Aruba PEC S.p.A.

Service Practice Statement Remote Automatic Identity Proofing – ***RAIP & S-RAIP***

Release: 1.2
Date update: 08/04/2026
Approved by: Andrea Sassetti
Document classification: Public

Sassetti
Andrea
15.04.2026
07:00:14
UTC

RELEASE	DATE	CHANGELOG
1.0	12/09/2024	First version
1.1	14/05/2025	**Par. 1.2 –** Addition regarding the method of communicating document updates to business partners; **Par. 2.1, 2.2, 2.3, 5.4** – Addition regarding accepted identity documents and minor revisions; **Chapter 3** – Addition of a new chapter on Trusted Roles.
1.2	08/04/2026	**Chapter 1 –** Updates on services in scope, targeted level & OID reference and definitions. **Chapter 2 –** Introdution of new supervised modality – *S-RAIP*; **Chapter 3 –** Addition of the new *Trusted Role – Supervisor Operator.* Additional integrations for the introduction of *S-RAIP* modality.

CONTENTS

1 INTRODUCTION AND ADMINISTRATION

1.1 Overview

Aruba PEC S.p.A. (Aruba PEC), a Qualified Trust Service Provider, accredited by AgID since 2007, provides qualified public key certification services, as well as various other trust services (for further information, go to the website - https://www.pec.it).

Identification of the users is the first and the main step to provide trust services. Aruba PEC allows users to identify themselves in many different ways. This document describes a new fully automated component which uses Artificial Intelligence (AI) techniques to process biometric data for identification, Remote identity proofing, that guarantees the highest level of confidence ensuring an user friendly experience and also the best standards in the identification methodologies to prevent any kind of fraud or identity theft.

The scope of the document is to describe the procedures and the general rules of *Remote Identity Proofing* identification process implemented by Aruba PEC to allow provision of trust services and qualified trust services including *Qualified Electronic Registered Delivery Services* – QERDS – and *Qualified Certificates*.

For such services, the Remote Identity Proofing process is implemented in accordance with Regulation (EU) No 910/2014 – eIDAS (current version), ETSI EN 319 401 - *General Policy Requirements for Trust Service Providers standard* and ETSI TS 119 461 - *Policy and security requirements for trust service components providing identity proofing of trust service subject*, at the *Extended Level of Identity Proofing* (**OID 0.4.0.19461.1.2**).

1.2 Practice Statement Administration

1.2.1 Version of the SPS and organization in charge

The version of Service Practice Statement (SPS) is indicated on the title page, it has been drawn up, published and updated by Aruba PEC.

The individual responsible within Aruba PEC is:

Andrea Sassetti
Director of Certification Services
Aruba PEC S.p.A.

This SPS is reviewed and, if necessary, updated at least annually.

Any new version of this SPS is immediately published to users and relying parties on the Aruba S.p.A. website (https://www.pec.it/termini-condizioni.aspx) in signed PDF format, in order to guarantee its origin and integrity.

A notification will also be sent to Aruba PEC's business partners who use *Remote Automatic Identity Proofing* to issue qualified trust services.

1.2.2 Approving parties

This document is approved by the Aruba PEC Services Department, following verification by the company departments involved and taking account of the provisions of ETSI TS 119 461 standard and ETSI TS 119 461 §6.1, §6.2 of ETSI EN 319 401 standard.

1.3 Definitions

Terms used in this document are defined as follows:

APCER	Attack Presentation Classification Error Rate.
Applicant	He/she is the natural person who is requesting to Aruba PEC a trust service for which identification is mandatory. The Applicant can also represent a legal person.
Aruba Legally Compliant Archiving Service	Aruba's component specifically designed for log-term legally compliant archiving of digital documents.
Authoritative evidence	Evidence that holds identifying attribute(s) that are managed by an authoritative source.
Authoritative source	Any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.
Binding to Applicant	Part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence the presented document is a genuine one and, more important, not cloned or copied in some way, preventing spoofing attacks like printed documents, high resolution digital pictures, cloned chip, etc the presented document is a genuine one and, more important, not cloned or copied in some way, preventing spoofing attacks like printed documents, high resolution digital pictures, cloned chip, etc..
BPCER	Bona Fide Presentation Classification Error Rate.
Digital identity document	Identity document that is issued in a machine-processable form, that is digitally signed by the issuer and that is in purely digital form. A digital identity document can be contained in a physical identity document, e.g. an eMRTD contained in a passport or national identity card.
Electronic identification means	Material and/or immaterial unit containing person identification data and which is used for authentication for an online service, as stated in Regulation (EU) 910/2014. material and/or immaterial unit containing person identification data and which is used for authentication for an online service.
Extended LoIP	Level of Identity Proofing (LoIP) reaching a high level of confidence based on the fulfilment of good practice minimum requirements for the identity proofing process. This level is considered suitable for identity proofing for issuing of qualified certificates and qualified electronic attestations of attributes according to eIDAS Regulation. For further information see also ETSI TS 119 461.
Identity document	Physical or digital document issued by an authoritative source and attesting to the applicant's identity physical or digital document issued by an authoritative source and attesting to the applicant's identity.

