Agenzia per la Cybersicurezza Nazionale

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. 4/23

(Certificate No.)

Prodotto: IDentity Applet v3.4-p2/eIDAS 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, ATE_DPT.2, AVA_VAN.5)

p. il Direttore Generale
dell'ACN

Il Capo Servizio
Certificazione e Vigilanza
(Andrea Billet)

Roma, 17 febbraio 2023

[ORIGINAL SIGNED]

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

This page is left intentionally blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

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

OCSI/CERT/CCL/11/2022/RC

Version 1.0

17 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	17/02/2023

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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Arrangement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other Acronyms

3DES	Triple DES
AES	Advanced Encryption Standard
API	Application Programming Interface
BAC	Basic Access Control

CAN	Card Access Number
CGA	Certificate Generation Application
DTBS/R	Data To Be Signed / Representation
EAC	Extended Access Control
EAL	Evaluation Assurance Level
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
IT	Information Technology
JCOP	Java Card Open Platform
LDS	Logical Data Structure
MRZ	Machine-Readable Zone
OS	Operating System
PACE	Password Authenticated Connection Establishment
PACE-CAM	PACE with Chip Authentication Mapping
PACE-GM	PACE with Generic Mapping
PIN	Personal Identification Number
QSCD	Qualified Signature Creation Device
RSA	Rivest, Shamir, Adleman
SCD	Signature Creation Data
SVD	Signature Verification 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

[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] IDentity Applet Suite v3.4 Administrator's Guide

[CR] Certification Report "IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71", OCSI/CERT/SYS/08/2016/RC, Version 1.0, 28 October 2020

[DEL] IDentity Applet v3.4 – The Delivery Documentation, Version: v0.02, Date: 2020-02-10

[ETRv2] "IDentity Applet v3.4-p2/eIDAS on NXP JCOP 4 P71" Evaluation Technical Report, v2, CCLab Software Laboratory, 20 December 2022

[ETRv3] "IDentity Applet v3.4-p2/eIDAS on NXP JCOP 4 P71" Evaluation Technical Report, v3, CCLab Software Laboratory, 7 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, 21.03.2008

[ICAO] ICAO Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015

[ICAO-9303-6] ICAO Doc 9303, Part 1: Machine Readable Passports, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, Sixth Edition – 2006

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

[NXP-CR2] Certification Report "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

[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

[PP-068] BSI-CC-PP-0068-V2-2011-MA-01, Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22 July 2014

[PP-086] BSI-CC-PP-0086, Protection Profile - Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2 PP), Version 1.01, 20 May 2015

[PP-087] BSI-CC-PP-0087, Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP), version 1.01, 20 May 2015

[PPSSCD] BSI-CC-PP-0059-2009-MA-01, Protection Profiles for secure signature creation device - Part 2: Device with key generation, Version: 2.0.1, Date: 21 February 2012

[TR-03110-1] BSI: TR-03110-1 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version: 2.20, Date: 26. February 2015

[TR-03110-2] BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 21 December 2016

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

[ST] Security Target ID&Trust IDentity Applet v3.4-p2/eIDAS – Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification and Active Authentication, Version: v1.06, Date: 01 February 2022

[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 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-p2/eIDAS on NXP JCOP 4 P71”, short name “IDentity Applet v3.4-p2/eIDAS”, developed by ID&Trust Ltd.

The TOE is a contactless smart card with the IDentity Applet Suite v3.4-p2 configured as IDentity Applet/eIDAS. The TOE is applicable as an electronic document with three applications (ePassport, eID and eSign), which comply to the relevant eIDAS standards and provides all necessary security protocols (PACE, EAC1 and EAC2).

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-p2/eIDAS”;
- 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/eIDAS on NXP JCOP 4 P71”, already certified by OCSI (Certificate n. 12/20 of October 28, 2020 [CR]). The re-evaluation will be carried out in accordance with the Common Criteria Evaluation and Validation process and scheme requirements.

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], [TR-03110-3], [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 is not affecting the TOE, so it is a minor modification. The 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 ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B of this Certification Report.

