*Ministero dello Sviluppo Economico*

*Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione*

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

# Certificato n. 2/16

*(Certification No.)*

**Prodotto:** **IDentity Card v3.2/PACE-EAC1**
*(Product)*

**Sviluppato da:** **ID&Trust**
*(Developed by)*

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

*The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:*

## EAL4+
**(ALC_DVS.2, ATE_DPT.2, AVA_VAN.5)**

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 22 marzo 2016

Common Criteria

SOGIS IT SECURITY CERTIFICATE

This page is intentionally left blank

*Ministero dello Sviluppo Economico*

*Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione*

Organismo di Certificazione della Sicurezza Informatica

# Certification Report

# IDentity Card v3.2/PACE-EAC1

OCSI/CERT/SYS/02/2016/RC

Version 1.0

March 22, 2016

# Courtesy translation

**Disclaimer**: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

# 1 Document revisions

| Version | Author | Information | Date |
|---|---|---|---|
| 1.0 | OCSI | First issue | 22/03(2016 |
| | | | |

# 2 Index

# 3 Acronyms

**BAC** Basic Access Control

**CC** Common Criteria

**CCRA** Common Criteria Recognition Arrangement

**CEM** Common Evaluation Methodology

**DPCM** Decreto del Presidente del Consiglio dei Ministri

**EAL** Evaluation Assurance Level

**eMRTD** electronic Machine Readable Travel Document

**HW** Hardware

**LGP** Linea Guida Provvisoria

**LVS** Laboratorio per la Valutazione della Sicurezza

**NIS** Nota Informativa dello Schema

**OCSI** Organismo di Certificazione della Sicurezza Informatica

**PACE** Password Authenticated Connection Establishment

**PP** Profilo di Protezione

**RFV** Rapporto Finale di Valutazione

**SAR** Security Assurance Requirement

**SFR** Security Functional Requirement

**SW** Software

**TDS** Traguardo di Sicurezza

**TOE** Target of Evaluation

**TSF** TOE Security Functionality

**TSFI** TOE Security Functionality Interface

# 4 Bibliography

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CCRA-2000] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, May 2000

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

[ADM] IDentity Applet Administrator's Guide Version 3.2.18

[AFNOR-1] AFNOR BSI contribution to TF4 Amendment to ICAO Technical Report – RF protocol and application test standard for ePassport Part 3, Tests for Application Protocol and Logical Data Structure, Version 1.01, February 2007 Supplemental Access Control Active Authentication

[AFNOR-2] AFNOR Advanced Security Mechanisms For Machine Readable Travel Documents – Extended Access Control (EAC) Tests For Security Implementation V.1.12, October 3, 2008

[BSI-56] BSI-CC-PP-0056-V2-2012, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, Version 1.3

[BSI-68] BSI-CC-PP-0068-V2-2011, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.0

[CCDB] CCDB-2012-04-001, Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, Version 1.2, April 2012

[CHANGES] CC Re-evaluation eMRTD with BAC, PACE-EAC1, "Changes of ID&Trust Identity Card 3.1 to 3.2", ID&Trust, Version 0.1, 25 October 2015

[CONF] IDentity Applet Initialization and configuration Version 3.2.07

[ETR-COMP] ETR for Composite Evaluation NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 EAL5+, Brightsight, 9 August 2013, revision 12 August 2014

[IAR] Impact Analysis Report "Changes of ID&Trust IDentity Card 3.1 to 3.2", Systrans SW Lab, Version 1.3, 13 November 2015

[ICAO-RF] ICAO RF protocol and application test standard for e-passport - part 3 v.2.01

[ICAO-TR] International Civil Aviation Organization, ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[ICAO-9303] International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006,

[NSCIB] Certification Report "NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3", NSCIB-CC-13-37760-CR2, 5 August 2013, revision 26 August 2014

[RC] Certification Report, "ID&Trust IDentity Card v3.1/PACE-EAC1", OCSI/CERT/SYS/04/2015/RC, Version 1.0, September 30, 2015

[RFV] ID&Trust IDentity Card v3.2/PACE-EAC1 Evaluation Technical Report, v1.1, 8 March 2016

