

Aruba PEC S.p.A.

Description of the IDS Platform and Identity Proofing processes

Version: 1.0

Last update: 29.09.2026

Document classification: Public

VERSION	DATE	CHANGELOG
1.0	29/09/2026	First issue

SOMMARIO

1	INTRODUCTION AND ADMINISTRATION	3
1.1	Overview	3
1.2	Document administration	3
1.2.1	Document version and responsible organisation	3
1.2.2	Parties responsible for approval	4
1.3	Definitions	4
2	IDS PLATFORM	6
2.1	DS Platform — Introduction	6
2.1.1	Actors and operational responsibilities	6
2.1.2	Architecture and configuration	6
2.1.3	Application integration, APIs and interfaces	7
2.1.4	Interfaces and tools	7
2.1.5	General identification process	7
2.1.6	Evidence management	7
2.1.7	Accepted identity documents and attributes collected	8
2.1.8	Processing of biometric data and use of AI	8
3	DESCRIPTION OF IDENTIFICATION METHODS	8
3.1	Identification methods with LoA High — LoIP Extended	8
3.1.1	DVO+ — Hybrid attended video identification	8
3.1.2	RAIP and S-RAIP – automated and hybrid unattended identification	11
3.1.3	Identification using CieID	15
3.1.4	Identification using TS-CNS	17
3.1.5	Identification using a qualified electronic signature	19
3.2	Other supported identification methods	21
3.2.1	DVO — Attended video identification	21
3.2.2	Identification using SPID Level 2 credentials	23
4	SECURITY MEASURES	26
4.1	Main reference standards	26
4.1.1	ISO/IEC 27001 and ISO/IEC 27002	26
4.1.2	ISO 27005	26
4.2	Framework adopted for Information Security management	27
4.2.1	GOVERN	28
4.2.2	IDENTIFY	28
4.2.3	PROTECT	28
4.2.4	DETECT	28
4.2.5	RESPOND	28
4.2.6	RECOVER	28
	APPENDIX 1 – OUTSOURCED TECHNOLOGIES	29

1 INTRODUCTION AND ADMINISTRATION

1.1 Overview

Aruba PEC S.p.A. (Aruba PEC) makes the IDS platform and its technological components available to its Customers for carrying out the identification processes described in this document.

The identity proofing processes managed through IDS are used by the Customer for its own purposes, depending on the identification method used and the applicable legislation, including the provision of the Customer's trust services, the activation of digital services and other purposes provided for under national, European or sector-specific legislation.

This document describes the IDS platform and the identification processes it supports, hereinafter also referred to as "Identity Proofing Services", made available to the Customer on a stand-alone basis. In this context, Aruba PEC acts exclusively as the provider of the technological solution used by the Customer for its own identification purposes.

References to Regulation (EU) No 910/2014 — eIDAS, as currently in force, and to ETSI TS 119 461 v. 2.1.1 — Policy and security requirements for trust service components providing identity proofing of trust service subject concern the characteristics of the processes described and the context in which they are used by the Customer.

1.2 Document administration

1.2.1 Document version and responsible organisation

The version of this document is indicated on the first page. The document has been prepared, published and updated by Aruba PEC S.p.A.

The organisation's details are as follows:

Item	Description
Organisation	Aruba PEC S.p.A.
Registered office	Via San Clemente n. 53 – 24036 Ponte San Pietro (BG)
VAT number	01879020517
REA registration number	BG - 445886
Website	www.aruba.it

1.2.2 Parties responsible for approval

Before its adoption, this document is reviewed and validated internally by the corporate units responsible for regulatory compliance and legal matters, as well as by the departments responsible for the operational management of the service.

1.3 Definitions

Term	Definition
APCER	<i>Attack Presentation Classification Error Rate. For further details, please refer to ETSI TS 119 461.</i>
Applicant	The natural person undergoing identification for the Customer's purposes through the means made available by Aruba PEC. The Applicant may represent a legal person.
Authoritative evidence	Evidence attesting to certain attributes of the Applicant, managed by an authoritative source.
Authoritative source	Any source, regardless of its form, that can be relied upon to provide accurate data, information and/or evidence that may be used to demonstrate the Applicant's attributes.
Binding to Applicant	The part of the identification process that verifies that the Applicant is the natural person identified by the document presented during the identification process. It also verifies that the identity document presented is authentic and has not been cloned or copied, preventing spoofing attacks involving printed documents, high-resolution digital images, cloned chips, etc.
BPCER	<i>Bonafide Presentation Classification Error Rate. For further details, please refer to ETSI TS 119 461.</i>
Customer	The legal person that is a customer of Aruba PEC and uses the IDS platform and identification processes for its own purposes.
DVO	Acronym standing for "De Visu Online", referring to a specific identification process in which an operator connects remotely with the Applicant.
Digital identity document	An identity document issued in machine-processable format, digitally signed by the Issuing Authority and in purely digital form. A digital identity document may be embedded in a physical identity document, such as an identity card or passport.
Electronic identification means	A material and/or immaterial unit containing person identification data and used for authentication for an online service.
Extended LoIP	A Level of Identity Proofing (<i>LoIP</i>) achieving a high degree of reliability, based on compliance with minimum good-practice requirements for the identification process. This level is considered suitable for identification for the purposes of issuing qualified certificates and qualified electronic attestations of attributes under the eIDAS Regulation. For further information, please also refer to ETSI TS 119 461.

Identification session	An individual identification session in which the Applicant is asked to perform certain activities to provide and validate their identity.
Identity document	A physical or digital document issued by an authoritative source and attesting to Applicant's identity.
Identity proofing context	External requirements affecting the identity proofing process as a result of the purposes of identity proofing, the related regulatory requirements and the resulting restrictions on the collection of attributes and evidence, as well as on the identity proofing process itself.
Identity proofing process	The process of verifying an Applicant's identity using evidence attesting to the required identity attributes.
Physical identity document	An identity document issued in physical, human-readable form.
IDS	Acronym standing for "IDentification Service", the platform used to manage and orchestrate the identity proofing processes described in this document.
Liveness detection	A technique for measuring and analysing biometric anatomical characteristics and voluntary or involuntary reactions to determine whether a biometric sample is being acquired from a real person present at the time of the identification process.
NFC	Near Field Communication — a short-range wireless communication technology that enables data exchange between devices in close proximity.
Proof of access	Any source, regardless of its form, considered reliable for collecting data, information and/or evidence that may be used in an identity proofing process, provided that the Applicant is able to demonstrate access to that source.
Trusted Register	A public register or database, or another type of reliable source for the transmission of identity attributes within the Applicant's identity proofing context.
Validation	The part of the Applicant's identity proofing process that determines whether the attributes are corroborated by the evidence obtained, by verifying its authenticity, validity and reliability.
Unattended automated identification component	A specific component implemented in Aruba PEC applications that enables the Applicant to undergo identification through biometric recognition and artificial intelligence techniques, as well as through NFC reading of an identity document held by the Applicant.