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

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “IDentity Applet v3.4-p2/eIDAS” 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/eIDAS on NXP JCOP 4 P71
Security Target	Security Target ID&Trust IDentity Applet v3.4-p2/eIDAS – Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification and Active Authentication, Version: v1.06, Date: 01 February 2023 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and 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	BSI-CC-PP-0087 [PP-087] BSI-CC-PP-0056-V2-2012 [PP-056] BSI-CC-PP-0086 [PP-086] BSI-CC-PP-0059-2009-MA-01 [PPSSCD] BSI-CC-PP-0068-V2-2011-MA-01 [PP-068]
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 “IDentity Applet v3.4-p2/eIDAS” is a smart card programmed according to [TR-03110-1] [TR-03110-2]. The smart card contains multiple applications (at least one). The programmed smart card is called an electronic document as a whole. Here, an application is a collection of data(groups) and their access conditions. We mainly distinguish between common user data, and sensitive user-data. Depending on the protection mechanisms involved, these user data can further be distinguished as follows:

- EAC1-protected data: Sensitive User Data protected by EAC1 (cf. [TR-03110-1])
- EAC2-protected data: Sensitive User Data protected by EAC2 (cf. [TR-03110-2]), and
- all other (common) user data: Other user data are protected by Password Authenticated Connection Establishment (PACE, cf. also [TR-03110-2]). Note that EAC1 recommends, and EAC2 requires prior execution of PACE

In addition to the above user data, there are also data required for TOE security functionality (TSF). Such data is needed to execute the access control protocols, to verify integrity and authenticity of user data, or to generate cryptographic signatures.

Application considered in [TR-03110-1] and [TR-03110-2] are

1. an electronic passport (ePass) application;
2. an electronic identity (eID) application and
3. a signature (eSign) application.

For more information about the possible configurations, see section 1.4.5 of [ST].

The TOE may also functionally support BAC, but this protocol is outside of the security policy defined by the Security Target [ST], and it’s not covered by the evaluated configuration of the TOE.

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:
  - Micro Controller (a secure smart card controller from NXP from the SmartMX3 family);
  - IC Dedicated Software (Micro Controller Firmware and Crypto Library);
  - IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);
  - Global Platform (GP) Framework;
- the Application Part of the TOE: “IDentity Applet v3.4-p2/eIDAS”;
- the associated guidance documentation:
  - ID&Trust Identity Applet Suite User’s Guide [USR];
  - ID&Trust Identity Applet Suite Administrator’s Guide [ADM].

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-p2/eIDAS” 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:
  - the biographical data on the biographical data page of the travel document surface;
  - the printed data in the Machine-Readable Zone (MRZ);
  - the printed portrait;
- the logical travel document as data of the travel document holder stored according to the Logical Data Structure (LDS) as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the travel document holder:
  - the digital Machine-Readable Zone Data (digital MRZ data);
  - the digitized portraits;
  - the biometric reference data of finger(s) and/or iris image(s);
  - the other data according to LDS;
  - the Document Security Object.

The TOE has two subsystems:

- the applet;
- the underlying platform.

Figure 1 shows the TOE boundaries, the dashed line denotes the whole composite 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-p2 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/eIDAS.