[TDS] ID&Trust IDentity Card v3.2/PACE-EAC1 Security Target, v0.43, 8 March 2016

[TR-210] BSI Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20 March 2012

[TR-220] BSI Technical Guideline TR-03110-4 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 4 – Applications and Document Profiles, Version 2.20, 3 February 2015

[USR] IDentity Applet User's Guide Version 3.2.19

# 5 Recognition of the certificate

## 5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA up to EAL4.

## 5.2 International Recognition of CC Certificates (CCRA)

The new version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

Certificates issued before 08 September 2014 are still under recognition according to the previous arrangement [CCRA-2000]: up to and including EAL 4 (and ALC_FLR). For on 08 September 2014 ongoing certification procedures and for maintenance and re-certifications of old certificates, a transition period on the recognition of certificates according to the same rules of CCRA-2000 is defined until 08 September 2017.

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

As this process is the re-certification of a new version of the same product, this certificate is recognized according to the rules of the previous arrangement [CCRA-2000], i.e. for all assurance components selected or up to EAL 4.

# 6 Statement of Certification

The Target of Evaluation (TOE) is the product “ID&Trust ID Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite 3.2/PACE-EAC1”, short name “IDentity Card v3.2/PACE-EAC1”, developed by ID&Trust Ltd.

The TOE is a composite product and comprises:

- the Platform “NXP J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65 Secure Smart Card Controller Revision 3”, short name “JCOP 2.4.2 R3”, certified under The Netherland CC Scheme at EAL5 augmented with ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5 [NSCIB];

- the Application Part of the TOE “ID&Trust IDentity Applet Suite Version 3.2”, configured as eMRTD application;

- the associated guidance documentation.

Therefore, the evaluation has been conducted using the results of the Platform CC certification [NSCIB] and following the recommendations contained in the document “Composite product evaluation for Smart Cards and similar devices” [CCDB], as required by the international agreements CCRA and SOGIS.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

This Certification Report was issued at the conclusion of the re-certification of an earlier version of the same TOE (IDentity Card v3.1/PACE-EAC1), already certified by OCSI (Certificate no. 2/15 of September 30, 2015 [RC]).

The TOE can be configured and used for different kind of electronic identity products based on the extended version of the standard BSI TR-03110 [TR-210].

Meanwhile, there is a new version of the standard (TR-03110 v2.20 [TR-220]) where many optional features are standardized. One of these new features is enabling access control for non-standard Data Groups within CV Certificates, so called “Authorization Extensions to be used for local Generic Attributes” (see [TR-220] sec. 2.2 for details). This feature is implemented by the new version of ID&Trust IDentity Card applet accordingly. The actual implementation of the change does not affect the certified functions of the IDentity applet. In order to be separated from the evaluation version, the TOE is renamed “IDentity Card v3.2/PACE-EAC1”.

The changes have been described by the developer in the document [CHANGES].

Note that the changes have also led to the revision of the Security Target [TDS]. Customers of the TOE are therefore advised to take also into account the new ST.

To assess the actual impact of the changes, it was deemed necessary to undertake a re-certification of the TOE.

The LVS Systrans SW Lab has initially carried out an impact analysis of the differences with respect to the already certified version (IDentity Card v3.1/PACE-EAC1), summarizing the results in the document [IAR]. On this basis, the evaluators were able to reuse many of the evidences already provided in the initial evaluation. In particular, functional tests were limited to conduct the activities related to the ATE_FUN.1 and ATE_IND.2 families only, while no new penetration tests were performed.

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with ALC_DVS.2, ATE_DPT.2, AVA_VAN.5, according to the information provided in the Security Target [TDS] and in the configuration shown in Annex B of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

# 7 Summary of the evaluation

## 7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “IDentity Card v3.2/PACE-EAC1” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

## 7.2 Executive summary

| | |
|---|---|
| **Name of TOE** | IDentity Card v3.2/PACE-EAC1 |
| **Security Target** | IDentity Card v3.2/PACE-EAC1 Security Target, v0.43, 8 March 2016 |
| **Evaluation Assurance Level** | EAL4 augmented with ALC_DVS.2, ATE_DPT.2, AVA_VAN.5 |
| **Developer** | ID&Trust |
| **Sponsor** | ID&Trust |
| **LVS** | Systrans SW Lab |
| **CC version** | 3.1 Rev. 4 |
| **PP claim** | BSI-CC-PP-0056-V2-2012 [BSI-56], BSI-CC-PP-0068-V2-2011 [BSI-68] |
| **Kickoff date** | February 24, 2016 |
| **Completion date** | March 8, 2016 |

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [TDS] are fulfilled.

