Qualified Certificates

Operating Manual / Certification Practice Statement and Certificate Policy

Version 1.9

(16 March 2023)

HISTORY OF CHANGES MADE

Version	Date	Changes
1.0	9 May 2017	First version of the document.
1.1	20 November 2017	P.1.1 – references to replacement certifying bodies added P.1.5.1 – references to document version and CPS supervisor added P.9.1.1 – URL for certifying body website added P.9.6.1 and 9.6.3 - specified obligations art. 32 of the CAD P.9.17.2 – paragraph with recommended document formats added P.9.8 – limitations of liability explained Appendix A - references to certification keys updated Appendix B – new appendix containing operating procedures for generating and verifying signatures added
1.2	26 April 2018	Whole document – Logo updated P.1.2 – AgID website link changed P.9.8 – formulation of limitations of liability changed P.9.16.3 – typo in the paragraph heading corrected P.1.4 – Availability of certain policies updated Appendix A – New CA key for ATe Model added
1.3	28 February 2019	P.1.3.1. Legal Representative details updated P.3.2.3 Remote identification procedures by means of a national e-ID scheme added (Procedure 4) and details of Procedure 2 provided P.3.2.5.2 details of OID 1.3.76.16.5 added P.4.9.3. Revocation procedure (online procedure) link amended, email address for offline procedure added and online link with revocation request procedures specified
1.4	23 May 2019	P.1.3.1. Legal Representative details updated P1.1, p1.4, p1.6, p1.7 (added), chapter 3, p.6.1.7.2, p.6.3.2, p.7.1, p.7.1.2, p.7.1.6, Appendix A: various additions and clarifications relating to qualified website authentication certificates (QWAC). P.9.4, 9.6.1 Personal data processing details updated. P.9.13 Jurisdiction indicated.
1.5	16 December 2019	P.4.3.1 - added methods for sending personal and emergency codes P.3.2.5.1 and 9.8 - limitations of liability in respect of slight negligence deleted P.3.1.2, 3.2.5.1, 4.1.1, 4.1.2.1, 4.8, 4.9.1, 9.6.4 and 9.6.5 - replaced 'role' by 'qualification' in references to certificates containing information on the professional qualification or position held by the Holder in third party organisations P.3.2.5.1 and 4.1.1 - replaced by references CNIPA Deliberation No 45/2009 (repealed) P.7.1 - inserted indications on the application of the recommendations issued by the Agency with Det. AgID n.121/2019

		P.4.9.16 - amended suspension period limit P.4.3.1 - updated list of personal code and emergency code transmission channels P.1.3.2 and 4.1.2 - reworded I&A responsibility of Applicants P.4.9.3 - specified how to deliver the user code Updated the list of editors and verifiers in this document P.5.1.1 - updated data center certification P.5.2.1 - inserted the autonomous figure of "Safety Officer" P.8.2 - removed the identity of second party auditors
1.6	21 February 2020	P.4.1.2.1 – improvements in the description to fill the request form P. 5.3.2 – removed references to pending proceedings for employees P. 9.8 – added further clarification of the CA's liability P. 4.9.3 – modified the description of the procedures for the revocation request.
1.7	31 July 2020	P.1.4 and 7 Updated the description of OID policies taking also into account the "Signature with SPID". P. 3.1.2 - Addition of a specification for the SAN following Determination no. 157/2020 P. 3.2.3 - Mode 6 added to allow identification by employer. Moved some paragraphs from mode 1 to par. 3.2.3. Updated the list of acceptable identification documents. Added sub "Mode 6" the description of the new identification model. Added the reference to the attachment "Permitted identification documents". P. 6.1.7.2.: Specific addition for "Signature with SPID" P. 7.1.2 - Specific additions consequent to Determination n. 157/2020 Added list of attachments with "Permitted identification documents".
1.8	3 March 2021	P. 1.6: Added paragraphs relating to definitions and acronyms 1.6.1 and 1.6.2; P. 3.2.3: added a further description for authentication in mode 2; P.4.1.2.1: minor changes; Appendices C and D added.

