Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica
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. 9/20
(Certification No.)

Prodotto: **IDentity Applet v3.4/BAC on NXP JCOP 4 P71**
(Product)

Sviluppato da: **ID&Trust Ltd.**
(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)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 28 ottobre 2020

Common Criteria

SOGIS

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IDentity Applet v3.4/BAC
on NXP JCOP 4 P71

OCSI/CERT/SYS/05/2016/RC

Version 1.0

28 October 2020

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	28/10/2020

2 Table of contents

3 Acronyms

API   Application Programming Interface

BAC   Basic Access Control

CBC   Cipher Block Chaining

CC   Common Criteria

CCRA   Common Criteria Recognition Arrangement

CEM   Common Evaluation Methodology

DES   Data Encryption Standard

DPCM   Decreto del Presidente del Consiglio dei Ministri

EAL   Evaluation Assurance Level

eMRTD   Electronic Machine Readable Travel Document

ETR   Evaluation Technical Report

GP   Global Platform

HW   Hardware

ICAO   International Civil Aviation Organization

IC   Integrated Circuit

IT   Information Technology

IV   Initialization Vector

JCOP   Java Card Open Platform

LDS   Logical Data Structure

LGP   Linea Guida Provvisoria

LVS   Laboratorio per la Valutazione della Sicurezza

MAC   Message Authentication Code

MRZ   Machine-Readable Zone

NIS   Nota Informativa dello Schema

OCSI   Organismo di Certificazione della Sicurezza Informatica

OS   Operating System

PP   Protection Profile

SAR   Security Assurance Requirement

SFR   Security Functional Requirement

SOGIS   Senior Officials Group Information Systems Security

ST   Security Target

SW   Software

TOE   Target of Evaluation

TSF   TOE Security Functionality

TSFI   TSF Interface

4   References

4.1   Criteria and regulations

[CC1]   CCMB-2017-04-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 5, April 2017

[CC2]   CCMB-2017-04-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 5, April 2017

[CC3]   CCMB-2017-04-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 5, April 2017

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

[CEM]   CCMB-2017-04-004, "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", Version 3.1, Revision 5, April 2017

[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

4.2 Technical documents

[ADM]   ID&Trust Identity Applet Suite Administrator's Guide, Version 3.4.1, 31 July 2020

[DEL]   ID&Trust Documents, Common Criteria Evaluation, IDentity Applet V3.4 Delivery Documentation, V0.02, 10 February 2020

[CR]   Certification Report "IDentity Card v3.2/BAC", OCSI/CERT/SYS/03/2016/RC, Version 1.0, 22 March 2016

[ETR]   "ID&Trust IDentity Applet v3.4/BAC/AA" Evaluation Technical Report, v4, CCLab Software Laboratory, 14 October 2020

[ETR-COMP]   Evaluation Technical Report for Composition NXP JCOP 4 P71 - EAL6+, 19-RPT-177, Version 7.0, 19 March 2020

[ICAO-9303] International Civil Aviation Organization (ICAO) Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015

[ICAO-TR1]   International Civil Aviation Organization (ICAO) Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, 15 April 2014

[ICAO-TR2]   International Civil Aviation Organization (ICAO) Technical Report, Radio Frequency Protocol and Application Test Standard for eMRTD Part 3 – Tests for Application Protocol and Logical Data Structure, Version 2.10, 7 July 2016

[JIL-COMP]   Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[NXP-CR1]   Certification Report "NXP JCOP 4 P71", NSCIB-CC-180212-CR2, TÜV Rheinland Nederland B.V., 20 March 2020

[NXP-CR2]   Certification Report "NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library", BSI-DSZ-CC-1040-2019-MA-01, BSI - Bundesamt für Sicherheit in der Informationstechnik, 4 March 2020

[PP-055]   BSI-CC-PP-0055, Protection Profile - Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009

[PP-056]   BSI-CC-PP-0056-V2-2012, Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012

[TR-03110]   BSI TR-03110-1, Advanced Security Mechanisms forMachine Readable Travel Documents and eIDAS Token – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015

[ST]   "Security Target IDentity Applet v3.4/BAC/AA – ePassport with BAC and Active Authentication", Version 1.01, ID&Trust Ltd., 13 October 2020

[USR]   ID&Trust Identity Applet Suite User's Guide, Version 3.4.1, 4 August 2020

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 https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized 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 current 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 EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

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

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

This certificate is recognised under CCRA up to EAL2.