Identity proofing context	External requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself. External requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself.
Identity proofing process	Process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes.
Liveness detection	Measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture.
PAD	Presentation Attack Detection.
Physical identity document	Identity document issued in physical and human-readable form.
Proof of access	Any source irrespective of its form that can be trusted for reliable data, information and/or evidence that can be used in an identity proofing process, provided that the applicant is able to demonstrate access to the source.
Recognition Session	Single identification session where the user is asked to perform few activities in order to provide and validate his/her identity.
Remote Automatic Identity Proofing (component)	A specific component, implemented in Aruba applications, that enables Applicant recognition through liveness and biometric AI-based techniques, as well as NFC reading of the identity document held by the Applicant.
Remote Identity Proofing (process)	Identity proofing process where the applicant is physically distant from the location of the identity proofing. Identity proofing process can be carried out in a fully automated – RAIP- or supervised - S-RAIP - manner.
Trusted Register	Public register, database, or other source that is trusted for conveyance of identity attributes in the identity proofing context national business register or national population register national business register or national population register.
Validation	Part of an identity proofing process that determines whether or not attributes are validated by the presented evidence and whether or not the evidence is genuine, authoritative and valid.

2 REMOTE AUTOMATIC IDENTITY PROOFING – RAIP & S-RAIP

Remote identity proofing is a crucial element in creating trust for digital services. Remote identity proofing is the process where a user proves he or she is the owner of a claimed identity.

The Remote identity proofing process is usually carried out over a webcam or a mobile device, where the users show their faces and display their government issued documents – legal identity cards or passports - or by other electronic identification means.

The Remote identity proofing provided by Aruba PEC is a process of identification of the Applicant to provide trust services or qualified trust services. The entire process is orchestrated by Aruba applications which integrate a specific AI-based component to enable the collection of Applicant data required for secure identification.

The remote identity proofing process may be carried out either:

- in a fully automated manner – also called ***Remote Automatic Identity Proofing - RAIP****, or*
- through an optional human supervised variant – *Supervised Remote Automatic Identity Proofing* – ***S-RAIP*.**

In the latter case, human supervision is limited to the verification phases of the collected data and information. Such supervision activities are performed by "*Supervisor operators*" who are formally appointed and periodically trained by Aruba PEC, in accordance with internal policies and procedures. These operators carry out their activities in compliance with specific internal procedures defined by Aruba PEC, ensuring consistency, reliability, and adherence to applicable regulatory requirements."

The Remote identity proofing process described in this document is composed by five different steps:

1. ***Initiation***
2. ***Attributes and evidences collection***
3. ***Attributes and evidences validation***
4. ***Binding to Applicant***
5. ***Issuing of proof***