1.9	16 March 2023	P.1.3.1: Updated email address (general); P. 1.4 Specific addition for eIDAS Regulation; removed the note at the end of the table; P.3.1.2: Specific addition CountryName Attribute interpretation (seal certificate); P.3.1.5.: Specific addition consequent to Notify AgID n.18/2021 P.3.2.3: Specific addition Procedure 2; minor change to Procedure 5; P. 4.1.2.1: modified the description of acceptance of electronic signatures and elimination of mandatory e-mail address; P. 4.2.1: specific addition of the exception of Appendix D; P. 4.3.1: modified the number 11) relating to the sending of personal codes and emergency codes; P. 4.6.1, 4.6.2, 4.6.3: specific additions for tacit renewal of the certificate; P. 4.9.1: clarifications introduced in case of loss of QSCD certification; P. 6.7: VA periodicity update; P. 8.6: minor changes to the acronym “CAB”; P. 8 Appendix D: modified last passage of the paragraph relating to the limit of use for signing documents.

Approved by:	Andrea Sassetti

LIST OF FIGURES

CONTENTS

1. INTRODUCTION

1.1 Overview

Aruba PEC S.p.A., a 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).

A certificate links a public key to a party (individual or organization). As holder of the certificate, that party possesses and uses the corresponding private key. The certificate is generated and supplied to the holder by a trusted third party, referred to as a **Certification Authority** (**CA**), and is signed digitally by the CA.

Aruba PEC fulfils the role of CA within the scope of the service described hereunder. Within the scope of this document, the terms "CA", "Provider" (of Trust Services) and "Certifier" are used as synonyms and all refer to Aruba PEC, understood as the party supplying the CA service, and/or the electronic systems used by Aruba PEC to provide the CA service, unless otherwise specified.

The reliability of a certificate, that is, the trust that can be placed in the connection between the public key and the party specified in the certificate, depends significantly on the operating procedures followed by the CA, on the obligations and responsibilities that the CA and the holder take on and on the physical, operational and technical security measures put into place by the CA for the protection of its processing systems. These aspects, together with other information necessary for evaluating the service offered by a CA, are described in a public document referred to as the **Certification Practice Statement** (**CPS**).

This document is Aruba PEC's CPS relating to the issue and management of **qualified certificates** in accordance with current laws, in particular EU Regulation no. 910/2014 (for the sake of brevity, hereinafter also referred to as the "eIDAS Regulation").

Aruba PEC S.p.A. is the CSP and documentation keeper replacing the following CSP, which is no longer active:

- Trust Italia S.p.A. (terminated on 20/02/2008)

The structure of this CPS is based on the RFC 3647 public specification.

Regarding Qualified Website Authentication Certificates (QWAC), Aruba PEC complies with the current version of the CA/Browser Forum "Guidelines for Issuance and Management of Extended Validation Certificates", published at http://www.cabforum.org. In the event of a conflict between this CPS and said Guidelines, the latter shall take precedence.

1.2 Name and Identification of the document

The version of this CPS is indicated on the title page.

The current version of the CPS is published on the CA's website (https://www.pec.it) and on the AgID website (http://www.agid.gov.it/). In the event of any discrepancies between the two publications, the version published on the CA website shall prevail.

This CPS is published in signed PDF format, in order to guarantee its origin and integrity.

1.3 PKI Participants

1.3.1 Certification Authority

Within the scope of the PKI to which this CPS refers, the role of the Certification Authority (CA) is fulfilled solely by the company Aruba PEC S.p.A. The company's identification details are provided below:

Company name:	**Aruba PEC S.p.A.**
Address of the registered offices and operational headquarters:	**Via S. Clemente, 53** **I-24036 Ponte San Pietro (BG)**
Legal representative:	**Giorgio Cecconi** (chairman of the board of directors)
Bergamo Companies Registry registration no.:	**01879020517 (REA [Economic and Administrative Index] no. 445886)**
Tax Code and VAT Registration:	**01879020517**
Telephone no. (switchboard):	**+39 0575 050.350**
ISO Object Identifier (OID):	**1.3.6.1.4.1.29741**
Main website:	**https://www.pec.it**
E-mail address (general):	**CPS-requests@ca.arubapec.it**

As set forth under Italian laws, the PKI implemented by Aruba PEC provides for only one level of certification keys (CA keys). As such, all the CA keys are "root" and, as a consequence, are self-signed.

The CA keys currently in use by Aruba PEC and covered by this CPS are listed in Appendix A.

