Certification Report

IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration)

Sponsor and developer:	***IDEMIA*** **18, Chaussée Jules César** **95520 Osny** **France**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-195748-CR**
Report version:	**1**
Project number:	**195748**
Author(s):	**Wouter Slegers**
Date:	**19 November 2018**
Number of pages:	**13**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
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 Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number: **CC-18-195748**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer: **IDEMIA**

18, Chaussée Jules César, 95520 Osny, France

Product and assurance level: **IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration)**

Assurance Package:

- EAL5 augmented with ALC_DVS.2 and AVA_VAN.5

Protection Profile Conformance:

- Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2
- Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), BSI-CC-PP-0068-V2-2011-MA-01, Version 1.0.1

Project number: **195748**

Evaluation facility: **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity: Date of 1st issue : **19-11-2018**

Certificate expiry : **19-11-2023**

PRODUCTS
RvA C078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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 license 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, in order 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 authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration). The developer of the IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) is IDEMIA located in Osny, France 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 Target of Evaluation (TOE) is a contact and contactless chip of a machine readable travel document (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO), EU requirements for biometric European passport and Biometric European Resident Permit. This product is intended to enable verification of the authenticity of the travel document and to identify its holder during a border control, using an inspection system. The verification process is based on Extended Access Control with Password Authenticated Connection Establishment (PACE), Chip Authentication v1, Terminal Authentication v1 and optionally Active Authentication (AA).

The TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446 supporting AA, as both applications (MRTD and IDL) share the same protocols and data structure organization.

The TOE also supports the Polymorphic eMRTD according to Polymorphic eMRTD Specification by the Dutch National Office for Identity Data (written by IDEMIA), allowing Polymorphic Authentication with Randomization of the Polymorphic Pseudonym, Polymorphic Identity and Polymorphic Complementary ID attributes.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2018-09-25 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 IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration), 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 IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) 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 and AVA_VAN.5.

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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) from IDEMIA located in Osny, France.

The TOE is comprised of the following main components:

Delivery item	Identifier	Version
IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration)	Software applet: IDeal Pass v2.3-i JC with Privacy Protection applet	7127-9301-0320-02.03.00.0009 (applet version 2.3.0.9, with applet build #9 in Flash memory of IDEMIA/Infineon platform)
	IDeal Citiz v2.17-i on Infineon M7892 B11 - Java Card Open Platform, also known as IDeal Citiz v2.1.3 Open Platform Certified by the French certification body (ANSSI-CC-2018/27) on 02-07-2018	Platform Identification for IDEMIA OS on Infineon chip is: 81 00 xx xx 49 21 80 30 21 71 with xx xx is: ‘78 01’ for SLE78CLFX4000P ‘78 05’ for SLE78CLFX4000PM ‘78 13’ for SLE78CFX4000P ’78 77’ for SLE78CLFX4007PM ’78 78’ for SLE78CLFX4007P ’79 85’ for SLE78CLFX408AP ’79 86’ for SLE78CLFX408APM
	Infineon M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware), certified by the German certification body (BSI-DSZ-CC-0782-V4-2018) on 09-01-2018	
Key set	Electronic document	n.a.

To ensure secure usage a set of guidance documents is provided together with the IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration). Details can be found in section 2.5 of this report. (Note that the guidance is only delivered via the Haarlem site.)

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, section 1.4.3.

2.2 *Security Policy*

The Target of Evaluation (TOE) is a contactless or contact based integrated circuit chip of machine readable travel documents (MRTD) and provides the Extended Access Control according to ‘ICAO Doc 9303’ as well as optional Active Authentication according to ‘ICAO Doc 9303’ if enabled during the personalization.

The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE), according to Electronic Passport Standards using the Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 *[PACEPP].* Polymorphic eMRTD extensions are present on the TOE that enable secure authentication with enhanced privacy protection features. It provides the holder the possibility to authenticate towards a service provider in a non-traceable and non-linkable manner thanks to usage of Polymorphic Pseudonyms and other Polymorphic ID attributes.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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.

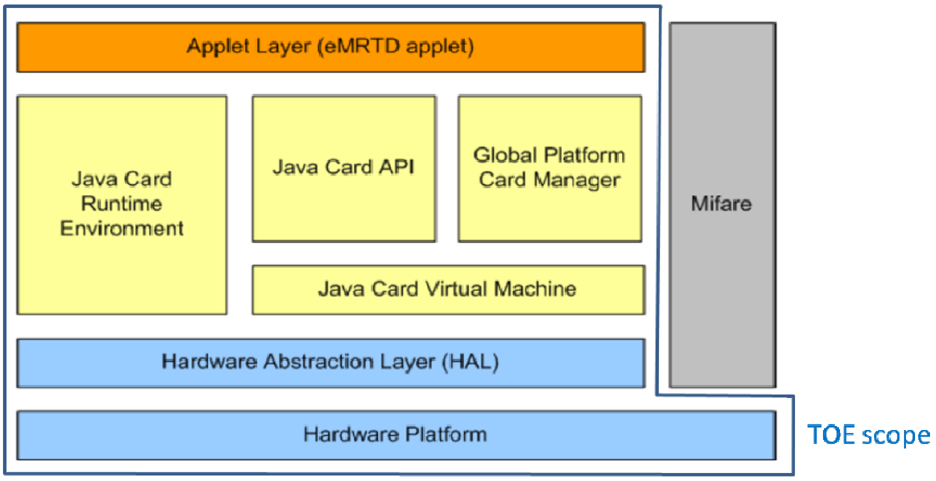
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalized must perform proper and safe personalization 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 consists of:


Applet Layer (eMRTD applet)
Java Card Runtime Environment
Java Card API
Global Platform Card Manager
Mifare
Java Card Virtual Machine
Hardware Abstraction Layer (HAL)
Hardware Platform
TOE scope

- The MRTD's chip circuitry and the IC dedicated software forming the Smart Card Platform (Hardware Platform and Hardware Abstraction Layer);
- The IC embedded software running on the Smart Card Platform consisting of
  - Java Card virtual machine, ensuring language-level security;
  - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
  - Java card API, providing access to card's resources for the Applet;
  - Global Platform Card Manager, responsible for management of Applets on the card;
  - Crypto Library
- The eMRTD Applet Layer is the IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration) Applet.