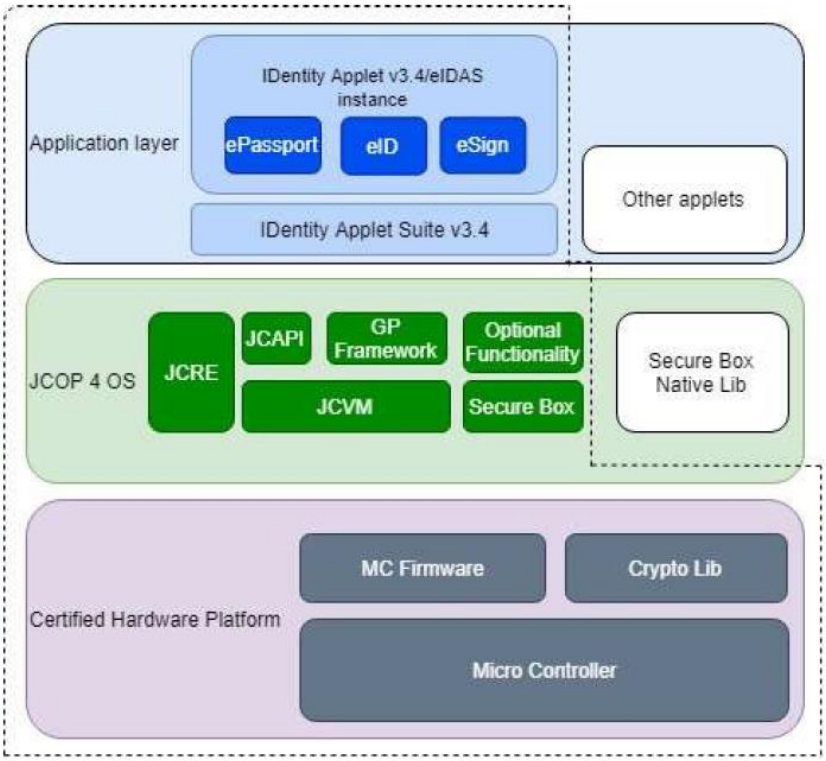

Figure 1 - TOE boundaries

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 terms of four life cycle phases: Development, Manufacturing, Personalisation of the Electronic Document, and Operational Use, described in section 1.4.3 of [ST], together with the operations allowed to users and administrators for each of them;
- the features of the Applet are provided in section 1.4.5 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 2.5 of the Security Target [ST].

7.3.2.2 ePassport functionality (PACE)

PACE is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and password-based authentication of the eMRTD chip and the inspection system. PACE establishes Secure Messaging between an eMRTD chip, and an inspection system based on weak (short) passwords. The security context is established in the Master File. The protocol enables the eMRTD chip to verify that the inspection system is authorized to access stored data and has the following features:

- strong session keys are provided independent of the strength of the password

- the entropy of the password(s) used to authenticate the inspection system can be very low

PACE uses keys derived from passwords with a key derivation function. The key can be derived from the Machine-Readable Zone (MRZ) or from the Card Access Number (CAN).

PACE supports the following Mappings:

- Generic Mapping;
- Integrated Mapping;
- Chip Authentication Mapping.

The PACE implementation of IDentity Applet v3.4-p2/eIDAS uses the READ BINARY, MSE: SET AT, GENERAL AUTHENTICATE commands.

Steps of Password Authenticated Connection Establishment:

- the inspection system sends a READ BINARY command to the TOE followed by an MSE: SET AT command (MANAGE SECURITY ENVIRONMENT command with SET Authentication Template function);
- as a result of a chain of GENERAL AUTHENTICATE commands the TOE randomly and uniformly chooses a nonce, encrypts it with the previously defined shared password and sends the ciphertext to the inspection system;
- the inspection system recovers the plaintext with the shared password;
- the TOE and the inspection system exchange additional data for the mapping of the nonce. For example, for Generic Mapping they exchange ephemeral key public keys, for Integrated Mapping the TOE sends an additional nonce to the inspection system;
- both the TOE and the inspection system compute the ephemeral domain parameters and perform an anonymous Diffie-Hellman key agreement based on the ephemeral domain parameters and generate the shared secret. During Diffie-Hellman key agreement the TOE checks whether the two public keys differ. Then the session keys are derived and the TOE and the inspection system exchange and verify the authentication token.

For Diffie-Hellman and Elliptic-curve Diffie-Hellman PACE uses 3DES or AES as cipher with key length 112, 128, 192 or 256. IDentity Applet v3.4-p2/eIDAS uses only prime curves with uncompressed points.