2 IDS PLATFORM

2.1 DS Platform — Introduction

IDS — Identification Service is a multi-tenant SaaS platform designed to integrate the identification of natural persons into application workflows. Integration primarily takes place through APIs exposed via an API Management Platform. The end-Applicant experience may be provided through the IDS white-label front end or, for compatible methods, through a front end developed by the Customer and integrated via APIs.

The processes managed by IDS differ according to the method of interaction with the Applicant, with whom the Customer has a direct relationship, the degree of automation, the nature of the authoritative evidence used and the presence or absence of human supervision. The platform orchestrates the lifecycle of the identification case and integrates its own services and external providers, maintaining the link between the initial data, execution of the method, consistency checks, outcome and evidence.

2.1.1 Actors and operational responsibilities

Customer / System Integrator	Integrates IDS into its systems, creates the case, specifies the data and permitted methods, receives notifications and the outcome, and retrieves the evidence according to the agreed configuration.
Applicant	The natural person undergoing the identification process through one of the enabled methods.
Operators	Manage the platform and tenants; perform DVO identification and, where configured, manually review cases and evidence.
IDS Platform	Orchestrates initiation, execution, status, consistency checks, evidence generation and association, and notifications.
External providers	Provide the identification components or methods integrated by IDS.

2.1.2 Architecture and configuration

The platform is configured according to a multi-tenant model. Graphical elements, dedicated URLs, available methods and optional workflow stages may be defined for each tenant.

Retention may differ by method, with more restrictive criteria for processes involving biometric data.

The platform's main features can be summarised as follows:

- Customisation of logos, colours, labels and interface text.
- Selective enablement of identification methods.
- Configuration of optional steps and operational timeframes.
- Differentiated retention rules at tenant and method level.

2.1.3 Application integration, APIs and interfaces

Cases are created through APIs, which enable case creation, status consultation, evidence retrieval, cancellation and, to the extent permitted by the case status, case updates.

Events are notified to the Customer/System Integrator through webhooks sent to configured endpoints. The API Management Platform provides a catalogue, technical documentation, subscriptions, application and credential management, testing and technical analytics.

A web and mobile SDK, for iOS and Android, is available for specific categories of processes — currently RAIP and S-RAIP, as described in the next chapter — enabling the Customer to develop the interface while retaining the IDS platform as the orchestration backend. The web workflow does not support NFC functionality.

2.1.4 Interfaces and tools

Interfaccia	Attori	Funzione principale
Developer Portal	Customer / System Integrator	API catalogue and documentation, subscriptions, applications/credentials and analytics.
IDS Front-end	Applicant	Selection of the method and completion of identification.
IDS Backoffice	Operators	Tenants, workflows, timeframes and case monitoring.
Validation Panel	Operators	Performance of de visu processes, DVO identification, S-RAIP review and decisions on cases.

2.1.5 General identification process

The standard lifecycle, common to all currently available identification methods, consists of the following stages, structured consistently with the ETSI TS 119-461 model:

- **Initiation of the identification process:** the Applicant receives preliminary information on the identification process they are required to undergo.
- **Data collection:** the Applicant provides the attributes and evidence required for identification.
- **Validation:** the prescribed checks are performed on data, documents, certificates, electronic evidence or biometric evidence.
- **Binding to Applicant:** the validated evidence is bound to the Applicant using the means provided for each identification method, as described in the next chapter.
- **Issuance of the identification result:** the outcome confirming identification is produced, together with the additional evidence obtained during the process.

IDS can also perform consistency checks between the data received from the Applicant during registration and the data obtained through the specific method.

2.1.6 Evidence management

The evidence generated during the identification process is managed by IDS in accordance with the arrangements applicable to the process and the service configuration agreed with the Customer.

2.1.7 Accepted identity documents and attributes collected

Accepted identity documents and attributes to be collected are determined according to the characteristics of the specific process, the Customer's related purposes and the technical requirements of the identification methods used.

2.1.8 Processing of biometric data and use of AI

Certain types of identification processes described in the next chapter — DVO+, RAIP and S-RAIP — use artificial intelligence systems. Applicants' personal data are not used to train the corresponding models.

Biometric data are processed exclusively for identification checks and deleted once their use has been completed, without being retained thereafter.

3 DESCRIPTION OF IDENTIFICATION METHODS

The processes described in the following sections are classified according to the reliability of the identification process, the level of assurance associated with the evidence or identification means used, and the applicable regulatory context.

The processes described are used for the Customer's purposes, which may include the provision of its own trust services or purposes other than certification.

For the provision of the Customer's qualified and non-qualified trust services, the identification methods described in this document may be used in compliance with the applicable legislation and according to the level of assurance or security required for the specific service.

Baseline/Substantial denotes a significant degree of reliability in identification. Extended/High entails stricter requirements and checks designed to ensure the highest degree of reliability and protection against identity fraud, in accordance with the respective eIDAS and ETSI 119-461 reference frameworks.

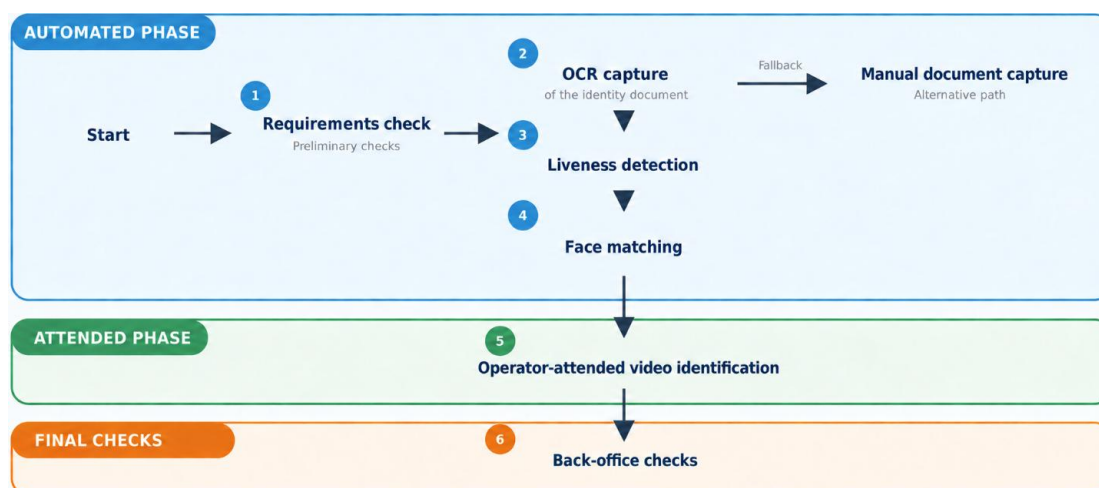
3.1 Identification methods with LoA High — LoIP Extended

3.1.1 DVO+ — Hybrid attended video identification

DVO+ is a remote "de visu" identification process based on a live video session with an operator, preceded by an unattended preliminary stage in which automated checks on the collected evidence support the operator and strengthen the process.

