# Certification Report

## HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00

Sponsor and developer: ***HID Global S.p.A.***
**Viale Remo De Feo 1**
**80122 Arzano (NA)**
**Itlay**

Evaluation facility: ***SGS Brightsight B.V.***
**Brassersplein 2**
**2612 CT Delft**
**The Netherlands**

Report number: **NSCIB-CC-0490186-CR**

Report version: **1**

Project number: **0490186**

Author(s): **Andy Brown**

Date: **05 September 2023**

Number of pages: **11**

Number of appendices: **0**





Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

# CONTENTS

# Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

# Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

## International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

## European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00. The developer of the HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00 is HID Global S.p.A. located in Arzano, Italy 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 is composite product made up of the Machine Readable Electronic Document application “ICAO Application - EAC-PACE-AA” in composition with the already certified Smart Card operating system “NXP JCOP 4” and “NXP P71” Integrated Circuit and Crypto Library.

The TOE provides the following advanced security mechanisms featured by the ICAO application:

- Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 8th ed. Part 11, and Terminal Authentication according to BSI TR-03110
- Password Authenticated Connection Establishment (PACE) according to ICAO Doc 9303 8th ed. Part 11
- Active Authentication according to ICAO Doc 9303 8th ed. 2015 Part 11

The TOE is delivered in phase 2 to the Card manufacturer as a microcontroller module which is ready to be embedded into a Smart Card or document booklet with the antenna and substrate, which are outside the physical boundaries of the TOE.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 05 September 2023 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 HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00, 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 HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00 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).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

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

# 2 Certification Results

## 2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00 from HID Global S.p.A. located in Arzano, Italy.

The TOE is comprised of the following main components:

| Delivery item type | Identifier | Version |
|---|---|---|
| Hardware | NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) (Certification ID: BSI-DSZ-CC-1136-V3) | B1 |
| Platform | NXP JCOP 4 Operating System, configuration Banking & Secure ID (Certification ID: NSCIB- CC-180212-5MA1) | JCOP 4 P71 v4.7 R1.01.4 |
| Software | HIDApp-eDoc suite ICAO Application – EAC-PACE-AA | 3_00 |

To ensure secure usage a set of guidance documents is provided, together with the HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00. For details, see section 2.5 “Documentation” of this report.

## 2.2 Security Policy

The TOE is a contact or contactless based integrated circuit chip of machine readable travel documents (MRTD) and provides Password Authenticated Connection Establishment mechanism and the Extended Access Control in accordance with ICAO Doc 9303 Part 11. The TOE is delivered to the Card manufacturer in Phase 2 as a microcontroller module which is ready to be embedded into a Smart Card or document booklet with the antenna and substrate, which are outside the physical boundaries of the TOE.

## 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 is composed of the following elements.

- NXP P71 microcontroller including the firmware for booting and low level functionality of the microcontroller e.g. writing to flash memory as well as software for implementing cryptographic operations called Crypto Library.
- NXP JCOP 4 Java Card platform, which can be split into the following components:
  - Software for implementing a Java Card Virtual Machine, a Java Card Runtime Environment and a Java Card Application Programming Interface.
  - Software for implementing content management according to GlobalPlatform called GlobalPlatform Framework.
  - Software for executing native libraries, called Secure Box.
- The applet, which is ICAO application compliant with [ICAO]
- The associated guidance documentation.

The TOE architecture can be depicted as follows:


The TOE implements the following security features.

- Active Authentication of the e-Document's chip, Password Authenticated Connection Establishment,
- Extended Access Control to the logical e-Document *[ICAO], [TR-03111]* in the case of HIDApp-eDoc suite ICAO Application – EAC-PACE-AA.
- Authentication by means of a PACE authentication; Extended Access Control version 2 authentication, composed by Terminal Authentication version 2 and Chip Authentication version 2 *[ICAO]* and *[TR-03111]*.

## 2.5 Documentation

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

| Identifier | Version |
|---|---|
| Initialization Guidance for HIDApp-eDoc suite | 1.4 |
| Personalization Guidance for HIDApp-eDoc suite – ICAO Application | 1.6 |
| Operational User Guidance for HIDApp-eDoc suite – ICAO Application | 1.5 |

## 2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

### 2.6.1 Testing approach and depth

The developer has performed extensive testing on functional specification and subsystems. The testing coverage and depth was achieved by implementing groups of tests to cover the functionalities provided by this TOE. Each group was run by a particular set of tools to verify the relevant behaviour. The results of tests were a pass. Where a pass result was not obtained the developer explained why the result was produced. The evaluators analysed the results and explanations and concluded that the results were consistent with the outcomes. The Evaluator also confirmed that all TSF subsystems and all modules in the TOE design were tested.

The sample of tests selected for repetition by the evaluators were chosen so that various aspects of the TOE functionality would be covered and seen.

The evaluator created additional test cases to confirm verification of the version of the TOE, and to examine crucial functionality of the TOE.

### 2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities could already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- 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. For this analysis, this was performed according to the attack methods in [JIL-AP]. An important source for assurance in this step was the technical report [JCOP-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 were not exploitable. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The test effort expended by the evaluators was 5 weeks. During that test campaign, 20% of the total time was spent on perturbation attacks and 80% on logical tests.

### 2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

### 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*

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 HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00.

## 2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the HIDApp-eDoc suite ICAO Application - EAC-PACE-AA Version 3_00, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 5** This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profiles *[PP_0056]* and *[PP_0068]*

## 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

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

# 3 Security Target

The HIDApp-eDoc suite Security Target ICAO Application EAC-PACE-AA, TCAE210002, Version 1.6, 07 June 2023 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

# 4 Definitions

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

| | |
|---|---|
| AA | Active Authentication |
| BAC | Basic Access Control |
| EAC | Extended Access Control |
| eIDAS | electronic IDentification, Authentication and trust Services |
| eMRTD | electronic MRTD |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| JIL | Joint Interpretation Library |
| MRTD | Machine Readable Travel Document |
| 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 |

# 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 “HIDApp-eDoc suite v3_00” – EAL4+/5+, 22-RPT-805, Version 3.0, 22 June 2023 |
| [PF-CERT] | Certification Report JCOP 4 P71, NSCIB-CC-180212-CR5, Version 1, 26 September 2022 |
| [PF-ETRfC] | SGS Brightsight B.V., 19-RPT-177 v14.0, Evaluation Technical Report for Composition NXP “JCOP 4 P71” – EAL6+, 14 September 2022 |
| [PF-MAINT] | Assurance Continuity Maintenance Report JCOP 4 P71, NSCIB-CC-180212-5MA1, Version 1, 23 January 2023 |
| [PF-ST] | JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050, Rev. 4.11, 2023-01-03 |
| [JIL-AAPS] | JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022 |
| [JIL-AM] | Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution) |
| [NSCIB] | Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019 |
| [PP_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, Version 1.0.1, 22 July 2014, registered under the reference BSI-CC-PP-0068-V2-MA-01 |
| [ST] | HIDApp-eDoc suite Security Target ICAO Application EAC-PACE-AA, TCAE210002, Version 1.6, 07 June 2023 |
| [ST-lite] | HIDApp-eDoc suite Security Target ICAO Application EAC-PACE-AA Public version, TCLE210005, Version 1.2, 07 June 2023 |
| [ST-SAN] | ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006 |
| [STAR] | Site Technical Audit Report - HID Global Arzano, 22-RPT-240, Version 1.0, 22 June 2023 |


(This is the end of this report.)