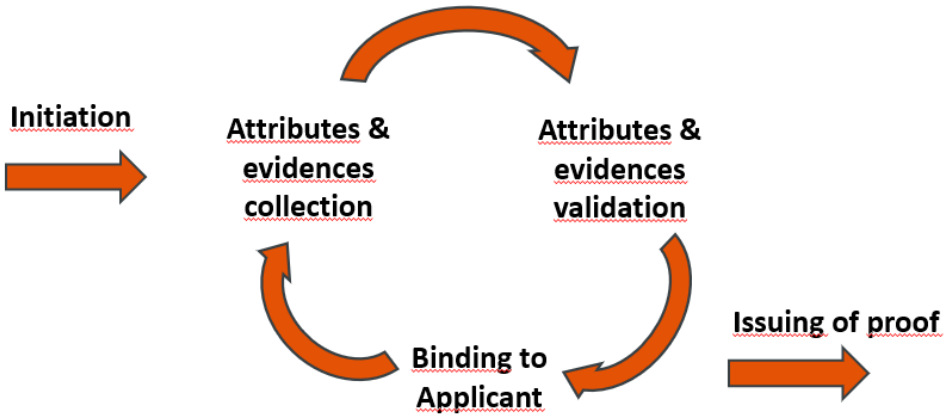

Figure 1 - Steps of remote identity Proofing

Depending on the identity proofing context, Aruba PEC may collect and validate autonomously other attributes or evidences through querying trusted registers, as national business register or national population register, or also through manual procedures. The proof generated at the end of the identification process contains all the evidences and attributes validated during the process.

In the case of the supervised variant of S-RAIP, the human supervision is applied exclusively during the *Validation of attributes and evidences* and *Binding to Applicant* phases, while all other phases of the process remain fully automated.

Aruba PEC defines and maintains target performance levels for *False Acceptance Rate* (FAR) and *False Rejection Rate* (FRR), aligned with industry best practices, for both RAIP and S-RAIP modalities. The service is designed and operated to achieve target values of FAR equal or better to 1/500.000 and FRR equal to 0.2. Aruba PEC also defines and maintains target performance levels for PAD metrics, including APCER and BPCER, with reference to PAD Level 1 to Level 3 and Level 5 (injection) scenarios. The expected APCER is 0% across all such levels, while BPCER remains within the defined target values.

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

A more detailed description is provided in the following chapters.

2.1 Initiation of the Remote Identity Proofing

The identification process is initialized by the Applicant after the request of a service provided by Aruba PEC, such for example an eIDAS compliant qualified certificate for electronic signatures and seals. The request for a trust service is formalized through an application form where the Applicant's data required for the provision and for handling of the trust service are collected by Aruba PEC.

If the Applicant is a natural person, this minimum set of personal data has been mandatory for the registration:

- Name and surname of the Applicant[1];
- National Unique identifier (Tax Identification Number – TIN – or, optionally, the number of identity document);
- Email address and telephone contact.

If the Applicant is a natural person representing a legal person, in addition to the previous list the following data has been necessary:

- Full name of the legal person;
- National Unique identifier of legal person (usually VAT or national registration number);
- Country of the registration of the legal person;
- Address of registered office.

[1] The use of pseudonyms is not permitted for the issuance of qualified trust services. Applicants shall declare their real identity, which must be verified through the identity proofing process. This ensures the unambiguous association between the Applicant and the issued services.

Depending on the trust service requested by the Applicant, Aruba PEC can request additional data to proceed with the provisioning.

If the trust service requested involves identification of the Applicant, he/she can choose one of the possible methods made available by Aruba PEC, including Remote Identity Proofing. The Applicant is then informed that the Remote Identity Proofing method accepts only electronic documents compatible with the ICAO-9303 standard[2] and that he/she must have a device equipped with an NFC reader and with the dedicated App installed.

Before starting the identification process through Remote Identity Proofing, this Service Practice Statement, the Terms&Conditions of the Remote Identity Proofing process of and the specific Privacy Policy about the processing biometric data of the Applicant will be shown and accepted by the Applicant. All the acceptances are mandatory to proceed with the beginning of the identification through Remote Proofing and are appropriately logged and stored by Aruba PEC.

All documents shown to the Applicant can be downloaded locally and available online at the Aruba PEC site https://www.pec.it/termini-condizioni.aspx and https://enterprise.aruba.it/home.aspx .

More restrictions in the registration and identification process may applied by Aruba PEC depending on the service requested by the Applicant.

2.2 Attributes and Evidences collection

At this stage the Applicant can begin the identification process through *Remote Identity Proofing,* in either RAIP or S-RAIP modality. The procedure is entirely guided by the dedicated App installed on mobile device held by the Applicant[3].

The App collects all the evidences needed to identify the Applicant and send them to Aruba's Data-Centers via TLS secure connection for the next steps of analysis and validation. Any error occurring during the data acquisition or upload phase results in the automatic rejection of the entire identification process. After transmission, the App deletes all data related to the Applicant from the mobile device.