7.3.2.3 eID functionality

The claimed Extended Access Control 2 includes the PACE protocol described above, and also the following protocols according to [TR-03110-2]:

- *Chip Authentication Version 2*:
  The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip. The protocol in Version 2 provides explicit authentication of the MRTD chip by verifying the authentication token and implicit authentication of the stored data by performing Secure Messaging using the new session key. If Chip Authentication was successfully performed, Secure Messaging is restarted using the derived session keys. Otherwise, Secure Messaging is continued using the previously established session key (PACE).

- *Terminal Authentication Version 2*:
  The Terminal Authentication Protocol is a two-move challenge-response protocol that provides explicit unilateral authentication of the terminal. Terminal Authentication enables the MRTD chip to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication must be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that will be used to set up Secure Messaging with Chip Authentication Version 2. The MRTD chip must bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal. If Terminal Authentication was successfully performed, the MRTD chip shall grant access to stored sensitive data according to the effective authorization of the authenticated terminal. The MRTD chip shall however restrict the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key, i.e., the MRTD chip shall compare the compressed representation of the terminal's ephemeral public key received as part of Terminal Authentication with the compressed representation of the ephemeral public key provided by the terminal as part of Chip Authentication. The MRTD chip must not accept more than one execution of Terminal Authentication within the same session.
- *Restricted Identification*:
  The Restricted Identification Protocol is a static Diffie-Hellman key agreement protocol that generates a sector-specific identifier of the MRTD chip with the following properties:
  - within each sector the sector-specific identifier of every MRTD chip is unique;
  - across any two sectors, it is computationally infeasible to link the sector-specific identifiers of any MRTD chip.

  The sector-specific identifier is used to (re-)identify the MRTD chip within each sector. Chip Authentication and Terminal Authentication must have been successfully performed before Restricted Identification is used.
  The MRTD chip's security status is not affected by Restricted Identification.

7.3.2.4 As an eSIGN application:

An eSign application, as defined in [TR-03110-2], is intended to generate qualified electronic signatures. The IDentity Applet v3.4/eIDAS is in strict conformance to [PPSSCD], which is required for QSCD.

It is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The eSIGN application 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 digital 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 certification;
- 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 eSIGN application;
    - 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/eIDAS 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.

7.3.2.5 Security functions

The document [ST] in section 7.1 lists the following security functions:

- **AccessControl**: The TOE enforces access control in order to ensure that only authorized users access User Data and TSF-data and maintains different security roles;
- **Authenticate**: The TOE supports several authentication mechanisms in order to authenticate Users, Terminals and to prove the genuineness of the electronic document. The supported mechanism and protocols are based on the following ICAO and BSI standards [ICAO-TR1], [ICAO-9303-6], [TR-03110-1], [TR-03110-2] and [TR-03110-3];
- **SecureManagement**: The TOE enforces the secure management of the security attributes, data and functions. Furthermore, the TOE restricts the available commands in each TOE life-cycle phase;

- **CryptoKey**: The TOE uses several cryptographic services such as digital signature creation and verification, asymmetric and symmetric cryptography, random number generation and complete key management. Furthermore, CryptoKey provides the secure messaging for the TOE;
- **AppletParametersSign**: The TOE enforces the integrity of itself in each life cycle phases;
- **Platform**: The TOE relies on the certified functions and services of the Platform. This TSF is collection of those SFRs, which are uses these functions and services.

7.4 Documentation

The guidance documentation specified in Annex A 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 section 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-0087, Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP), version 1.01, 20 May 2015 [PP-087].

This PP describes the requirements for a smart card programmed according to [TR-03110-1] and [TR-03110-2]. The smart card contains multiple applications (at least one). The programmed smart card is called an electronic document as a whole.

The PP BSI-CC-PP-0087 claims strict conformance to the following PPs:

- BSI-CC-PP-0059-2009-MA-01, Common Criteria Protection Profiles for Secure Signature Creation Device - Part 2: Device with key generation [PPSSCD];
- 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 [PP-056];
- BSI-CC-PP-0086, Protection Profile - Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2 PP), Version 1.01, 20 May 2015 [PP-086].