## 7.3 Evaluated product

This section summarizes the main functional and security requirements of TOE; for a detailed description, please refer to the Security Target [TDS].

The TOE “IDentity Card v3.2/PACE-EAC1” is an electronic travel document representing a contact based/contactless smart card containing components for machine readable travel documents (MRTD), based on the requirements and recommendations of the International Civil Aviation Organization [ICAO-TR].

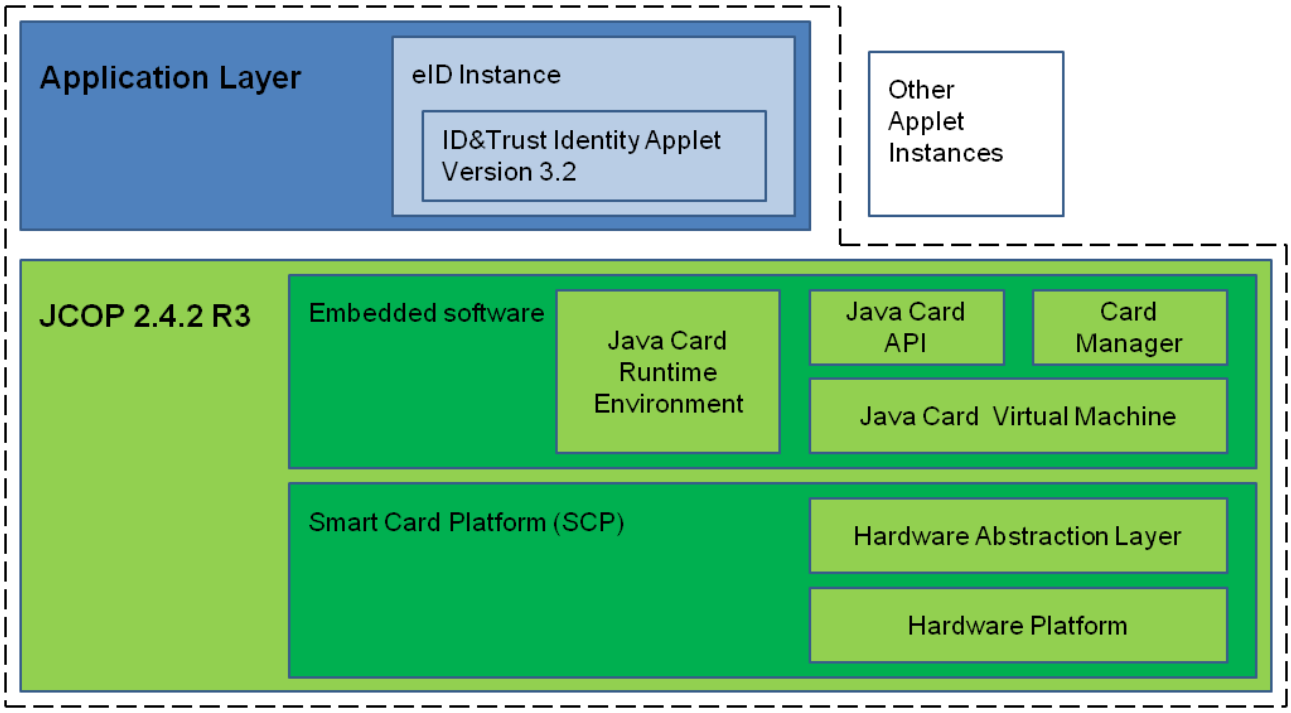


Figure 1 – The logical architecture of the TOE

The TOE is a composite product and comprises (Figure 1):