6   Statement of Certification

The Target of Evaluation (TOE) is the product "IDentity Applet v3.4/BAC on NXP JCOP 4 P71", short name "IDentity Applet v3.4/BAC", developed by ID&Trust Ltd.

The TOE is a contactless integrated circuit chip containing components for a machine-readable travel document (MRTD) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control (BAC).

The TOE is a composite product and comprises:

- The underlying Platform of the TOE: "NXP JCOP 4 P71", developed by NXP Semiconductors Germany GmbH;

- the Application Part of the TOE: "IDentity Applet v3.4/BAC";

- the associated guidance documentation.

Therefore, the evaluation has been conducted using the results of the Platform CC evaluation [NXP-CR1], and following the recommendations contained in the mandatory supporting document "Composite product evaluation for Smart Cards and similar devices" [JIL-COMP], 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 v3.2/BAC), already certified by OCSI (Certificate no. 3/16 of 22 March 2016 [CR]).

The already certified version was based on the NXP JCOP 2.4.2 R3 platform, while the new version of the TOE is based on the NXP JCOP 4 P71 platform, so it was deemed necessary to undertake a full re-certification of the TOE. The evaluation actually started in 2016 on a TOE named "IDentity Applet v3.3/BAC on NXP JCOP 3 SECID P60 OSB Smart Card", based on the JCOP 3 platform. During the evaluation, the Sponsor decided to update the TOE to use the JCOP 4 platform. The new TOE "IDentity Applet v3.4/BAC" has exactly the same functionality of v3.3 but on the updated platform. Therefore, the LVS CCLab Software Laboratory used the results of the v3.3 ongoing evaluation as a base.

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

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; 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, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration 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 Applet v3.4/BAC" 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 [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	IDentity Applet v3.4/BAC on NXP JCOP 4 P71
Security Target	"Security Target IDentity Applet v3.4/BAC/AA - ePassport with BAC and Active Authentication", Version 1.01 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_DVS.2
Developer	ID&Trust Ltd.
Sponsor	NXP Semiconductors Netherlands B.V.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	BSI-CC-PP-0055 [PP-055]
Evaluation starting date	6 September 2016
Evaluation ending date	14 October 2020

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 [ST] are fulfilled.

7.3 Evaluated product

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

The TOE "IDentity Applet v3.4/BAC" is a contactless integrated circuit chip with IC Dedicated Software (Micro Controller Firmware, Crypto Library), Embedded Software (JCOP4) and an electronic travel document applet, containing components for a machine-readable travel document (MRTD) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control (BAC) according to [TR-03110] and [ICAO-9303], and optionally Active Authentication defined in [ICAO-9303].

The TOE is a composite product and comprises:

- The underlying Platform of the TOE: "NXP JCOP 4 P71", developed by NXP Semiconductors Germany GmbH, certified at EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 [NXP-CR1]; it consists of:

    a) Micro Controller (a secure smart card controller from NXP from the SmartMX3 family);

    b) IC Dedicated Software (Micro Controller Firmware and Crypto Library);

    c) IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);

    d) Global Platform (GP) Framework;

- the Application Part of the TOE: "IDentity Applet v3.4/BAC";

- the associated guidance documentation.

The intended user of the product is the Card Issuer, who is in charge of the issuance of the product to the smart card holders.

7.3.1   TOE Architecture

The TOE "IDentity Applet v3.4/BAC" is a composite TOE, and is viewed as a unit of the following elements:

- the physical part of the travel document in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder:

    o the biographical data on the biographical data page of the travel document surface;

    o the printed data in the Machine-Readable Zone (MRZ);

    o the printed portrait.