Method	Remote attended, with an automated preliminary stage and biometric checks (ETSI 119-461, C.3.4)
Declared level	Extended (High)
Specific checks	OCR, document validation, liveness detection, anti-spoofing checks, face matching, operator; optional back-office review

The end-to-end workflow may be summarised as shown in the following diagram.



The Applicant is guided through a process providing an operator-attended identification experience, consisting of the following stages.

Initialisation

Preliminary verification of prerequisites: verification of the technical requirements of the device and Internet connection, to ensure that the identification session provides high-quality evidence acquisition and appropriate levels of cybersecurity.

Collection of data and evidence; pre-validation of the identity document

OCR capture of the identity document:

- The Applicant captures images of the identity document through the guided interface made available by Aruba.
- The OCR component automatically extracts the data contained in the Visual Inspection Zone (VIZ) and, where available, the Machine Readable Zone (MRZ).
- Depending on the document, the data collected include personal details, tax identification number, nationality, residence, document details, validity and place or country of issue. In the Italian context, collection of the health card is not necessary where the Applicant uses their electronic identity card.

- The system performs preliminary validation of the collected data and evidence, verifying their authenticity and validity.

Preliminary Binding to Applicant

Liveness detection: the system verifies that identification is being performed by a real person and does not constitute an attempt at manipulation or falsification using techniques such as photo morphing, deepfakes, masks or similar means.

- The service assists the individual in capturing their facial image, providing real-time instructions to ensure correct facial positioning and suitable lighting conditions and image quality.
- During capture, the system detects and analyses the face in real time for the subsequent biometric checks.

Face matching: the system automatically compares the Applicant's face with the face shown in the identity document, supporting the operator in the subsequent stages of the process.

Final validation of data and evidence; final Binding to Applicant

Video session with a video identification operator: the operator conducts video identification in accordance with a dedicated procedure and an internal checklist.

- **Back-office checks**, where applicable depending on the process configuration: an operator reviews all the evidence collected and the identification process as a whole, in accordance with strict internal procedures and with the support of scores generated through automated checks.
 - Acceptance or rejection of the video identification session: based on the results of the back-office checks, the operator decides whether to approve or reject the session.

Issuance of the proof of evidence

Following successful completion of identification, an evidence package is generated, comprising:

- The audio-video recording.
- Images of the identity documents.
- Images captured during liveness detection.
- The audit trail containing the results of the checks performed. The audit trail also includes the cryptographic hashes of the individual files produced.

The documentation is encrypted using a public key generated by Aruba.

3.1.2 RAIP and S-RAIP – automated and hybrid unattended identification

Aruba PEC makes two methods of automated remote identity proofing available: Remote Automatic Identity Proofing (RAIP), which is fully automated, and Supervised Remote Automatic Identity Proofing (S-RAIP), which incorporates human supervision at specific stages of the process.

Both identification methods may be used for the provision of the Customer's trust services, including qualified trust services, and comprise the following stages: initialisation, collection of data and evidence, validation, Binding to Applicant, and issuance of the result confirming identification.

The differences between the two processes concern three main elements:

	RAIP	S-RAIP
Method	Fully automated	Automated with human supervision
Human intervention	Not envisaged	Limited to validation and Binding to Applicant
Additional evidence	Results of automated checks	Outcome of supervision

Aruba PEC defines and maintains target performance levels for the *False Acceptance Rate* (FAR) and *False Rejection Rate* (FRR), in line with industry best practices. Aruba PEC also defines and maintains target performance levels for PAD metrics, with reference to PAD scenarios from Level 1 to Level 3 and Level 5 (injection).

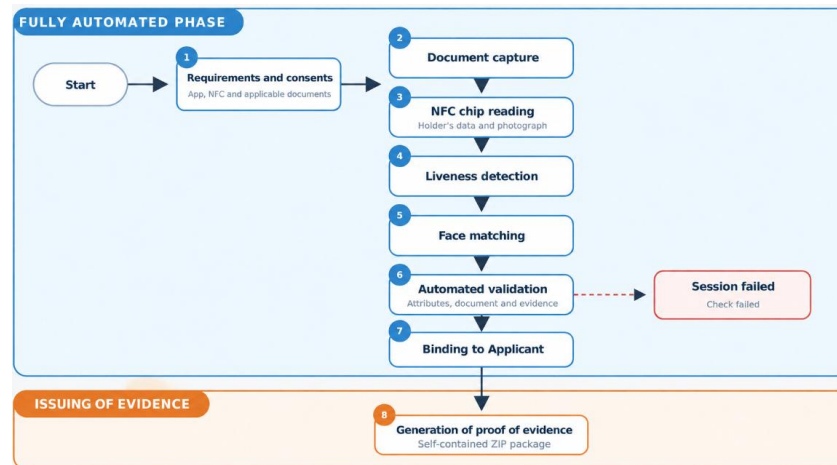
The Injection Attack Detection system used by Aruba has passed an assessment equivalent to the High level under CEN/TS 18099. It has also been evaluated in accordance with ISO/IEC 19795-1 and 19795-2 over more than one million comparisons, achieving an FMR of 0.005%, an FNMR of 2.21% and an FTA of 0%.

All these parameters are subject to continuous monitoring and periodic review to ensure ongoing compliance with the applicable standards and alignment with industry best practices.

3.1.2.1 RAIP - Remote Automatic Identity Proofing

Method	Remote unattended, with automated operations (ETSI 119-461, C.3.4)
Level	Extended (High)
Checks	NFC, document validation, liveness detection, anti-spoofing checks, face matching

The end-to-end workflow can be summarised as shown in the following diagram:



Initialisation

Before the process starts, the Applicant is shown the content agreed with the Customer according to the identification purposes determined by the latter.

