Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

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. 1/23

(Certificate No.)

Prodotto: IDentity Applet v3.4-p2/QSCD 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+
(AVA_VAN.5)

Il Capo Servizio
Certificazione e Vigilanza
(Andrea Billet)

Roma, 15 febbraio 2023

[ORIGINAL SIGNED]

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IDentity Applet v3.4-p2/QSCD on NXP JCOP 4 P71

OCSI/CERT/CCL/10/2022/RC

Version 1.0

15 February 2023

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute 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	15/02/2023

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM Decreto del Presidente del Consiglio dei Ministri

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

OCSI Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

cPP collaborative Protection Profile

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

PP Protection Profile

SAR Security Assurance Requirement

SFR Security Functional Requirement

SOG-IS Senior Officials Group Information Systems Security

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

3.3 Other acronyms

API Application Programming Interface

CGA Certificate Generation Application

CRS Certificate Request Signature

CSP Certification Service Provider

DTBS/R	Data To Be Signed / Representation
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification Authentication and Signature
eMRTD	Electronic Machine Readable Travel Document
GP	Global Platform
HW	Hardware
IAS-ECC	Identification, Authentication and electronic Signature - European Citizen Card
ICAO	International Civil Aviation Organization
IC	Integrated Circuit
IFD	Interface Device
IT	Information Technology
JCOP	Java Card Open Platform
OS	Operating System
PIN	Personal Identification Number
PSO	Perform Security Operation
QSCD	Qualified Signature Creation Device
RAD	Reference Authentication Data
RSA	Rivest, Shamir, Adleman
SCA	Signature Creation Application
SCD	Signature Creation Data
SVD	Signature Verification Data
SW	Software
VAD	Verification Authentication Data

4 References

4.1 Normative references and national scheme documents

[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

[eIDAS] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014

[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, July 2020

[BSI-TR3] BSI Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version: 2.21, Date: 21. December 2016

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

[CR] Certification Report "IDentity Applet v3.4-p1/QSCD on NXP JCOP 4 P71", OCSI/CERT/CCL/07/2021/RC, Version 1.0, 11 October 2021

[ETRv2] "Evaluation Technical Report Evaluation Assurance Level EAL 4 augmented with AVA_VAN.5 based on ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security ID &Trust Identity Applet v3.4-p2/QSCD, v2, CCLab Software Laboratory, 20 December 2022

[ETRv3] "Evaluation Technical Report Evaluation Assurance Level EAL 4 augmented with AVA_VAN.5 based on ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security ID &Trust Identity Applet v3.4-p2/QSCD, v2, CCLab Software Laboratory, 2 February 2023

[ETR-COMP] Evaluation Technical Report for Composition NXP "JCOP 4 P71" – EAL6+, Version: 11.0, Date: 14 September 2022

[IAS-ECC] European Card for e-Services and National e-ID Applications - IAS ECC, Revision 1.0.1, 23 February 2009

[ICAO-TR] 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 "JCOP 4 P71", NSCIB-CC-180212-CR5, TÜV Rheinland Nederland B.V., Report version: 1, Date: 26 September 2022

[NXP-CR2] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4)", BSI-DSZ-CC-1136-V3-2022, BSI - Bundesamt für Sicherheit in der Informationstechnik, 7 September 2022

[PPQSCD1] EN 419211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation

[PPQSCD2] EN 419211-4:2013, Protection profiles for Secure signature creation device - Part 4: Device with key generation and trusted communication with certificate generation application

[ST] "Security Target IDentity Applet v3.4-p2/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS", Version: v1.09, ID&Trust Ltd., 1 February 2023

[USR] ID&Trust IDentity Applet Suite User's Guide, Version: 3.4.5, Date: October 2022

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 recognised under the terms of this agreement by signatory nations.

This certificate is recognised 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] was ratified on 8 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-p2/QSCD on NXP JCOP 4 P71”, short name “ID & Trust Identity Applet v3.4-p2/QSCD”, developed by ID&Trust Ltd.