If the Applicant is natural persons, the Remote Automatic Identity Proofing process collects at minimum the following set of data:

- Name and surname of the Applicant;
- Scan of the physical identity document used in the procedure;
- Photo of the Applicant extracted from the chip of the digital identity document held by the Applicant;
- Data related to the digital identity document (e.g ID document, Tax Identification Number – TIN - , validity, country, issuer, etc...);
- Photos of the Applicant's face (face scan consisting in 60-180 frontal frames with resolution at least of 640x480 and 50 frames per second) extracted from the Remote Proofing Process;
- Metadata related to the identification session (ID, start date, end date, duration, warnings);

[2] Currently, only the Italian Electronic Identity Card (CIE) and the Italian Electronic Passport are accepted.
[3] Security measures required for the mobile device are descripted in Chapter 4.

- Result of the identification session (success/fail).

If the Applicant is a natural person representing a legal person, in addition to the above evidences collected for natural person, Aruba PEC applications independently proceed to query trusted registers to collect at minimum the following data:

- Full name of the legal person;
- Unique identifier of legal person (Tax Identification Number – TIN - or other national unique code depending on the context);
- Name, Surname and, if possible, the Unique Identifier of the natural person representing the legal person.

For some types of legal persons, the information is not collected in national trusted registers, in this case Aruba provides a manual procedure that involves the upload by the Applicant of specific types of documents and attestation as evidence about the role of the Applicant concerning the legal person.

Depending on the service requested by the Applicant and the context of identification, Aruba PEC provides a list of documents accepted for verification of the Applicant's powers of representation on its website https://www.pec.it.

All the communications towards trusted registers are secured by using encrypted protocol and authentication.

2.3 Validation of attributes and evidences

The Remote Automatic Identity Proofing process involves two types of evidence validation:

- Physical and digital identity document validation,
- Liveness and face matching.

For the first one, after the acquisition via App of front/back pictures of the physical identity document of the Applicant, Aruba PEC verifies that the physical document is among those accepted compatible to the ICAO-9303 MRTD standard (Italian e-Passport or italian e-ID Card). This limitation is mandatory and ensures the presented document is a genuine one and, more important, not cloned or copied in some way, i.e. issued by a trusted organization. This verification prevents spoofing attacks like printed documents, high resolution digital pictures, cloned chip, etc. If the document is not an ICAO-9303 MRTD compatible one, the process ends immediately, marking the entire session as failed.

In addition, Aruba PEC compares the extrapolated data through NFC from the chip of the identity document with respect to the data stated by the Applicant in registration stage, in particular Name and Surname as well as the Tax Identification Number – TIN – and/or the ID document. Also, the validity and the authenticity of the digital signature of the Issuer is verified to prevent any fraud due to counterfeited document. In case of the presence of accents or diacritics marks, the ICAO 9303 Part 3 standard is applied for encoding and validation. Any other mismatch results in an automatic failure of the remote identity proofing process.

For the liveness and face matching phase, the mobile App, immediately after the start of the recognition session, asks for the liveness check in order to ensure the Applicant is a real person and not a tentative of spoof.

If the liveness detection identifies it as a possible treat or attack the process ends immediately, marking the entire session as failed. Also, the Remote Automatic Identity Proofing verifies the match between the picture

extracted by NFC reading from the chip of the identity document, the image printed on the physical identity document, and 3D model of the Applicant's face created with images extrapolated during the identification session.

In case the matching score does not reach the expected level of accuracy, the identification session will be marked as failed.

In the case of the supervised variant S-RAIP, supervision activities are performed by operators formally appointed and periodically trained by Aruba PEC (referred as "*Supervisor*" operators), who act in accordance with strict internal supervision procedures. Such supervision is carried out using dedicated computerized tools to zoom in on details supporting face matching and evidence verification. Furthermore, if during the supervision phase any mismatch or inconsistency is detected among the collected evidences, the entire identification session shall be rejected by the *Supervisor Operator.* In case of natural person representing a legal person, Aruba PEC applications, after the validation of the Remote Automatic Identity Proofing component about the natural person identity, verify the attributes and the evidences collected by trusted registers about the legal person with respect to the data stated in registration stage. Such evidences concerning the legal person may also be subject to supervision activities, where applicable, performed in accordance with Aruba PEC internal procedures. In case of errors, Aruba PEC provides a manual procedure that involves the upload by the Applicant of specific types of documents and attestation as evidence about the role of the Applicant concerning the legal person; the collected evidence will be verified by an Aruba PEC designed officer. If the reliability of the role of the Applicant cannot be confirmed by the officer, the identification session will be marked as failed.