The process requires an NFC-enabled smartphone and a document compliant with ICAO 9303, selected from those accepted by Aruba PEC in the operational manual dedicated to the specific process, entitled “MODAP_A_31_SPS”. As at the date of this document, the Italian Electronic Identity Card and Italian electronic passport may be used.

Collection of attributes and evidence

The process guides the Applicant through the acquisition of the necessary evidence and collects:

- Images of the front and back of the document.
- The data and user’s photograph stored in the document’s chip.
- Session identification and time-related metadata.
- Any alerts generated by the checks.

Once transmission to Aruba’s systems has been completed, identification-related data are deleted from the mobile device. Any errors in the collection or transfer of evidence cause the session to fail.

For representatives of legal persons, additional attributes can be obtained by querying trusted registers. Where the information is unavailable, the Applicant may be invited to provide documents or attestations demonstrating their powers of representation.

Validation

Aruba’s systems verify that the document is among those accepted and check its authenticity and validity. Data obtained through NFC reading are compared with the data declared by the Applicant. The validity of the electronic

signature applied by the Issuing Authority to the digital document is also verified. Where diacritical characters are present, the comparison is carried out by applying the transliteration rules set out in ICAO 9303.

Binding to Applicant

The automated component also performs:

- **Liveness detection**, to verify that the biometric sample originates from a real person present during the session. Images of the Applicant's face are captured at this stage.
- **Face matching**, by comparing the Applicant's face with the photograph stored in the chip and the photograph shown on the physical document.

Any discrepancies, detection of potential attacks or failure to meet the prescribed reliability thresholds result in an unsuccessful session. Checks and decisions are processed in Aruba's Data Centres, rather than in the app installed on the Applicant's device.

Issuance of the proof of evidence

The collected and validated evidence is bound to the Applicant through the generation of a unique, self-contained proof of evidence, consisting of a ZIP package. The package includes at least:

- Images of the face captured during liveness detection.
- The photograph extracted from the document's chip.
- Images of the identity document.
- Data obtained through NFC reading.
- Session metadata, including the identifier, date, time and duration.
- The overall session report and the results of the individual checks.

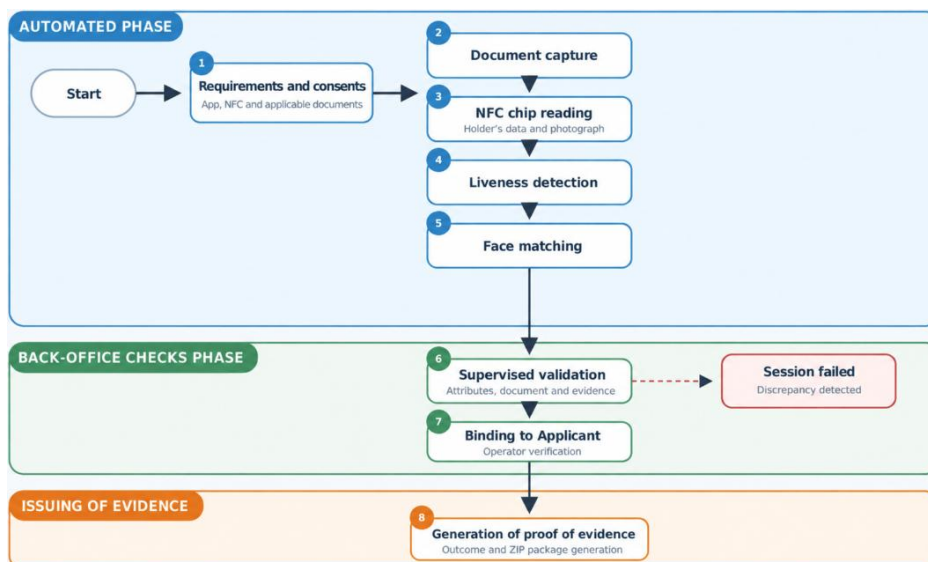
For representatives of legal persons, evidence concerning the legal person and the powers of representation is also included.

3.1.2.2 S-RAIP - Supervised Remote Automatic Identity Proofing

S-RAIP uses the same initialisation, data acquisition and evidence collection methods as RAIP.

Method	Hybrid remote unattended, with manual and automated operations (ETSI 119-461, C.3.4)
Level	Extended (High)
Checks	NFC, document validation, liveness detection, anti-spoofing checks, face matching; back-office review

The end-to-end workflow may be summarised as shown in the following diagram:



Initialisation and evidence collection

As in the RAIP process described above, the Applicant uses an NFC-enabled device and one of the ICAO 9303-compliant documents accepted by Aruba PEC in the operational manual dedicated to the specific process, entitled "MODAP_A_31_SPS".

Before the process starts, the Applicant is shown the content agreed with the Customer according to the identification purposes determined by the latter.

Automated preliminary validation

Aruba's systems verify that the document is among those accepted and check its authenticity and validity. Data obtained through NFC reading are compared with the data declared by the Applicant. The validity of the electronic signature applied by the Issuing Authority to the digital document is also verified. Where diacritical characters are present, the comparison is carried out by applying the transliteration rules set out in ICAO 9303.

Associazione dell'evidenza al Richiedente

The automated component also performs:

- **Liveness detection**, to verify that the biometric sample originates from a real person present during the session. Images of the Applicant's face are captured at this stage.
- **Face matching**, by comparing the Applicant's face with the photograph stored in the chip and the photograph shown on the physical document.

Any discrepancies, detection of potential attacks or failure to meet the prescribed reliability thresholds result in an unsuccessful session. Checks and decisions are processed in Aruba's Data Centers, rather than in the app installed on the Applicant's device.

Final validation of data and evidence; final Binding to Applicant

The evidence and check results are subsequently reviewed by a back-office operator. The Operator performs the checks in accordance with internal procedures and using dedicated IT tools that allow documents to be examined, facial images to be compared and relevant details to be enlarged.

Supervision is limited to evidence validation and correct Binding to Applicant. Initialisation, data collection and production of the evidence package remain automated. Any discrepancy or inconsistency detected by the operator results in rejection of the session.

For representatives of legal persons, supervision may also include examination of the attributes obtained from trusted registers and the documentation provided to demonstrate powers of representation.

Issuance of the proof of evidence

S-RAIP produces an evidence package in .zip format containing the same evidence as RAIP, as described in the preceding subsection.