The TOE is a Qualified Signature Creation Device (QSCD) representing a contact or contactless integrated circuit chip with IC Dedicated Software (Micro Controller Firmware, Crypto Library), Embedded Software (JCOP4) and IDentity Applet v3.4-p2/QSCD which functions to generate signature creation data (SCD) and create qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized signatory can use it. Additionally, the TOE supports its authentication as QSCD by the certificate generation application (CGA) of the Certification service provider (CSP) and a trusted communication with this CGA for protection of signature verification data (SVD) generated and exported by the TOE and imported by CGA.

The TOE is a composite product and comprises:

- underlying platform of the TOE “JCOP 4 P71”, which is evaluated by Brightsight and certified at Evaluation Assurance Level, EAL6 augmented by ASE_TSS.2 and ALC_FLR.1, by TÜV Rheinland Nederland B.V.;
- the application part of the TOE: “ID&Trust IDentity Applet Suite v3.4-p2/QSCD”;
- 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 Applet v3.4-p1/QSCD on NXP JCOP 4 P71), already certified by OCSI (Certificate no. 10/21 of October 11, 2021 [CR]).

The IDentity Applet Suite v3.4 is a multi-purpose smart card platform, that is compliant with the most relevant standards (e.g., [IAS-ECC], [BSI-TR_3], [ICAO]).

The product modification is necessary to meet the Customer’s requirements and because of the new JCOP4 P71 Platform certification [NXP-CR1]. The modified Applet components are outside of the scope of the TOE: the changes do not have any security impact on the TOE. In addition, the new platform certification does not affect the TOE, so it is a minor modification. Evaluators were able to reuse part of the documentation and evidences already provided in the previous evaluation.

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 AVA_VAN.5, 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-p2/QSCD” 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-p2/QSCD on NXP JCOP 4 P71
Security Target	Security Target IDentity Applet v3.4-p2/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS, Version: v1.09, ID&Trust Ltd., 1 February 2023 [ST]
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5
Developer	ID&Trust Ltd.
Sponsor	NXP Semiconductors Germany GmbH
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	EN 419 211-2:2013 [PPQSCD1] EN 419 211-4:2013 [PPQSCD2]
Evaluation starting date	9 June 2022
Evaluation ending date	20 December 2022

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 is IDentity Applet v3.4-p2/QSCD on NXP JCOP 4 P71, which claims conformance to Protection profiles for secure signature creation device — Part 2: Device with key generation and Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application.

The TOE is a Qualified Signature Creation Device (QSCD) representing a contact or contactless integrated circuit chip with IC Dedicated Software (Micro Controller Firmware, Crypto Library), Embedded Software (JCOP4) and IDentity Applet v3.4-p2/QSCD which functions to generate Signature Creation Data (SCD) and create qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized signatory can use it. Additionally, the TOE supports its authentication as QSCD by the certificate generation application (CGA) of the Certification service provider (CSP) and a trusted communication with this CGA for protection of signature verification data (SVD) generated and exported by the TOE and imported by CGA.

The TOE stores SCD and Required Authentication Data (RAD). The TOE may store multiple instances of SCD. In this case the TOE provides a function to identify each SCD and the Signature-Creation Application (SCA) can provide an interface to the signer to select an SCD for use in the signature creation function of the QSCD.

The TOE supports Certificate Request Signature (CRS) to provide evidence about the validity of the SVD for the CGA. The CRS also proves that the SVD belongs to the TOE.

The CRS key pair is generated separately from the SCD/SVD key pair on the TOE, but in case of the generation of the SCD/SVD key pair, the TOE signs the SVD with the private CRS key. So, the CGA is able to verify the validity of the SVD by checking the CRS.

The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. 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 (MC FW 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-p2/QSCD”;
- the associated guidance documentation.

A certification service provider and a qualified trust service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions may include:

- initializing the RAD;
- generating a key pair;
- storing personal information of the legitimate user.

After preparation, the SCD shall be in a non-operational state. Upon receiving a TOE, the Signatory shall verify its non-operational state and change the SCD state to operational.

After preparation, the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, providing this information shall protect the confidentiality of the corresponding RAD. There is a special VAD, which can be used only once in the TOE lifetime, the Signature Transport PIN, which has to be changed to Signature PIN in order to create digital signatures.