The entire process of validation of attributes is hosted internally into Aruba's Data Centers, in a protected environment as described in the next chapters; no decision step is implemented in the mobile App installed on the device held by the Applicant in order to reduce risk of injection, malicious code etc.

2.4 Binding to Applicant

After the validation stage, the Remote Identity Proofing binds to Applicant all the evidences collected and validated in the previously stages creating the proof of evidence as *.zip bundle file*. All evidences are stored into the bundle file following a well-defined schema.

In particular for RAIP variant the .zip bundle file consisting in:

- Photos captured from the Applicant as liveness audit photo (facescan in high and low resolution)
- Photo of the Applicant extracted by the digital identity document of the Applicant;
- Front/back pictures of the physical identity document of the Applicant;
- Execution reports with the summary of each phase of Remote Identity Process;
- Data extracted from the digital identity document (ID, tax code, validity, issuer entity, etc...);
- Metadata of the session (as date, duration, ID of the session etc…).

In the case of the supervised variant S-RAIP, in addition to the elements listed above, the outcome of the supervision activity performed by the Supervisor operator is also recorded and stored in Aruba PEC systems, ensuring the integrity, completeness, and security of the related logs and records.

In case the Applicant is a natural person representing a legal person, Aruba PEC applications will add all the collected and validated evidences about the legal person and the role of the Applicant to the .zip bundle file described above.

2.5 Issuance of identity proofing result

The proof of evidence, unique and self-consistent, is stored into Aruba Legally Compliant Archiving Service for the time required by laws, depending on the service required by the Applicant. At the end of the retention time, all the evidences collected during the identification process will be deleted from Aruba systems.

More details about the archiving of the evidences obtained from identification process has been reported in par. 5.5 and in the Policy Statement of the services provided by Aruba PEC.

2.6 Termination

Aruba PEC S.p.A. can disable or terminate the RAIP and/or S-RAIP component and process in any moment and for any reason. Before the planned termination:

- at least 90 days prior to the scheduled termination date of the Service, a notice will be sent to the supervisory body (AgID), the compliance assessment body (CAB) and all the relevant third parties;
- an information note will be published in a manner that stands out on the Aruba PEC site, in order that information is made available to all customers and all Relying Parties, including all possible subcontractors;
- the responsibility for storing evidences can be transferred to another trustworthy entity that that can guarantee its storage for an adequate time period can guarantee its storage for an adequate time period.

The termination of the Service does not automatically result in termination of other services provided by Aruba PEC, e.g. certification authorities services. In the latter case more details are provided in the Practice Statement of the involved service.

3 TRUSTED ROLES

The organizational structure is established in compliance with the ETSI EN 319 401 standards and in compliance with current laws.

The trusted roles and the related responsibilities are formally assigned by the Management through letters of appointment. The requirements for retaining an appointment are re-evaluated at least annually and against changes in the company's organizational structure. Appointees can make use of employees and staff members to carry out their activities, in compliance with the general provisions established by the company.

Personnel functions and tasks are allocated in such a way that a single person is not able to circumvent the security measures for protection of the Aruba PEC systems; moreover, the designated parties are free from conflicts of interest that could harm the impartiality of the activities assigned to them.

Aruba PEC has established the following *trusted roles* in positions of responsibility as part of the *Remote Automatic Identity Proofing* service*:*

- **Security Manager:** responsible for implementing and managing security procedures. This role corresponds to the 'Security Manager' referred to in current regulations;
- **Security Officers**: responsible for supporting the Security Manager in implementing and managing security procedures;
- **System Administrator**: responsible for the installation, configuration and maintenance of Aruba PEC's IT systems relating to *Remote Automatic Identity Proofing* service;
- **System Operator:** responsible for the daily operation of the systems relating to the *Remote Automatic Identity Proofing* service;;
- **System Auditor**: responsible for verifying logs and archives relating to the *Remote Automatic Identity Proofing* service;
- **Identity Verification Officer**: responsible for ensuring that the identity verification processes carried out through the *Remote Automatic Identity Proofing* process comply with those required;
- **Supervisor Operator**: responsible for verifying the readability, completeness, validity, authenticity, integrity, and correctness of the documentation and evidences collected during the Applicant's idenitty proofing process*.*

Some persons may hold multiple roles provided that this does not prejudice the security and trustworthiness of the PKI and is not prohibited by applicable regulations and standards.