- the Platform "NXP J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65 Secure Smart Card Controller Revision 3", short name "JCOP 2.4.2 R3", certified under The Netherland CC Scheme at EAL5 augmented with ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5 [NSCIB];
- the Application Part of the TOE "ID&Trust IDentity Applet Suite Version 3.2", configured as eMRTD application;
- the associated guidance documentation.
  - IDentity Applet Initialization and configuration Version 3.2.07 [CONF]
  - IDentity Applet Administrator's Guide Version 3.2.18 [ADM]
  - IDentity Applet User's Guide Version 3.2.19 [USR]

The intended customer of the product is the Card Issuer (State or other Organization), who is in charge of delivering the product to the smartcard holders, after storing their personal data, such as biographical data, printed portrait, etc.

The travel document is viewed as unit of the "physical" part (in form of paper and/or plastic and chip), which presents visual readable data, and the "logical" part, where data are stored according to a structure readable from contact or contactless digital machines. The issuing State or Organization implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part is identified by the document number and protected by physical security measures, while the logical part is protected in authenticity and integrity by a digital signature created by the issuing State or Organization.

The TOE communicates with the electronic terminals via the protocol Password Authenticated Connection Establishment (PACE), according to the requirements specified in [BSI-68].

In general, products of this kind can also support the mechanism of access control Basic Access Control (BAC). However, a product that implements the TOE with the mechanism BAC operates outside of the security policy defined in the TDS.

### 7.3.1 TOE Architecture

For a detailed description of the TOE, consult the Security Target [TDS], and in particular:

- the physical and logical parts of the TOE are described in par. 1.4.1 and 1.4.3;
- the features of the Applet are provided in par. 1.4.6;
- the TOE life cycle is described in terms of four life cycle phases: development, manufacturing, personalization and operational use, described in par. 1.4.4, together with the operations allowed to users and administrators for each of them.

### 7.3.2 TOE security features

*7.3.2.1 Platform compatibility*

Some aspects related to security features of the TOE, including security objectives, assumptions, threats and organizational security policies, defined in the Security Target, are covered directly by the Platform. For details see par. 2.5 of [TDS].

*7.3.2.2 Security functions*

The TOE security functions are described in detail in par. 7.1 of [TDS], the most significant aspects are below informally summarized:

- **AccessControl**: the TOE provides access control mechanisms that allow among others the maintenance of different users, each able to perform distinct actions.
- **Authenticate**: TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication.
- **SecureManagement_MRTD**: this function manages the various phases of the life cycle of the TOE, following a sequence defined and protected by authentication.
- **CryptoKey_MRTD**: this function handles the generation of cryptographic keys on board of the platform and their overwriting after use.
- **AppletParameters_Sign**: some configuration and control parameters can only take values in accordance with the requirements and can be signed, allowing the user to verify their safety.
- **Platform**: this TSF covers the security functionalities based on the security functionalities of the certified cryptographic library and the certified IC Platform.

## 7.4 Documentation

The guidance documentation specified in Annex A - Guidelines for the safe use of the product is delivered to the customer together with the product. The intended customer of the product is the Card Issuer (State or other Organization), who is in charge of delivering the product to the smartcard holders.

The guidance documentation contains all the information for secure initialization, configuration and secure use the TOE in accordance with the requirements of the Security Target [TDS].

Customers should also follow the recommendations for the safe use of the TOE contained in par. 8.2 of this report.

## 7.5 Protection Profile (PP) claim

The TOE is an electronic travel document representing a contact based/contactless smart card, based on the requirements and recommendations of the International Civil Aviation Organization [ICAO-TR]; so, it claims strict conformance to the following Protection Profiles:

- BSI-CC-PP-0056-V2-2012 [BSI-56], which defines the security objectives and requirements for the contact based/contactless smart card of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organization [ICAO-TR]. It addresses the advanced security methods Password Authenticated Connection Establishment, Extended Access Control, and Chip Authentication similar to the Active Authentication in [ICAO-9303];

- BSI-CC-PP-0068-V2-2011 [BSI-68], which refers to contact based/contactless smart card with software application used for implementing electronic travel documents, such as electronic passports and similar.