If the use of an SCD is no longer required, then it can be destroyed (e.g. overwritten) as well as the associated certificate info, if any exists.

7.3.1 TOE architecture

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

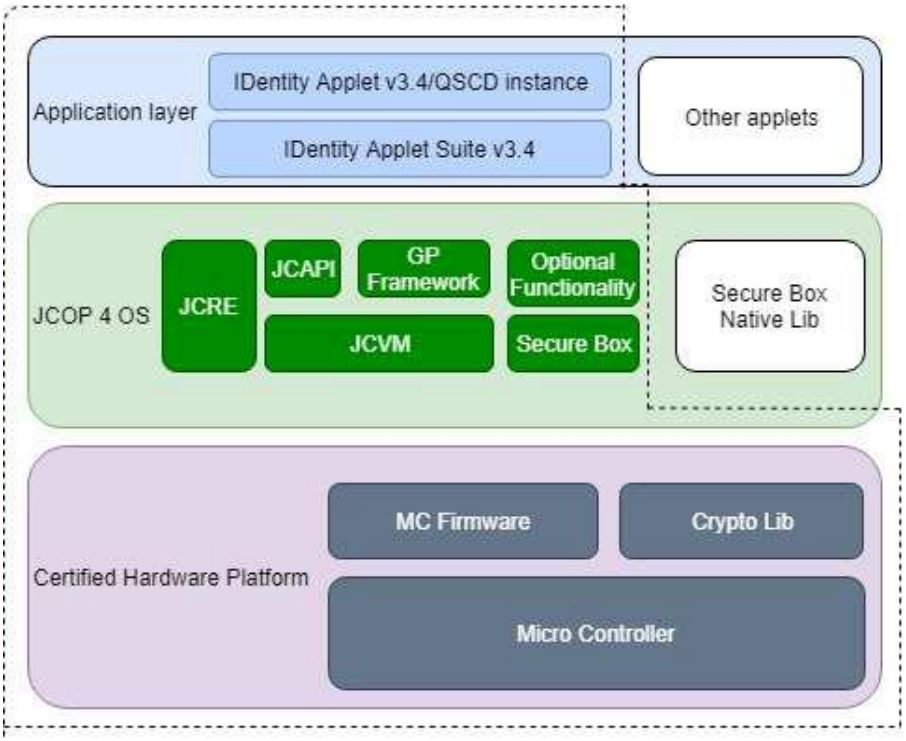

Figure 1 - TOE logical scope and boundaries

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. In this Certification Report the common short name of certified hardware platform and JCOP 4 OS is Platform.

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-p2/QSCD.

The boxes marked white are not certified.

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 section 1.4.2 of [ST];
- the TOE life cycle is described in section 1.4.5 of [ST] in terms of the Development, Preparation and Operational Use stages;
- the TOE security features are summarized in section 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 section 2.4 of the Security Target [ST].

7.3.2.2 QSCD functionality

The TOE as a qualified signature creation device has the following distinct operational environments:

- the preparation environment, where it interacts with a certification service provider through a certificate-generation application (CGA) to obtain a certificate for the signature verification data (SVD) corresponding with signature creation data (SCD) the TOE has generated. The TOE can export the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference authentication data (RAD);
- the signing environment where it interacts with a signer through a signature-creation application (SCA) to sign data after authenticating the signer as its signatory. The signature-creation application provides the unique representation of data to be signed, thereof (DTBS/R) as input to the TOE signature-creation function and obtains the resulting digital signature;
- the management environments where it interacts with the user or a qualified trust service provider to perform management operations, e.g., for the signatory to reset a blocked RAD. A single device, e.g., a smart card terminal, may provide the required secure environment for management and signing.