4 SECURITY MEASURES

Aruba PEC has implemented an information security management system certified using the ISO 27001 standard.

The ISO 27001 security standard ensures information security through the adoption of appropriate procedures, behavioural norms, measures and training courses.

The standard is based on the following principles:

- ***Information Security***: preserve confidentiality, integrity and ensure the availability of information.
- ***Confidentiality***: ensure that information is only accessible to those who are authorised.
- ***Integrity***: safeguard the accuracy and completeness of information and preserve the technique by which information is processed.
- ***Availability***: ensuring that information is available and accessible to authorised personnel when necessary.
- ***Risk Assessment, Risk Analysis***: detecting threats and their impact on the system, analysing the vulnerability of information and processes, calculating the probability of events occurring.
- ***Risk Management***: identify, control, contain and eliminate the security risk that may affect the system.

Aruba PEC has all the security guarantees compatible with the type of service provided, both at physical and IT level. More details about these measures have been reported in Policy Statement of the services provided by Aruba.

4.1 Risk scenarios and adopted security measures

In the following, we outline the main risk scenarios specific to the recognition method and the countermeasures adopted by the organisation.

RISK SCENARIOS	DESCRIPTION	DESCRIPTION OF THE MAIN COUNTERMEASURES ADOPTED
Delivery of digital identity to illegitimate Holder	Illegitimate APP-API calls.	Client credential authentication. Session uniqueness using GUID with 24-hour validity. User initialized session expires within 10 minutes.
	Tampering of mobile device (hijacking of device hardware, hijacking of network traffic, reverse engineering of application code, injection and substitution of application code at runtime, etc.).	Tamper detection through rooting/ jailbreaking. Fingerprinting of essential device components. Detection of the presence of suspension lock. Detection of hooking techniques. Detection of debuggers.
	Presence of artefacts built to trick the system (print attacks, replays attacks, 3D masks attacks, Deep Fake attacks, etc.).	Biometric Presentation Attack Detection (PAD) techniques.
	False/cloned/stolen or altered identity document.	Certificate verification and eventual revocation. Use of chip authentication (NFC) to verify the original identity document.

RISK SCENARIOS	DESCRIPTION	DESCRIPTION OF THE MAIN COUNTERMEASURES ADOPTED
		Exclusive use of ICAO-9303 MRTD electronic documents.
	Holder not corresponding to the document.	Comparison of document image with video acquired via APP. The recognition flow is blocked in case of negative verification.
Theft or tampering with the Holder's recognition and identification data	API calls redirection to illegitimate systems.	TLS adoption with certificate pinning.
	Theft or tampering of data in transit.	TLS adoption including certificate verification and encryption of data sent by the APP. Encryption keys are not stored on the devices. Encryption keys are rotated every 90 days.
	Theft or tampering of data stored.	No data storage on the device. Storage of unencrypted data on central systems limited to the time required for recognition operations, with removal at the end of the flow. Documents are stored in encrypted form.
Supply Chain Compromise	Lack of adoption of best practices.	Selection of a supplier having the necessary sector and security certifications (OWASP ASVS Level 2; ISO/IEC 30107-3 Level 1/2). Contractualisation of the security requirements to be respected. VA/PT test execution.
	Introduction of errors in software updates.	Non-regression test and VA/PT test execution.

5 GENERAL TERMS

5.1 Introduction

These terms and conditions apply to the relationship between Applicant (“Applicant”) and Aruba PEC, in case of the same chose the identification method “*Remote Automatic Identity Proofing*” (also “Service”), , in either RAIP or S-RAIP modality.

These terms govern the access and use of the remote identity verification for the services provided by Aruba PEC to the Customer.

These terms and conditions may be updated from time to time. Any changes will be indicated by updating the "Last Updated" for each change that will be made.

5.2 General Dispositions

Remote Automatic Identity Proofing is designed to verify the identity of the Applicant remotely to access services provided by Aruba PEC. The Applicant accepts that the services provided by Aruba PEC that integrate the aforesaid method are regulated separately by the specific service provision conditions.

5.3 Duties of the Applicant

The Applicant must provide the following identity information as described in the previous paragraphs.

Additionally, the Applicant agrees and confirms that:

- The identity verified through the submitted information and documents matches the identity claimed while using Aruba PEC Services;
- All information provided is complete and accurate;
- The Applicant will comply with all applicable local, state, national, and international laws, regulations, and conventions when using this process.

