. Any use or application requires prior approval.

# 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/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) on NXP JCOP 4.5 P71 v4.0.9219, v 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 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 |
| [PP_0056] | Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, registered under the reference BSI-CC-PP-0056-V2-2012 |
| [PP_0068] | Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE-PP), Version 1.0.1, 22 July 2014, registered under the reference BSI-CC-PP-0068-V2-2011-MA-01 |


® TrustCB is a registered trademark. Any use or application requires prior approval.

[PP_0086] Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 (EAC2-PP), Version 1.01, 20.05.2015, registered under the reference BSI-CC-PP-0086-2015

[ST] Security Target ID&Trust IDentity Applet v4.0/PACE-EAC1 (eMRTD)/PACE-EAC2 (eIDAS) - Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification and Active Authentication, v1.0, 12 January 2026

(This is the end of this report.)

® TrustCB is a registered trademark. Any use or application requires prior approval.