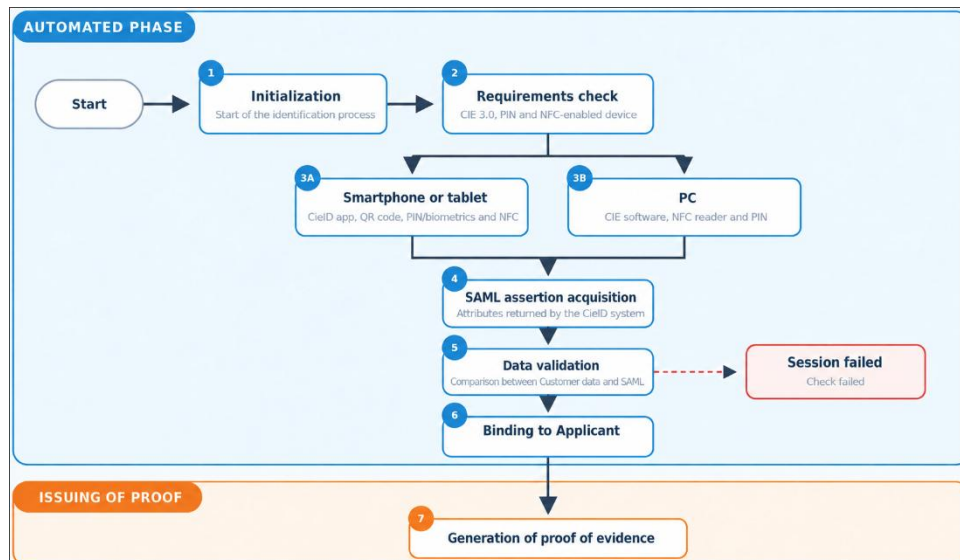
The outcome of the operator's activities and the corresponding logs are managed in accordance with the arrangements applicable to the process and the service configuration.

3.1.3 Identification using CielD

The process enables remote verification of the Applicant's identity through authentication using the Electronic Identity Card. The CIE is an electronic identification means notified under the eIDAS Regulation with a High level of assurance. The process does not require operator intervention.

Method	Identification using a notified Level 3 digital identity scheme (ETSI 119-461, C.3.2)
Level	Extended (High)
Checks	Verification of evidence of successful authentication

The end-to-end workflow may be summarised as shown in the following diagram:



Inizializzazione

Before authentication, IDS checks or communicates the availability of the necessary prerequisites:

- A valid and active CIE version 3.0.
- The Electronic Identity Card PIN.
- An NFC-enabled smartphone or tablet with the CieID app installed and configured by the Applicant; or
- A computer equipped with CIE software and an NFC/RFID contactless reader.

Collection of data and evidence

Authentication may be performed through two alternative paths.

When using a smartphone or tablet, the Applicant enters the CIE serial number, opens the CieID app and scans the displayed QR code. Authentication continues by entering the last four digits of the PIN or, where previously configured in the app, by using the biometric system available on the device. The Applicant then places the CIE close to the NFC sensor and completes the indicated steps, including generation of the code required by the interface.

When using a computer, the Applicant installs and configures the CIE software, connects the contactless reader, places the Card close to the device and enters the last four digits of the PIN.

Following authentication, the CieID system returns a SAML assertion containing the Applicant's identification attributes. Accordingly, the process does not involve Aruba independently collecting images of the document or biometric samples intended for facial recognition.

Validation of data and evidence

IDS checks consistency between the registration data transmitted by the calling system and the attributes contained in the SAML assertion returned by the CielD system. The set of attributes to be checked depends on the process and the specifications agreed with the Customer.

The process may proceed only if CielD authentication is successfully completed and the acquired data are consistent with those associated with the service request.

Binding to Applicant

Where the outcome is positive, the SAML assertion and the validated attributes are bound to the Applicant and the corresponding request. This binding uniquely links the identity attested by the CielD system to the previously collected data.

Emissione della proof of evidence

Identification evidence is generated in a format suitable for preservation, together with the CielD SAML assertion and the additional elements provided for by the service.

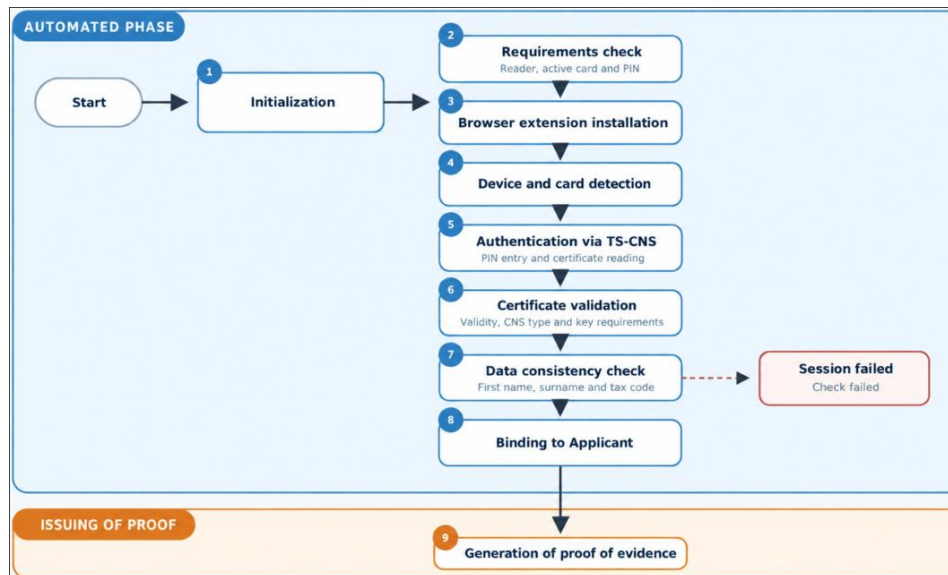
The evidence is managed by IDS in accordance with the arrangements applicable to the process and the service configuration agreed with the Customer.

3.1.4 Identification using TS-CNS

The process enables automated identification of the Applicant through the authentication certificate contained in a Health Card with active CNS functionality or in a National Services Card.

Method	Identification using a notified Level 3 digital identity scheme (ETSI 119-461, no specific use case)
Level	Extended (High)
Checks	Verification of the CNS certificate and credentials

The end-to-end workflow can be summarised as shown in the following diagram:



Initialisation

The Applicant selects the TS-CNS method on the IDS platform and starts the process.

Preliminary activities, notices and any acceptances are defined according to Customer's service and the agreed integration arrangements.

The system informs the Applicant of the necessary prerequisites:

- A smart card reader connected to the computer.
- An active TS-CNS or CNS.
- The PIN associated with the card.
- The browser extension required to interact with the device.