## 7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

Please refer to the Security Target [TDS] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

All the Security Functional Requirements (SFR) have been selected or derived by extension from CC Part 2 [CC2]. In particular, considering that the Security Target claims strict conformance to two PPs [BSI-56, BSI-68], all extended components from such PPs are included: FIA_API from [BSI-56], FAU_SAS, FCS_RND, FMT_LIM and FPT_EMS from [BSI-68].

## 7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

Therefore, considering that the TOE is a composite product, the evaluation has been conducted following the recommendations contained in the document “Composite product evaluation for Smart Cards and similar devices” [CCDB], as required by the international agreements CCRA and SOGIS. Since this is a re-certification, the evaluators have initially carried out an impact analysis of the differences with respect to the already certified version (IDentity Card v3.1/PACE-EAC1), summarizing the results in the document [IAR]. On this basis, they considered still valid the results of the previous evaluation: in particular, please note that the penetration tests have been completed on January 13, 2015, within 18 months from the Platform vulnerability analysis (July 2013, the reference date indicated in the relevant certification [NSCIB]).

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [TDS]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) Systrans.

The evaluation was completed on March 8, 2016 with the issuance by LVS of the Final Evaluation Report [RFV], which was approved by the Certification Body on March 15, 2016. Then, the Certification Body issued this Certification Report.

## 7.8 General considerations on the validity of the certification

The evaluation focused on the security features declared in the Security Target [TDS], with reference to the operating environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

# 8 Evaluation outcome

## 8.1 Evaluation results

Following the analysis of the Final Evaluation Report [RFV] issued by the LVS Systrans and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “IDentity Card v3.2/PACE-EAC1" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_DVS.2, ATE_DPT.2, AVA_VAN.5, with respect to the security features described in the Security Target [TDS] and the evaluated configuration, shown in Annex B.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_DVS.2, ATE_DPT.2, AVA_VAN.5.

| **Assurance classes and components** | | **Verdict** |
|---|---|---|
| **Security Target evaluation** | **Classe ASE** | Pass |
| Conformance claims | ASE_CCL.1 | Pass |
| Extended components definition | ASE_ECD.1 | Pass |
| ST introduction | ASE_INT.1 | Pass |
| Security objectives | ASE_OBJ.2 | Pass |
| Derived security requirements | ASE_REQ.2 | Pass |
| Security problem definition | ASE_SPD.1 | Pass |
| TOE summary specification | ASE_TSS.1 | Pass |
| **Development** | **Classe ADV** | Pass |
| Security architecture description | ADV_ARC.1 | Pass |
| Complete functional specification | ADV_FSP.4 | Pass |
| Implementation representation of the TSF | ADV_IMP.1 | Pass |
| Basic modular design | ADV_TDS.3 | Pass |
| **Guidance documents** | **Classe AGD** | Pass |
| Operational user guidance | AGD_OPE.1 | Pass |
| Preparative procedures | AGD_PRE.1 | Pass |
| **Life cycle support** | **Classe ALC** | Pass |
| Production support, acceptance procedures and automation | ALC_CMC.4 | Pass |
| Problem tracking CM coverage | ALC_CMS.4 | Pass |

| Assurance classes and components | | Verdict |
|---|---|---|
| Delivery procedures | ALC_DEL.1 | Pass |
| Sufficiency of security measures | ALC_DVS.2 | Pass |
| Developer defined life-cycle model | ALC_LCD.1 | Pass |
| Well-defined development tools | ALC_TAT.1 | Pass |
| **Test** | **Classe ATE** | Pass |
| Analysis of coverage | ATE_COV.2 | Pass |
| Testing: security enforcing modules | ATE_DPT.2 | Pass |
| Functional testing | ATE_FUN.1 | Pass |
| Independent testing - sample | ATE_IND.2 | Pass |
| **Vulnerability assessment** | **Classe AVA** | Pass |
| Advanced methodical vulnerability analysis | AVA_VAN.5 | Pass |

Table 1 – Final verdicts for assurance requirements

## 8.2 Recommendations

The conclusions of the Certification Body OCSI are summarized in Section 6 - Statement of Certification.