The TOE is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The QSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory. It comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature, providing the following functions:

- to generate signature-creation data (SCD) and the correspondent signature-verification data (SVD):
    - The TSF is capable of generating an SCD/SVD pair in accordance with specified cryptographic key generation algorithms:

    - RSA with cryptographic key sizes 1024-4096 bits and
    - ECDSA cryptographic key sizes 160-521 bits;
- to export the SVD for certificate generation through a trusted channel to the CGA;
- to prove the identity of the TOE as QSCD to external entities;
- to optionally, receive and store certificate info;
- to switch the TOE from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps:
    - select an SCD if multiple are present in the QSCD;
    - authenticate the signatory and determine its intent to sign;
    - receive the unique representation of data to be signed thereof (DTBS/R);
    - apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

The IDentity Applet v3.4-p2/QSCD performs Qualified Signature Creation using the commands PSO hash and PSO compute digital signature. The service is performed in two steps. The first one performs the last round of the partial hash, and the second one realizes the digital signature computation over the entire hash computed thanks to the last round computation.

Steps of Qualified Signature Creation:

- the IFD (Interface Device) performs the partial hash calculation over M. The computation outcomes are the following:
    - PartialHash(M);
    - Counter(M);
    - RemainingMessage(M);
- the IFD sends partial hash data to the Integrated Circuit Card and require final hash round calculation. Using the command ‘PSO Hash’;
- the Integrated Circuit Card initializes the hashing context with incoming data resulting from the partial hash calculation, then ends the hash over the last data block. Hash(M) is available;
- the IFD requires the signature calculation. Using the command ‘PSO Compute Digital Signature’;
- the card calculates the signature with the selected private key and returns the result.

7.3.2.3 Security functions

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

- **AccessControl**: this function provides the access controls to data in the file system, initialization, personalization and pre-personalization data. During earlier life phases, when the applet may not be present yet, the Platform responsible for managing the accesses correctly.
  The TOE provides access control mechanisms that allow the maintenance of different security roles: Administrator role and Signatory role.
  The AccessControl function provides that the Signatory role is only valid in Operational phase of IDentity Applet life cycle.
  The AccessControl function ensures that nobody is allowed to read all TOE intrinsic secret cryptographic keys stored in the TOE, such as RAD, SCD.
  The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication;

- **Authenticate**: this function manages the identification and authentication of the Signatory and Administrator and enforces role separation. After activation or reset of the TOE no user is authenticated. TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication;

- **SecureManagement**: all security attributes are modified in a secure way so that no unauthorised modifications are possible. This function is responsible for the secure management of the security attributes, data and functions;

- **TrustedChannel**: this function is responsible for the command and response exchanges between the TOE and the external devices (e.g., CGA) and it is responsible for confidentiality, data integrity and data authenticity;

- **CryptoKey**: this function is responsible for providing cryptographic support to all the other TSFs, including secure key generation (SCD/SVD key pair) and digital signature creation. It also provides a secure key destruction method;

- **AppletParametersSign**: during the IDentity Applet life cycle phases after LOADED state of the IDentity Applet, it becomes the default Application and reaches SELECTABLE state of IDentity Applet. This phase is called the Initialization phase of IDentity Applet. 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 of IDentity Applet, and the personalization phase of IDentity Applet 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.

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 of the TOE in accordance with the requirements of the Security Target [ST].

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

7.5 Protection Profile conformance claims

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

- EN 419211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation [PPQSCD1];
- EN 419211-4:2013, Protection profiles for Secure signature creation device - Part 4: Device with key generation and trusted communication with certificate generation application [PPQSCD2].

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 Profiles EN 419211-2:2013 [PPQSCD1] and EN 419211-4:2013 [PPQSCD2], the ST also includes the following extended functional requirements from these PPs:

- FIA_API.1 from the family FIA_API: Authentication Proof of Identity;
- FPT_EMS.1 from the family FPT_EMS: TOE Emanation.

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 were completed on 21 September 2022, within 18 months from the Platform vulnerability analysis (25 August 2022, 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 20 December 2022 with the issuance by LVS of the Evaluation Technical Report [ETRv2], which was approved by the Certification Body on 22 December 2022. An additional ETR ([ETRv3]) was delivered on 6 February 2023 including minor editorial changes. 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 regularly check 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 [ETRv2] 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-p2/QSCD" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with AVA_VAN.5, 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 AVA_VAN.5.

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
Identification of security measures	ALC_DVS.1	Pass

Assurance classes and components		Verdict
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
Advanced methodical vulnerability analysis	*AVA_VAN.5*	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
ADV_COMP: Composite design compliance	ADV_COMP.1	Pass
ALC_COMP: Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1	Pass
ASE_COMP: Consistency of composite product Security Target	ASE_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 section 6 (Statement of Certification).