Since the last two above PPs claim strict conformance to [PP-068], the PP BSI-CC-PP-0087 implicitly also claims strict conformance to:

- BSI-CC-PP-0068-V2-2011-MA-01, Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22 July 2014 [PP-068];

However since [PP-056] and [PP-086] already claim strict conformance to [PP-068], this implicit conformance claim is formally mostly ignored within this ST for the sake of presentation.

The ST conformance claim covers the part of the security policy for the eSign application of the TOE corresponding to the security policy defined in [PPSSCD], and hence is applicable if the eSign application is operational.

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-0087 [PP-087], all extended functional requirements from this PP are also included:

- FAU_SAS.1 from the family FAU_SAS from [PP-068]: Audit data storage;
- FCS_RND.1 from the family FCS_RND from [PP-068]: Generation of random numbers;
- FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM from [PP-068]: Limited capabilities and availability;
- FPT_EMS.1 from the family FPT_EMS from [PP-068]: TOE Emanation;
- FIA_API.1 from the family FIA_API from [PP-086]: Authentication Proof of Identity.

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 30 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 7th 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. 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 [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/eIDAS" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_DVS.2, ATE_DPT.2 and 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
Sufficiency of security measures	*ALC_DVS.2*	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: security enforcing modules	*ATE_DPT.2*	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/eIDAS” 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 sections 3.3 and 3.4 of the Security Target [ST] are respected, particularly those compatible with the Platform (see [ST] section 2.5).

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A 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 [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/eIDAS on NXP JCOP 4 P71”, short name “IDentity Applet v3.4-p2/eIDAS”, 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 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:
  - Micro Controller (a secure smart card controller from NXP from the SmartMX3 family);
  - IC Dedicated Software (Micro Controller Firmware and Crypto Library);
  - IC Embedded Software JCOP 4 (Java Card Virtual Machine, Runtime Environment, Java Card API);
  - Global Platform (GP) Framework;
- the Application Part of the TOE: “IDentity Applet v3.4-p2/eIDAS”;
- 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 ALC_DVS.2, ATE_DPT.2 and 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/eIDAS 024A;
- the test card reader Gemalto Prox-DU Contactless_12400279 0;
- the test tool 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 eIDAS 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 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-TR2];
- BSI Technical Guideline TR-03105 Part 3.3: Test Plan for eID-Cards with Advanced Security Mechanisms - EAC 2, Version 1.03, 24 September 2010 [BSI-TR2];
- Amendment to BSI TR-03105 Part 3.3, Release 3, 04 June 2012 [BSI-TR2A];
- 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-TR3];
- Test plan for eID-Cards with eIDAS v1.0.0.

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 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 have designed independent testing to verify the correctness of the TSFI.

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/eIDAS 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 (eg. '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 the evaluation. The conclusion of this first phase was that the smart card technology is well documented and a potential attacker can get deep understanding of how a smart card and an electronic passport work 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 manufacturer documentation was reviewed to achieve familiarity with the TOE, its electronic identification functionalities, and to identify the possible attack surfaces. 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. During this step the Evaluators 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 Evaluators focused on potential vulnerabilities and testing related to the implementation of the authentication functionality. The Evaluators 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 potential vulnerabilities, the Evaluators created an attack plan with different attack scenarios. For the attack scenarios, exact attack potentials were calculated, considering 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 any existing vulnerabilities.

The Evaluators defined the following attack scenarios:

- The attacker attempts to conduct a PIN verification forced through an insecure channel. Succeeding with such an attack would result in new attack surfaces as sensitive and security related data could be sniffed using man-in-the-middle type attacks;
- The attacker attempts to modify sensitive, non-modifiable data in the application. By breaching the necessary security protocols, a successful attack would render the target non-compliant with the relevant eIDAS standards as it would be a subject of forgery;
- The attacker discovers undocumented interfaces, which can be used as attack surface for further escalation.

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.

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

During the site visits the Evaluators 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 Evaluators did not identify residual vulnerabilities, i.e., vulnerabilities that could be exploited only by an attacker with attack potential beyond High.