Potential customers of the product "IDentity Card v3.2/PACE-EAC1" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the security environment specified in par. 1.4.6.4 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the TDS are respected, particularly those compatible with the Platform HW (see [TDS] par. 2.5).

This Certification Report is valid for the TOE in the evaluated configuration; in particular, Annex A includes a number of recommendations relating to delivery, initialization, configuration and safe use of the product, according to the guidance documentation provided together with the TOE ([CONF, ADM, USR]).

# 9 Annex A – Guidelines for the safe use of the product

This annex provides considerations particularly relevant to the potential customers of the product.

## 9.1 Delivery

Since the TOE is a composite product, the delivery procedures entail interactions between the application developer (ID & Trust) and the Platform manufacturer (NXP).

In particular, the platform manufacturer implements the application in the integrated circuit and activates the process of initialization and customization, with the cooperation of the application developer. The document just created, encrypted with a special transport key, is delivered to the customer, i.e. the Card Issuer (State or other Organization) of the electronic document, by an express courier company, DHL, TNT, FEDEX, SKY, etc. If the document is lost, however, it cannot be altered, since, after the application is loaded and configured, it becomes read-only. Finally, the Card Issuer delivers the individual documents to the smartcard holders personally at the official issuer site, or sending by post, according to the local regulations.

The application developer is responsible for the maintenance of the security aspects (integrity, confidentiality, availability).

More detail on such a procedure are contained in:

- IDentity Applet Initialization and configuration Version 3.2.07 [CONF];
- IDentity Applet Administrator's Guide Version 3.2.18 [ADM].

## 9.2 Initialization and secure use of the TOE

The secure initialization of the TOE and the safe preparation of its operational environment in accordance with the security objectives specified in [TDS], should be done by following the instructions in the appropriate sections of the guidance documentation:

- IDentity Applet Initialization and configuration Version 3.2.07 [CONF];
- IDentity Applet Administrator's Guide Version 3.2.18 [ADM];
- IDentity Applet User's Guide Version 3.2.19 [USR].

# 10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “ID&Trust ID Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite 3.2/PACE-EAC1”, short name “IDentity Card v3.2/PACE-EAC1”, developed by ID&Trust Ltd.

The TOE is a composite product and comprises the following HW/SW components, representing the evaluated configuration of the TOE, as reported in [TDS], to which the evaluation results apply.

- the Platform “NXP J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65 Secure Smart Card Controller Revision 3”, short name “JCOP 2.4.2 R3”, certified under The Netherland CC Scheme at EAL5 augmented with ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5 [NSCIB], which in turn consists of:
  - smart card and smart card controller “NXP Secure Smart Card Controllers P5CD145V0v/ V0B(s) and P5CC145V0v/V0B(s)”;
  - Crypto Library “V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/V1A(s)”;
  - Embedded Software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager);
  - Native MIFARE application (physically always present but logical availability depends on configuration);
- the Application Part of the TOE “ID&Trust IDentity Applet Suite Version 3.2”, configured as eMRTD application;
- the associated guidance documentation.
  - IDentity Applet Initialization and configuration Version 3.2.07 [CONF]
  - IDentity Applet Administrator’s Guide Version 3.2.18 [ADM]
  - IDentity Applet User’s Guide Version 3.2.19 [USR]

# 11 Annex C – Test activity

This annex describes the task of both the evaluators and the developer in testing activities. For the assurance level EAL4, augmented with ALC_DVS.2, , ATE_DPT.2, AVA_VAN.5, such activities include the following three steps:

- evaluation of the tests performed by the developer in terms of coverage and level of detail;
- execution of independent functional tests by the evaluators;
- execution of penetration tests by the evaluators.

Since this is a re-certification, the evaluators have initially carried out an impact analysis of the differences with respect to the already certified version (IDentity Card v3.1/PACE-EAC1), summarizing the results in the document [IAR]. On this basis, they established to perform new activities related to ATE_FUN.1 and ATE_IND.2 families only, while they considered still valid the results of the previous evaluation for ATE_COV.2 and ATE_DPT.2 families, which are reported here for completeness.