- the logical travel document as data of the travel document holder stored according to the Logical Data Structure as specified by ICAO in [ICAO-TR1] on the contact based or contactless integrated circuit.

The stored data is protected with the following advanced security methods:

- Basic Access Control (BAC) defined in [TR-03110] and [ICAO-9303].

- Active Authentication defined in [ICAO-9303] (optional).

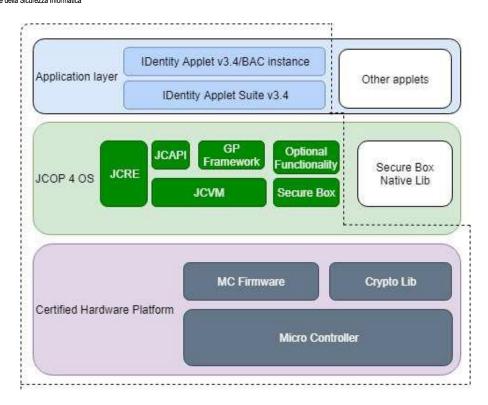Figure 1 shows the logical scope of the TOE and TOE boundaries.

Figure 1 - TOE logical scope and boundaries

The TOE is a composite TOE and the dashed line denotes the whole TOE. The underlying certified hardware platform and JCOP 4 OS are marked with purple and green. The blue box marks the application layer. The ID&Trust IDentity Applet Suite v3.4 could be loaded in the Flash. During the creation phase an instance is created in the Flash and after several configuration steps it will be personalized as IDentity Applet v3.4/BAC.

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

- the physical and logical parts of the TOE are described in sections 1.4.1 and 1.4.2 of [ST];

- the TOE life cycle is described in terms of four life cycle phases: Development, Manufacturing, Personalisation of the Travel Document, and Operational Use, described in sect. 1.4.4 of [ST], together with the operations allowed to users and administrators for each of them;

- the features of the Applet are provided in sect. 1.4.6 of [ST].

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 sect. 2.5 of the Security Target [ST].

7.3.2.2 Basic Access Control

The TOE "IDentity Applet v3.4/BAC" performs Basic Access Control using the commands GET CHALLENGE and EXTERNAL AUTHENTICATE with mutual authenticate function. Authentication and Key Establishment is provided by a three-pass challenge-response protocol using 3DES as block cipher.

Steps of Basic Access Control:

- The inspection system requests a challenge by sending the GET CHALLENGE command, the TOE responds with a generated nonce.

- The inspection system generates the necessary nonce and key material, computes the cryptogram, checksum and finally sends the EXTERNAL AUTHENTICATE command with mutual authenticate.

- The TOE checks the checksum of the cryptogram and decrypts it, then extracts the previously generated nonce from the concatenation and checks whether the inspection system returned the correct value. The TOE generates keying material and concatenation, then computes the cryptogram and its checksum and sends the response to the inspection system.

- The inspection system checks the checksum of the cryptogram and decrypts it, then extracts the nonce from the concatenation and checks if the returned value is correct.

- Both the inspection system and the TOE derive session keys.

The TOE uses two key 3DES in CBC mode with zero IV for computation of the cryptogram and MAC algorithm 3 with block cipher DES, zero IV (8 bytes) and padding method 2 for computation of the cryptographic checksums.

7.3.2.3 Security functions

The TOE security functions are described in detail in sect. 7.1 of the Security Target [ST]. The most significant aspects are summarized below:

- **AccessControl**: the TOE provides access control mechanisms that allow the maintenance of different security roles (Manufacturer, Personalisation Agent, Basic Inspection System) and the access control policies and functions.

- **Authenticate**: TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication. After activation or reset of the TOE no user is authenticated.

- **SecureManagement**: All security attributes under access control are modified in a secure way so that no unauthorized modifications are possible.

- **CryptoKey**: this functionality manages the generation of cryptographic keys on the platform and their destruction (overwriting) after use.