Collection of data and evidence

Where necessary, the Applicant installs the required browser extension. The system detects the reader and the inserted card, then prompts the Applicant to enter the PIN.

Following authentication, IDS obtains from the CNS certificate the holder's identification data required for the process. The data set depends on the process and the specifications agreed with the Customer. The PIN is used exclusively to enable the operation on the card and is not an item of identification data collected by IDS.

Data and evidence validation

IDS automatically verifies:

- That the certificate is valid and has not expired.
- That the certificate is associated with a CNS card.
- That the cryptographic key meets the technical requirements laid down by the applicable legislation.
- That the identification attributes extracted from the certificate are consistent with the data received from the calling system.

Identification is completed only if all checks are successful. The absence of the device, entry of an invalid PIN, an unsuitable certificate or a data mismatch prevents completion of the session.

Binding to Applicant

The data extracted from the certificate and the check results are bound to the Applicant and the corresponding request. Matching the first name, surname and tax identification number links the identity attested by the TS-CNS or CNS to the data already held in the calling system.

Issuance of the proof of evidence

Identification evidence is managed by IDS in accordance with the arrangements applicable to the process and the service configuration agreed with the Customer.

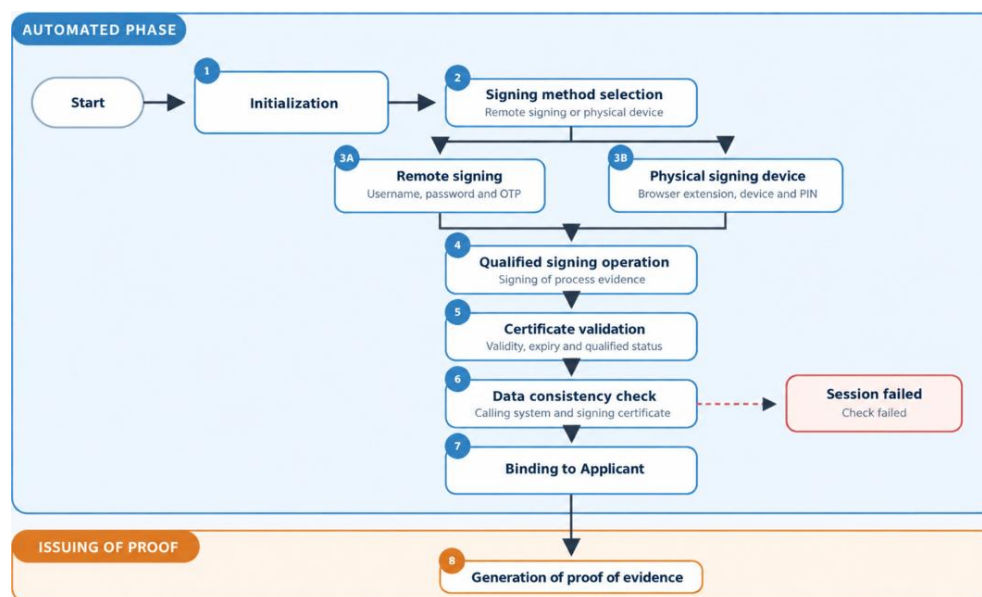
3.1.5 Identification using a qualified electronic signature

The process enables identification of the Applicant through a qualified electronic signature certificate issued by a qualified trust service provider. The method is based on the association between the holder and the certificate used to sign the evidence required by the process.

The process may be completed using either a remote qualified electronic signature or a local qualified electronic signature installed on a physical device, such as a smart card or cryptographic token.

Method	Identification using a notified Level 3 digital identity scheme (ETSI 119-461, C.3.3)
Level	Extended (High)
Checks	Verification of the certificate and correct execution of the signature

The end-to-end workflow may be summarised as shown in the following diagram:



Initialisation

The system presents the necessary prerequisites according to the selected path.

Remote signature. The Applicant uses the signing service credentials — username and password — and the OTP generated through one of the enabled channels. IDS obtains the certificate associated with the signature and the identification data contained in it.

Local signature. The Applicant has a local qualified electronic signature installed on a physical device connected to the computer and the corresponding PIN. Where necessary, the Applicant installs the required browser extension. The system then detects the device and enables the signing operation.

Under both paths, the Applicant signs the document or evidence required by the process using a qualified electronic signature.

Validation of data and evidence

IDS automatically verifies:

- The certificate's validity and expiry.
- The qualified status of the certificate and signature.
- Correct execution of the signing operation.
- Consistency between the data received from the calling system and the data contained in the certificate. The set of attributes to be checked depends on the process and the specifications agreed with the Customer.

Identification is successfully completed only if all the prescribed technical and consistency checks on the Applicant's certificate are passed. Otherwise, the session ends with a negative outcome.

Binding to Apploicant

The data extracted from the certificate, the signed document and the verification results are uniquely bound to the Applicant and the corresponding request. Matching the identification data uniquely links the identity attested by the certificate to the information received from the calling system.

Issuance of the proof of evidence

The outcome and generated evidence are made available to the Customer in accordance with the agreed integration arrangements. Any signed document is the document defined by the Customer for its service. Preservation is managed by the Customer or through the service selected by the Customer, unless use of Aruba's preservation service is contractually provided for. Any communication to the Applicant and activation of the service are managed by the Customer, where applicable.

3.2 Other supported identification methods

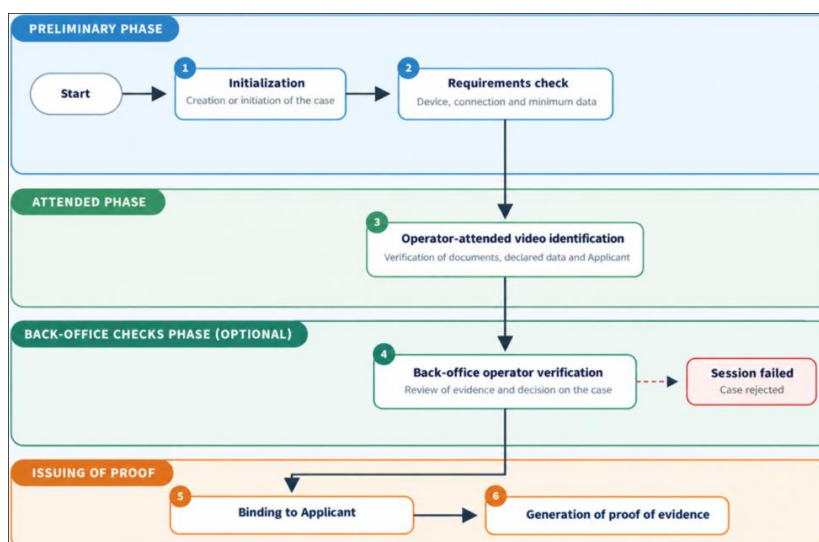
3.2.1 DVO — Attended video identification

DVO is an attended remote identification method based on a live video session between the Applicant and an identification operator. The process is implemented to meet the Substantial level of assurance and may also be used through IDS as a stand-alone identity proofing service, independent of the issuance of certificates or provision of other trust services.