## 11.1 Test configuration

For the execution of these activities a test environment has been placed at the LVS site with the support of the developer, which provided the necessary resources. In particular, the test configuration consists of the test card, a test card reader connected to the test PC, running the test cases, developed for Global Tester environment running within Eclipse.

Before the tests, the software application has been initialized and configured in accordance with the guidance documentation [CONF, ADM, USR], as indicated in par 9.2.

Moreover, considering that the TOE is a composite product, the recommendations contained in the document [CCDB] have been followed. In particular, the hardware platform has already been certified and the results were reused from LVS, who was able to directly evaluate the software application.

## 11.2 Functional tests performed by the developer

### 11.2.1 Test coverage

The test plan presented by the developer has been largely based on the following reference documents, normally used for products such as electronic passports and similar:

- ICAO RF protocol and application test standard for e-passport - part 3 v.2.01 [ICAO-RF];
- AFNOR BSI contribution to TF4 Amendment to ICAO-TR Technical Report – RF protocol and application test standard for ePassport Part 3, Tests for Application Protocol and Logical Data Structure, Version 1.01, February 2007 Supplemental Access Control Active Authentication [AFNOR-1];

- AFNOR Advanced Security Mechanisms For Machine Readable Travel Documents – Extended Access Control (EAC) Tests For Security Implementation V.1.12, October 3, 2008 [AFNOR-2].

In addition, the developer designed independently other additional tests in order to demonstrate the complete coverage of the functional requirements SFR and of the security functions.

### 11.2.2 Test results

The evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

## 11.3 Functional and independent tests performed by the evaluators

Therefore, the evaluators have designed independent testing to verify the correctness of the TSFI.

They did not used testing tools in addition to the specific components of the TOE that allowed to check all TSFI selected for independent testing.

In the design of independent tests, the evaluators have considered aspects that in the developer test plan were not present or ambiguous or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The evaluators also designed and executed some tests independently from similar tests of the developer, based only on the evaluation documentation.

Finally, considering that the TOE is a composite product, the behavior of the TOE as a whole has been verified, carrying out the additional activities specified in the family ATE_COMP, according to the document [CCDB].

All tests performed by independent evaluators generated positive results.

## 11.4 Vulnerability analysis and penetration tests

Since this is a re-certification, the evaluators, on the basis of the impact analysis [IAR] of the differences with respect to the already certified version, considered still valid the results of the penetration tests performed in the previous evaluation, which are reported here for completeness.

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see. par. 11.1)

The evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the [TDS], par. 1.4.

In a first phase, the evaluators have conducted researches using various sources in the public domain, such as Internet, books, publications, conference proceedings, including the various editions of ICCC, JIL and CCDB documents, etc., in order to identify known vulnerabilities applicable to types of products similar to the TOE, i.e. electronic documents

eMRTD. They identified several potential vulnerabilities, most of which, however, refer to the hardware platform already certified EAL5+, and therefore not exploitable with the High potential attack belongs to AVA_VAN.5.

In a second step, the evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture and operational documentation, including the Platform) to identify any additional potential vulnerabilities of the TOE. From this analysis, together with the source code examination, the evaluators have actually determined the presence of other potential vulnerabilities; however, also in this case, most of them have already been considered during the evaluation of the Platform, as documented in the relevant Final Report [ETR-COMP].

The evaluators have analyzed in detail the potential vulnerabilities identified in the two previous steps, to ensure their effective exploitability in the TOE operating environment. This analysis led to identify six actual potential vulnerabilities.

Therefore, the evaluators have designed some possible attack scenarios, with High attack potential, and penetration tests to verify the exploitability of the vulnerabilities potential candidates. The penetration tests have been described with sufficient detail for their repeatability using for this purpose test sheets, also used, appropriately compiled with the results, as the report of the tests themselves.

Moreover, considering that the TOE is a composite product, the behavior of the TOE as a whole has been verified, carrying out the additional activities specified in the family AVA_COMP, according to the document [CCDB].

On the basis of the penetration tests, the evaluators have actually found that no attack scenario with potential High can be completed successfully in the operating environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively. They have not identified residual vulnerabilities, i.e. vulnerabilities that, although not exploitable in the operating environment of the TOE, could be exploited only by an attacker with attack potential beyond High.