- **AppletParametersSign**: certain configuration and control parameters are signed, and this signature is verified before closing the Initialization phase. Only the unsigned parameters can be changed by the Initializer. This way only those Application Profiles can be applied which are validated by the Developer and conform to the requirements. The Initialization state cannot be finished by reaching the INITIALIZED state, and the personalization phase cannot be started without successful signature verification. These signatures can be verified during the whole IDentity Applet life-cycle, thus the non-authorized changed become detectable by applying this security functionality.

- **Platform**: covers the security functionalities based on the security functionalities of the certified cryptographic library and the certified IC Platform.

The IDentity Applet v3.4/BAC application provides the following security functionalities:

- ePassport security functionality (Data integrity).

- Active Authentication support function (prevention of the usage of a copied IC chip).

- Write protection function (protection against writing data on an already issued TOE).

- Verification of authenticity and integrity of user data (Passive Authentication).

7.4   Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

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

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.3 of this report.

7.5   Protection Profile conformance claims

The Security Target [ST] claims strict conformance to the following Protection Profile:

- BSI-CC-PP-0055, Protection Profile - Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009 [PP-055]

This PP defines the security objectives and requirements for the contactless chip of machine-readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the document [ICAO-9303].

7.6   Functional and assurance requirements

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

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Considering that the Security Target claims strict conformance to the Protection Profile BSI-CC-PP-0055 [PP-055], all extended functional requirements from this PP are also included:

- FIA_API.1 from the family FIA_API: Authentication Proof of Identity

- FAU_SAS.1 from the family FAU_SAS: Audit data storage

- FCS_RND.1 from the family FCS_RND: Generation of random numbers

- FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM: Limited capabilities and availability

- FPT_EMS.1 from the family FPT_EMS: TOE Emanation

The FIA_API family is taken from [PP-056] because of the optional functionality of the TOE (Active Authentication).

Please refer to the Security Target [ST] 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.

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].

Since 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" [JIL-COMP], as required by the international agreements CCRA and SOGIS. In this regard, it should be noted that the penetration tests have been completed on August 2020, within 18 months from the Platform vulnerability analysis (31 May 2019, the date of the oldest ETR for Composition indicated in the Platform certifications [NXP-CR1] and [NXP-CR2]).

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 [ST]. 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) CCLab Software Laboratory.

The evaluation was completed on 14 October 2020 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 16 October 2020. Then, the Certification Body issued this Certification Report.

7.8   General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. 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, and 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 Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "IDentity Applet v3.4/BAC" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_DVS.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

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.

Assurance classes and components		Verdict
Security Target evaluation	**Class 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	**Class 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	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		Verdict
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	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 1 - Final verdicts for assurance requirements

8.2   Additional assurance activities

The mandatory supporting document "Composite product evaluation for Smart Cards and similar devices" [JIL-COMP] includes additional assurance requirements that are specific to the composite TOE type.

The document defines refinements to existing assurance requirements for a composite product evaluation. The objective of these sub-activities is to precisely define the Evaluator tasks for the different parts of the composite TOE evaluation.

Table 2 summarizes the final verdict of the composition-specific assurance activities required by [JIL-COMP] carried out by the LVS.

Composition-specific assurance activities		Verdict
ASE_COMP: Consistency of composite product Security Target	ASE_COMP.1	Pass
ALC_COMP: Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1	Pass
ADV_COMP: Composite design compliance	ADV_COMP.1	Pass
ATE_COMP: Composite functional testing	ATE_COMP.1	Pass
AVA_COMP: Composite vulnerability assessment	AVA_COMP.1	Pass

Table 2 - Final verdicts for composition-specific assurance activities

8.3   Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product "IDentity Applet v3.4/BAC" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions and the Organizational Security Policies described, respectively, in sect. 3.3 and 3.5 of the Security Target [ST] are respected, particularly those compatible with the Platform (see [ST] sect. 2.5).