Potential customers of the product “IDentity Applet v3.4-p2/QSCD” 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 section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational Security Policies and the Assumptions described, respectively, in section 3.3 and 3.4 of the Security Target [ST] are respected, particularly those compatible with the Platform (see [ST] section 2.4).

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

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “IDentity Applet v3.4-p2/QSCD on NXP JCOP 4 P71”, short name “IDentity Applet v3.4-p2/QSCD”, 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 (MC FW 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-p2/QSCD”;
- the associated guidance documentation:
  - ID&Trust Identity Applet Suite User’s Guide [USR];
  - ID&Trust Identity Applet Suite Administrator’s Guide [ADM].

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 section 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 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.

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/QSCD 024A;
- the test card reader Gemalto Prox-DU Contactless_12400279 0;
- the test tools OpenSCDP with Eclipse 2018-12, GlobalTester TestManager.

Before the tests, the software application has been initialized and configured in accordance with the guidance documentation [ADM] and [USR], as indicated in section 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 selected the QSCD applet 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 documents:

- 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-TR];
- BSI Technical Guideline TR-03105 Part 3.4: Test plan for eID-Cards with eSign-application acc. to BSI TR-03117, Version 1.0, 01 April 2010 [BSI-TR].

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 analyse the repeatability and reproducibility of the industry standard and proprietary tests. The Evaluator has conducted some of these tests, on the Developer's site during site visit 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

The Evaluators decided to focus on testing the immutability of essential data on the TOE, using a sampling strategy to test the following interfaces:

- PUT DATA;
- Comprehensive testing for all possible undocumented TSFIs.

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 behaviour 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-p2/QSCD 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 on 1st September 2022,

with different keyword combinations (e.g. ‘smartcard’, ‘QSCD vulnerabilities’, ‘Password Authenticated Connection Establishment’, PACE, ‘vulnerabilities’, ‘attack’, ‘attack techniques to sscd’, ‘BAC vulnerabilities’, ‘BAC exploit’, ‘EAC exploits’, ‘EID vulnerabilities’, ‘sscd exploits on smart cards’, ’Java Card Applet vulnerabilities’, ‘PIN Attack’, ‘PKCS vulnerabilities’) 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 this evaluation. The conclusion of this phase was that the smart card technology is well documented, and attacker can get deep understanding of how a smart card and electronic signature devices work based on industry standards and publicly available information on smart cards. The documentation of the TOE is not publicly available (i.e., not available 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 manufacturer documentation was used to get familiar with the electronic signature functionalities and to identify the possible attack surfaces. As mentioned before, there is no publicly available documentation on the Manufacturer's website. The Evaluator got the first impression about 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. During this step the Evaluator identified possible attack vectors related to possible undocumented interfaces. Due to the product type of the TOE and the strict standardization in the industry of smart cards the Evaluator focused on potential vulnerabilities and testing related to the implementation of the electronic signature functionality. The Evaluator gained insight based on the information gathering that authentication related potential vulnerabilities should be investigated.

With all the gathered intelligence about the TOE and the possible vulnerabilities, the Evaluator created an attack plan broken down to different attack scenarios. For the attack scenarios, exact attack potentials were calculated, taking into account the fact, that publicly available information about smart cards are very detailed, rich, and relatively easy to learn.

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

- the attacker attempts to unblock a previously blocked PIN of the eSIGN application by bypassing the required authentication for such operation;
- the attacker attempts to modify sensitive data that belongs to the eSIGN application and is required for safe and correct functionality;
- the attacker discovers undocumented interfaces, which can be used as attack surface for further escalation.

Then the Evaluator has tried to successfully penetrate the protection of the TOE using the tests defined by the above attack scenarios.

The results of the tests were documented with enough details for their repeatability.

The executed penetration test could not identify existing vulnerabilities in the TOE with High attack potential.

During site visit the Evaluator performed source code analysis with an enhanced focus on the implementation of authentication functionalities and the applied countermeasures against side channel and fault injection attacks.

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