A MIFARE application can be optionally delivered as part of the TOE hardware depending on the used hardware platform. For the TOE the MIFARE application is out of scope, but this poses no security risk to the TOE.

2.5 Documentation

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

Delivery item	Identifier	Version
[AGD_OPE]	2018_2000035864 - OPERATIONAL PROCEDURES FOR IDEAL PASS V2.3-i JC with Privacy Protection. V1.2. IDEMIA	Revision 1.2
[AGD_PRE]	2018_2000035863- PREPARATIVE PROCEDURES FOR IDEAL PASS V2.3-i JC with Privacy Protection. V1.3. IDEMIA	Revision 1.3

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, subsystem and module level. All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the commands return the expected values.

The underlying hardware, crypto-library and Javacard test results are extendable to composite evaluations, as 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 has provided samples and a test environment. The evaluators have 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 penetration tests are devised after performing the Evaluator Vulnerability Analysis. The reference for attack techniques to which smart card-based devices such as the TOE must be protected against is the document named "Attack methods for smart cards" and referenced as *[JIL-AP].* The susceptibility of the TOE to these attacks has been analysed in a white box investigation.

The methodical analysis performed was conducted along the following steps:

1. When evaluating the evidence in the classes ASE, ADV and AGD potential vulnerabilities were identified from generating questions to the type of TOE and the specified behaviour.
2. A couple of detailed code reviews were performed on increasing versions of the implementation representation of the TOE, identified potential vulnerabilities were addressed.
3. An attack oriented analysis was performed according to the attack list in *[JIL-AP]*. For each of the attacks assurance for protection against the attacks was analysed using the knowledge gained from all evaluation classes. An important source for assurance against attacks in this step is the *[JC-ETRfC]* of the underlying platform. No additional potential vulnerabilities were concluded from this step.
4. All potential vulnerabilities were analysed for their protection using the total of the knowledge gained from all evaluation classes and the review on the implementation representation. It was concluded that for each of the potential vulnerabilities the TOE is protected such that the attack is not practical.
5. In a next step choices were made for penetration testing. Because no suspicion remained for potential vulnerabilities a choice for penetration testing was made to verify resistance against perturbation attacks for PMA functionality.

A perturbation attack was tested with laser fault injection, for one week. A side channel attack was tested for four weeks. Logical attacks have also been tested.

2.6.3 Test Configuration

The TOE has been tested in pre-personalisation, personalisation and operational life-cycle states with applet instance configurations specified in the Security Target *[ST]* section 1.4.2.

2.6.4 Testing 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 algorithmic security level exceeds 80 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 5 site re-use report approaches for:

- IDEMIA site in Osny R&D (development)
- IDEMIA site in Meyreuil R&D (development)
- IDEMIA site in Noida R&D (development)
- IDEMIA site in Haarlem (development and production)
- IDEMIA site in Noida plant (production)

No sites have been visited as part of this evaluation.

Significant re-use of the CC-19-180351 certification (the same applet and configuration on another JavaCard platform) was made.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration). The guidance documents describes how to verify the TOE and configure it.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] 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 IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration), to be **CC Part 2 extended, CC**

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

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 *[PACE-PP]* and *[EACPP-V2].*

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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. There are no particular obligations or recommendations for the user apart from following the user guidance.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 any proprietary or non-standard algorithms or protocols that use the Polymorphic Authentication functionality.

Note that the same TOE in BAC and optional AA Configuration is certified under ID NSCIB-CC-196231.

Note that the ROCA attack does not apply to the functionality added by this TOE, compared to the underlying platform, because there is no RSA key generation performed.

As part of the composition activities, it was verified that the certification of the underlying JavaCard platform considered the ROCA attack and determined that the platform was resistant at AVA_VAN.5 level.

Note also that the guidance of this TOE and the underlying platform must be followed for any other application added to this TOE.

To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

3 Security Target

The Security Target IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration), Ref:2018_2000034833, version 1.4, 07/09/2018 *[ST]* is included here by reference.

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

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MRTD	Machine readable travel document
MRZ	Machine readable zone
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

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

[EACPP-V2] Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5th December 2012.

[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.

[ETR] Evaluation Technical Report IDeal Pass v2.3-i JC with Privacy Protection EAL5+ (SAC/EAC/Polymorphic eMRTD Configuration), document reference 18-RPT-534, version 3.0, dated 19 September 2018.

[JC-ETRfC] Evaluation Technical Report (ETR for composition) - EAGLE-V3, Ideal Citiz v2.1.3 open platform, LETI.CESTI.EAV3.COMPO.001 V1.2, 13/06/18

[JIL-AP] JIL, (Mandatory) Application of Attack Potential to Smartcards, Version 2.9, January 2013

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.

[PACE-PP] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-MA-01, Version 1.0.1, 22 July 2014, BSI.

[ST] Security Target IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration), Ref:2018_2000034833, version 1.4, 07/09/2018

[ST-lite] Security Target Lite IDeal Pass v2.3-i JC with Privacy Protection (SAC/EAC/Polymorphic eMRTD Configuration), Ref:2018_2000037744, version 1.0, 07/09/2018.

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

(This is the end of this report).