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

9 Annex A – Guidelines for the secure usage of the product

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

9.1 TOE Delivery

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

The delivery procedures between ID&Trust and NXP is the following:

1. The Developer (ID&Trust) develops a new version of the IDentity Applet v3.4.

2. After the new version is tested by ID&Trust a new release is issued and stored in configuration management system of ID&Trust.

3. The new version of the IDentity Applet v3.4 is sent to NXP.

4. NXP loads the applet into the Platform's chip.

The underlying Platform itself provides several security functions to protect IDentity Applet v3.4 during the transportation between several possible entities.

NXP offers two ways of delivery of the product:

1. The customer collects the product at the NXP site ("Collection").

2. The product is sent by NXP to the customer ("Shipment"). To guarantee that the product is not manipulated during the delivery, the product is delivered in parcels sealed with special tape. The tape is printed with consecutive numbers and has special adhesive features which make any manipulation visible. NXP encloses a form in the parcel which the customer is asked to return. By this NXP is informed that the customer has received the undamaged parcel.

Both methods guarantee that the customer gets authentic products. Additionally, the customer can use a special Transport Key to authenticate the chip.

More details on such procedures are contained in ID&Trust's IDentity Applet V3.4 Delivery Documentation [DEL].

9.2 Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure

operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- ID&Trust Identity Applet Suite User's Guide [ADM];

- ID&Trust Identity Applet Suite Administrator's Guide [USR].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product "IDentity Applet v3.4/BAC on NXP JCOP 4 P71", short name "IDentity Applet v3.4/BAC", 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 [ST], to which the evaluation results apply:

- The Platform "NXP JCOP 4 P71", developed by NXP Semiconductors Germany GmbH, certified at EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 [NXP-CR1]; it consists of:

  a) Micro Controller (a secure smart card controller from NXP from the SmartMX3 family);

  b) IC Dedicated Software (Micro Controller Firmware and Crypto Library);

  c) IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);

  d) Global Platform (GP) Framework;

- the Application Part of the TOE: "IDentity Applet v3.4/BAC" configured as an eMRTD application;

- the associated guidance documentation:

  o ID&Trust Identity Applet Suite User's Guide [ADM];

  o ID&Trust Identity Applet Suite Administrator's Guide [USR].

The Platform Micro Controller Firmware and IC Dedicated Software are covered by the following certification: "NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library" [NXP-CR2].

For more details, please refer to sect. 1.4 of the Security Target [ST].

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, 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.

11.1 Test configuration

For the execution of these activities a test environment was set up at the LVS site. The Developer provided all the resources needed for testing except the test tool and the card reader.

In particular, the Evaluators test configuration consisted of:

- the sample card identified as IDentity Applet v3.4.7470/BAC;

- the test card reader HID Omnikey 5x21 CL0;

- the test tool OpenSCDP with Eclipse 2018-12.

Before the tests, the software application has been initialized and configured in accordance with the guidance documentation [ADM] and [USR], as indicated in sect. 9.2. The Developer provided a personalization script for the installation of the TOE. The Evaluators were able to install the TOE to the underlying Platform correctly. The Evaluators successfully performed BAC authentication which is a proof that the card was installed properly and in a known state.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The test plan presented by the Developer was largely based on the following industry standard technical document:

- ICAO Technical Report, Radio Frequency Protocol and Application Test Standard for eMRTD Part 3 - Tests for Application Protocol and Logical Data Structure, Version 2.10 [ICAO-TR2].

In addition, the Developer designed independently additional proprietary tests in order to demonstrate the complete coverage of the functional requirements (SFRs) and of the security functions.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification.

11.2.3 Test results

The Evaluators executed a sample of tests from the developer test plan to analyze the repeatability and reproducibility of the industry standard and proprietary tests. The Evaluators compared the actual results of these tests with the expected results defined in the test specification and found that all tests produced the same actual results as the expected results.

11.3 Functional and independent tests performed by the Evaluators

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

The TSF includes a large number of interfaces, making it impractical to rigorously test all of them. So, the Evaluators decided to focus on testing authentication mechanisms of the TOE, using a sampling strategy to test the following interfaces:

- SELECT

- GET CHALLENGE

- EXTERNAL AUTHENTICATE

- READ BINARY

The Evaluators verified the actual test results and found that they were consistent with the expected test results.