The Applicant must NOT:

- Use Remote identity proofing for any fraudulent, commercial, or competitive purposes;
- Falsely claim an identity that is not their own or that they are not authorized to establish on behalf of someone else;
- Falsely claim to be associated with another person or entity;
- Modify, alter, or interfere with any content or information;
- Use any automated tools, such as bots or scraping tools, to access, collect, or interact with Aruba PEC;
- Circumvent any measures designed to prevent violations of these terms and conditions.

5.4 Access Requirements

The Applicant must need a trusted mobile device (smartphone) equipped with a camera and video capabilities, NFC reader capability, an electronic identity document compatible with ICAO-9303 MRTD standard, such as an Italian Electronic Identity Card or Italian Electronic Passport, and be connected to the internet.

For optimal security and performance during the Identity Services process:

- The images and videos you capture must show the entire document and a clear, full headshot. They should be sharp, well-lit, high-contrast, and free of any blurriness or obstructions;
- It’s recommended to use the latest versions of Aruba PEC’s mobile application;
- The device used must have all security updates installed.

5.5 Types of stored data and retention period

Aruba PEC stores the following types of data: the execution phases of each identification session, including the start and end date/time of the session, the session result, and the report of the identification session carried out through Remote Automatic Identity Proofing.

For each action, Aruba PEC stores the related evidences:

- face scans: verification images (audit photos) in high and low quality;
- document scan: front/back images of the document + NFC image + NFC data + extracted user data + device type + device model + device IP address;
- date of creation of the identification request;
- date and time of the start of the identification session (i.e. when the Applicant starts the NFC scanning);
- date and time of the end of the identification session;
- where applicable, the result of the supervision activities of the identification process;
- privacy consents.

The data retention period may vary depending on the type of requested trust service. The maximum data retention period is set to 20 years. The exact data retention period is defined and specified in the contractual documentation of the specific service, to which reference is made.

5.6 Limitation of Liability

Aruba PEC will not liable for any loss or damage arising from the use of the system of Remote Automatic Identity Proofing, including issues related to device security, incorrect information, or unauthorized access.

Any and further limitations of liability regarding the use of remote identity proofing is governed by the specific general terms and conditions where it is integrated.

We will not be liable or responsible for any failure to fulfil, or delay in fulfilling, any of our obligations under these terms and conditions caused by any act or event beyond our reasonable control, including the unavailability of the Service due to your own error, the unavailability of third-party platforms, errors caused by API providers (or similar), network issues, or outages.

5.7 Assessment of Remote Identity Proofing

Remote identity proofing is a system based on the EU eIDAS Regulation.

The policies and standards governing this service are:

- ETSI TS 119 461 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
- ETSI EN 319 401 - General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 1/2 - Policy and security requirements for Trust Service Providers issuing certificates.
- Relevant ISO Standard, e.g. ISO 27001.
- Regulation (EU) 2016/679 (EU GDPR).

5.8 Contact Information

For any questions or concerns regarding these Terms or the use of Remote identity proofing:

- Call centre on accessible through the channels on https://assistenza.aruba.it
- By communication to the address CPS-requests@ca.arubapec.it

5.9 Governing Law

These Terms are governed by and construed in accordance with the laws of Italy and all disputes are referred to the jurisdiction of the court of Arezzo, unless otherwise regulated in the specific supply conditions where the service is integrated.

5.10 Final Dispositions

Aruba PEC may transfer its rights and obligations under these terms and conditions to another organization, but this will not affect your rights or our obligations under these terms and conditions.

Applicant may only transfer your rights or obligations under these terms and conditions to another person if we agree in writing.

A person who is not a party to these terms and conditions has no right to enforce any of these terms and conditions.

If we do not insist that you perform any of your obligations under these terms and conditions, or if we do not enforce our rights against Applicant, or if we delay in doing so, this does not mean that we have waived our rights against you and does not mean that you are not required to comply with those obligations. If we do waive a default by you, we will only do so in writing, and this does not mean that we will automatically waive any future defaults by you.

Each of the conditions in these terms and conditions operates separately. If any court or competent authority decides that any of them are unlawful or unenforceable, the remaining conditions will remain in full force and effect.

5.11 Referral Clause

For all matters not governed by these terms and conditions, please refer to the specific terms and conditions of provision of the services where the Service is integrated.