Unlike DVO+, DVO does not include a preliminary stage consisting of OCR capture of the document, liveness detection and face matching. Identity verification is primarily performed by the operator during the video session with the Applicant.

Method	Remote attended
Checks	Manual verification of the Applicant's identity and document

The end-to-end workflow may be summarised as shown in the following diagram:



Initialisation

The Customer creates the case through APIs, transmitting the Applicant's identification data to IDS.

Before the session starts, the technical requirements of the device and Internet connection are checked, and the minimum data necessary to manage the case are collected.

Collection of data and evidence

The Applicant joins the live video session with an operator and presents the required identity document. During the session, the data declared by the Applicant and the evidence required by the internal video identification procedure are collected.

At this stage, all evidence presented by the Applicant is assembled into a complete set. The session is also recorded in full and documented through images, metadata and application logs.

Validation of data and evidence

The operator conducts video identification by applying a dedicated procedure. In particular, the following may be checked:

- The correspondence between the Applicant connected to the session and the document presented.
- Consistency between the declared data and the data shown on the document.
- The legibility, validity and apparent integrity of the document.
- The Applicant's behaviour and interactions during the session.
- Correct completion of the activities required by the procedure.

IDS may also perform consistency checks between the data previously provided by the Customer and/or the Applicant and the data collected during identification. Such checks typically concern the first name, surname and tax identification number and may be configured according to the Customer's requirements.

A subsequent back-office checking stage may be provided for. Where configured, a second operator reviews the session evidence, applies the internal checks and approves or rejects the case, recording the reasons for the decision. In the absence of supervision, the outcome derives from the session conducted by the operator.

Binding to Applicant

IDS associates the collected data, session evidence, video identification outcome and, where applicable, the back-office operator's decision with the Applicant's case.

The association is made using the case references and the identification data transmitted by the Customer, ensuring that the outcome can be traced to the specific Applicant.

Issuance of the proof of evidence

Upon conclusion of the identity proofing process, a result confirming identification is issued.

Following successful completion of identification, an evidence package is generated, comprising:

- The video recording.
- Images of the identity documents.
- The audit trail containing the results of the checks performed. The audit trail also includes the cryptographic hashes of the individual files produced.

The generated documentation is protected by Aruba's systems using secure cryptographic techniques.

At the end of the process, IDS generates a positive or negative outcome and updates the case status. The Customer receives notification of the outcome through a webhook and may consult the status and retrieve the evidence through the available APIs.

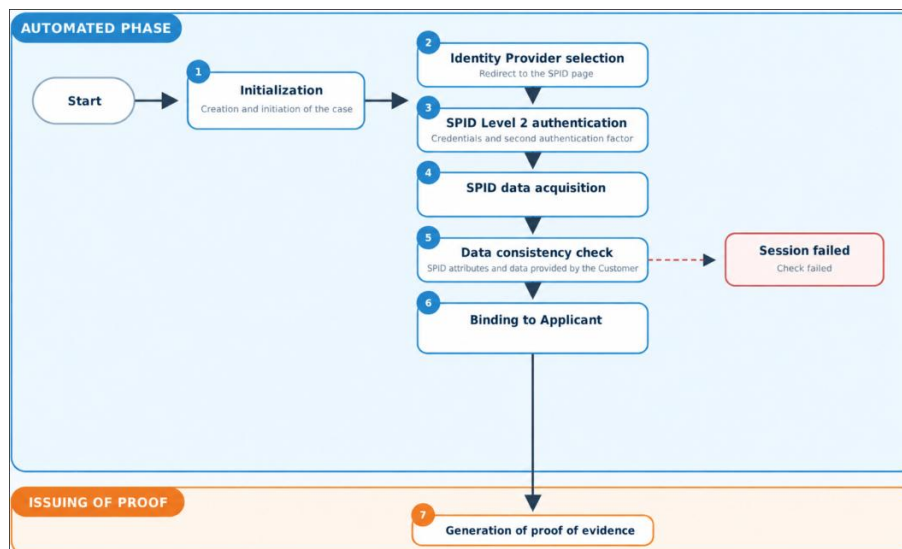
The evidence is made available to the Customer and managed in accordance with the arrangements provided for by the service configuration and the applicable contractual agreements, including with regard to any preservation of that evidence.

3.2.2 Identification using SPID Level 2 credentials

SPID is an automated identification method based on authentication using a Level 2 SPID identity, designed to achieve a "substantial" security level. The method is intended for users who hold a SPID identity and enables IDS to use the attributes returned by the Identity Provider as the basis for identification.

Method	Identification using a notified Level 2 digital identity scheme
Checks	Verification of evidence of successful authentication

The end-to-end workflow may be summarised as shown in the following diagram:



Initialisation

The Customer creates the case through APIs, transmitting to IDS the data of the person to be identified and specifying SPID among the permitted methods.

The Applicant is directed to the IDS front end or to the interface developed by the Customer and integrated with IDS, where the Applicant starts the identification process.

Collection of data and evidence

The Applicant is redirected to the SPID authentication page and selects their Identity Provider.

Authentication is performed using SPID Level 2, through the credentials issued by the Identity Provider and a second authentication factor, such as an OTP generated by the IdP's application.

Following authentication, IDS obtains the identification attributes returned by the Identity Provider.

Validation of data and evidence

IDS verifies successful completion of authentication and, where applicable, compares the SPID attributes with the data communicated by the Customer when creating the case.

Where present, consistency checks typically concern the first name, surname and tax identification number. The Customer may configure the checks to be applied according to its operational requirements.

The case may proceed only if authentication is successfully completed and the compared data are consistent. Otherwise, the process ends with a negative outcome.

Binding to Applicant

The SPID attributes, authentication outcome and generated technical evidence are associated with the case and bound to the Applicant through the corresponding identifiers.

Issuance of the proof of evidence

At the end of the process, IDS generates the identification outcome and updates the case status. The Customer is informed through a webhook and may consult the status and retrieve the evidence through the platform's APIs.