Moreover, considering that the TOE is a composite product, the Evaluators verified the behavior of the TOE as a whole, carrying out the additional activities specified in the ATE_COMP family, according to the document [JIL-COMP], also taking into considerations the obligations and recommendations for the Applet evaluator in the Platform's ETR for Composition [ETR-COMP].

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE sample already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

Since the TOE is a composite product, the Evaluators carried out the additional activities specified in the AVA_COMP family, according to the document [JIL-COMP], and examined the results of the vulnerability assessment in the Platform's ETR for Composition [ETR-COMP] to determine that they can be reused for the composite evaluation of the Applet.

The Evaluators used two approaches: a sampling strategy was employed to test the functionality of a subset of the TSFIs instead of testing all of the interfaces, and a brute force attack was implemented and executed to discover any undocumented APIs. The Evaluators verified the behaviour of IDentity Applet v3.4/BAC as a whole, considering that it is a composite product.

The early phase of the vulnerability assessment was the information gathering about the TOE. As the initial step, multiple public searches were conducted with different keyword combinations (e.g., "Basic Access Control known vulnerabilities", "smartcard bac security research") to identify the publicly available bugs and vulnerabilities for the TOE. For this phase public vulnerability databases and research papers were reviewed as well. Publicly known vulnerabilities are either outdated or only relevant for the underlying platform, which is not in the scope of the evaluation. The conclusion of this phase was that the smart card technology is well documented and a potential attacker can get deep understanding of how a smart card and Basic Access Control works based on industry standards and publicly available information on smart cards. The documentation of the TOE is not publicly available (i.e., not on the manufacturer's website). This is a relevant information for the attack potential calculations. According to the publicly available information, no relevant public vulnerability was found for the TOE.

As a second step, the evaluators conducted a focused vulnerability analysis of the manufacturer documentation to identify potential vulnerabilities and areas of concern. As mentioned before, there is no publicly available documentation on the manufacturer's website. The Evaluators reviewed the functionalities of the TOE based on the documentation and by using tools provided by the manufacturer of the underlying platform to interact with the interfaces of the TOE. Due to the product type of the TOE and the strict standardization in the industry of smart cards, the Evaluators focused on potential vulnerabilities and testing related to the implementation of the authentication functionality.

With all the gathered intelligence about the TOE and the potential vulnerabilities, the Evaluators created an attack plan with different attack scenarios to meet the requirements of AVA_VAN.3. For the attack scenarios, exact attack potentials were calculated, considering that publicly available information about smart cards is very detailed, rich, and relatively easy to learn.

With the defined attack scenarios, the Evaluators conducted penetration tests against the TOE to identify any existing vulnerabilities.

The Evaluators defined the following attack scenarios:

- The attacker accesses protected data without proper authentication and secure channel. If Basic Access Control functionality is not implemented correctly, the related test would successfully collect sensitive data from the card.

- The attacker overwrites protected data of the user. If Basic Access Control functionality is not implemented correctly, the related test would successfully overwrite user data or sensitive security related data (e.g., identification or attack counter variable).

- The attacker discovers an undocumented interface. This interface would provide an additional attack surface.

Then the Evaluators tried to penetrate the protection of the TOE with the tests designed according to the above attack scenarios.

The results of the tests were documented with enough details for their repeatability, and the results were also gathered in a table for the sake of clarity.

The executed penetration test could not identify existing vulnerabilities in the TOE exploitable with an Enhanced-Basic attack potential.

During the site visits the Evaluators performed source code analysis with an enhanced focus on the implementation of Basic Access Control functionality and the applied countermeasures against side channel and fault injection attacks.

Based on the available information, the Evaluators did not identify residual vulnerabilities, i.e., vulnerabilities that could be exploited only by an attacker with attack potential beyond Enhanced-Basic.