The evidence is made available to the Customer and managed in accordance with the arrangements provided for by the service configuration and the applicable contractual agreements, including with regard to any preservation of that evidence.

Following download or submission for preservation, the data held in IDS are deleted in accordance with the configured data retention policies.

4 SECURITY MEASURES

Aruba PEC uses trustworthy systems and applies security measures based on recognised European and international standards and best practices. Its Information Security Management System (ISMS) is compliant with and certified according to ISO/IEC 27001.

The main standards and frameworks adopted for the management of information security are described below.

4.1 Main reference standards

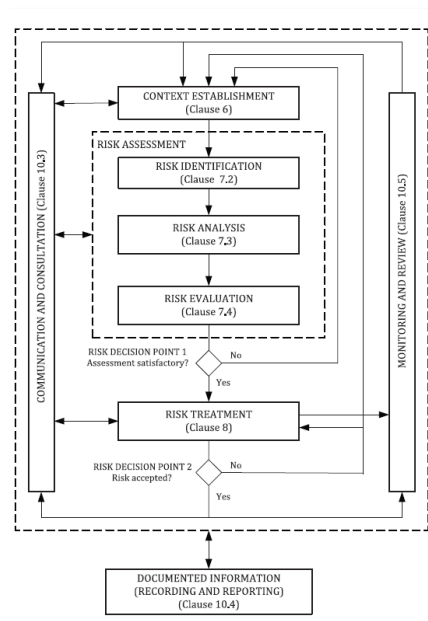
4.1.1 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 defines the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS), supporting the identification and management of risks affecting the confidentiality, integrity and availability of information.

ISO/IEC 27002 provides guidance on the implementation of information security controls, covering organisational, procedural and technological aspects. These controls support, but do not replace, the organisation's risk assessment and risk treatment activities.

4.1.2 ISO 27005

ISO/IEC 27005 provides guidance on information security risk management in support of the principles and requirements set out in ISO/IEC 27001 and consistently with the general risk management approach defined by ISO 31000.



ISO/IEC 27005: Information Security Risk Management Process

4.2 Framework adopted for Information Security management

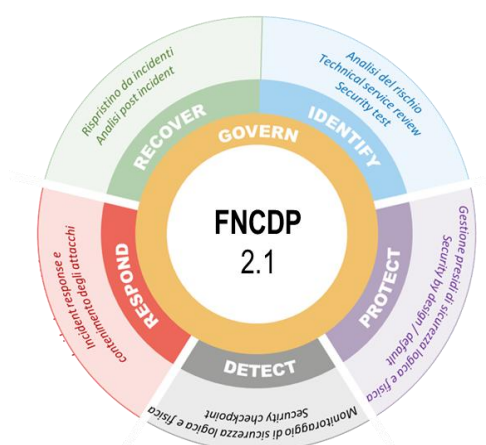
Information Security for the **Identification Platform** is managed in accordance with the National Framework for Cybersecurity and Data Protection (FNCDP) — 2025 Edition, v2.1, developed by the CIS Research Centre at Sapienza University of Rome and the CINI National Cybersecurity Laboratory, with the support of the National Cybersecurity Agency (ACN).

The Framework supports the management of cybersecurity and data protection risks by integrating organisational, procedural, technological and regulatory aspects. It is used to support risk management, the definition and monitoring of security measures and the continuous improvement of the security posture of the Identification Platform.

The Framework is structured around six Functions:

- **Govern (GV):** definition of cybersecurity strategies, policies, roles, responsibilities and risk governance processes.
- **Identify (ID):** identification of assets, processes, dependencies and relevant cybersecurity risks.
- **Protect (PR):** implementation of organisational, physical and technical safeguards to protect information and services.
- **Detect (DE):** monitoring and timely identification of anomalous events, vulnerabilities and security incidents.
- **Respond (RS):** management, containment and mitigation of cybersecurity incidents, including the related communication activities.
- **Recover (RC):** restoration of services and operational capabilities and implementation of measures aimed at improving resilience.

The adoption of the Framework supports a structured approach to cybersecurity, operational resilience, service continuity and compliance with applicable requirements.



Framework adopted for the proper management of Information Security

Details of each function are provided below.

4.2.1 GOVERN

The GOVERN function establishes the governance framework for cybersecurity and IT risk management, including strategies, policies, roles, responsibilities and continuous improvement activities.

4.2.2 IDENTIFY

The IDENTIFY function supports the identification of information assets, infrastructure, processes, dependencies and risks relevant to the Identification Platform, enabling appropriate protection priorities and risk treatment measures to be defined.

4.2.3 PROTECT

The PROTECT function covers the organisational, physical and logical measures adopted to safeguard information and services, including access management, data protection, staff awareness and technical security controls.

4.2.4 DETECT

The DETECT function covers monitoring and detection activities aimed at promptly identifying anomalous events, vulnerabilities and security incidents affecting the Identification Platform.

4.2.5 RESPOND

The RESPOND function covers the activities required to manage, analyse, contain and mitigate cybersecurity incidents and their impact on the Identification Platform.

4.2.6 RECOVER

The RECOVER function covers the activities required to restore services and operational capabilities following a security incident and to improve organisational and technological resilience.

Further details on security measures are provided in the Policy Statement applicable to the services provided by Aruba PEC.

APPENDIX 1 – OUTSOURCED TECHNOLOGIES

For certain process-related components, Aruba PEC relies on technologies supplied by the following providers:

- **FACETEC, INC.**

Available at: <https://www.facetec.com/>.

FaceTec supplies the biometric components used by Aruba PEC on-premises within automated remote identification processes, including facial recognition, biometric comparison and liveness detection functionalities. These are intended to verify that the Applicant matches the identity document and is actually present during the process.

FaceTec technology has undergone independent testing and assessment with reference, among others, to ISO/IEC 30107-3 for Presentation Attack Detection and ISO/IEC 19795-2 for biometric system performance. The corresponding reports, tests and certifications are available at:

<https://dev.facetec.com/studies-reports-tests-certifications>.

- **TOCTOC S.r.l.**

Available at: <https://www.toctoc.me>.

TocToc supplies a technology platform used by Aruba PEC on a SaaS basis to carry out remote identification processes, both in operator-supervised and automated modes. The platform supports the collection and verification of the Applicant's documents and information, performance of the prescribed checks, and production of evidence relating to the identification process. The provider's data centres are located in the EU.

TocToc's Identity Proofing processes comply with ETSI TS 119 461. TocToc has also obtained ISO 9001, ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 certifications.

Information on the certifications and standards adopted is available on [TocToc](#) website.