1.3.2 Registration Authority

The identification and authentication (I&A) of parties requesting certificates may be implemented both directly by CA staff and also by delegated third parties (or "Registration Authorities", RA) based on the specific agreements stipulated with the CA. The RAs are also referred to as Local Registration Centres (CDRL).

Normally, but not necessarily, RAs also undertake "registration" activities, consisting of the sending of personal data on the Applicants (future Holders) and other data associated therewith to the CA, using secure procedures, in order for said data to be stored in the CA systems for the purpose of issuing certificates.

RAs are responsible towards the CA for the correct and safe I&A of Applicants, as wells as for processing their data in full compliance with legislation on privacy and other applicable laws. In any case, the CA remains fully responsible, for the I&A of Applicants, whether implemented by the CT itself or by the RAs.

RAs are subject to inspections by the CA, intended for verifying the RAs' compliance with the agreements stipulated with the CA.

The CA makes available to the RAs instruments and procedures for undertaking user registration operations, as well as for the issue and subsequent management (e.g. suspension or revocation) of certificates. Only RA operators expressly authorized by the CA may access said instruments.

Depending on circumstances, the RAs can also hold the role of "interested third party" (see the decree [3]) and therefore have the consequent rights and duties.

1.3.3 End users (holders)

The holder of a certificate issued in accordance with this CPS may be:

a) a natural person;

b) a natural person associated with a legal entity;

c) a legal entity (e.g. a company, a government entity or another type of organization).

1.3.4 Relying parties

The “Relying Parties” are all parties that rely on the information contained in the certificates. In particular, as concerns the CA service described here, they are all parties that verify electronic signatures and electronic seals through certificates issued in accordance with this CPS.

1.3.5 Other participants

In the context of the PKI, the national supervisory body, **AgID** (**Agenzia per l’Italia Digitale [Digital Italy Agency]**), has a very important role to play. Pursuant to the European eIDAS Regulation, the AgID publishes on its website the national Trust Service List (TSL), which lists all the accredited, qualified CAs.

1.4 Established use of certificates

Qualified certificates issued in accordance with this CPS are to be used in order to verify **seals** and **advanced electronic signatures** or for **website authentication**, depending on the type of certificate. Other uses of certificates are not provided for and are to be avoided. The CA reserves the right to revoke the certificates if it learns that they are being used improperly.

The certificates used in accordance with this CPS change in profile depending on whether the holder is a natural person or a legal entity, on whether or not the corresponding private key is located on a secure signature device (QSCD) and on whether or not signing occurs remotely. In the case of QSCDs, we refer to those certified pursuant to articles 31 and 39 of the eIDAS Regulation, or for which the transitional measures referred to in art. 51 eIDAS apply. Find listed below the **OIDs** (**Object Identifiers**) **of the policies supported** by this CPS and, for each one, the policy of reference specified in the ETSI EN 319 411-2 standard.

Policy OID specified in the certificates issued by Aruba PEC	Reference policy ETSI EN 319 411-2	Person	Keys on QSCD	Remote signature
1.3.6.1.4.1.29741.1.7.1	**QCP-n-qscd**	Physical	YES	NO
1.3.6.1.4.1.29741.1.7.2	**QCP-n-qscd**	Physical	YES	YES
1.3.6.1.4.1.29741.1.7.3	**QCP-n**	Physical	NO	NO
1.3.6.1.4.1.29741.1.7.4	**QCP-n**	Physical	NO	YES
1.3.6.1.4.1.29741.1.7.5	**QCP-l-qscd**	Legal	YES	NO
1.3.6.1.4.1.29741.1.7.6	**QCP-l-qscd**	Legal	YES	YES
1.3.6.1.4.1.29741.1.7.7	**QCP-l**	Legal	NO	NO
1.3.6.1.4.1.29741.1.7.8	**QCP-l**	Legal	NO	YES
1.3.6.1.4.1.29741.1.7.9	**QCP-w**	Giuridica	NO	NO

In addition, additional OIDs may be indicated in the Appendices to this document.

The certificates normally contain two Policy OIDs: Aruba PEC's owner OID and the standard one specified in the ETSI EN 319 411-2 standard. There may be a third Policy OID in the case of certificates for "verified digital signature" keys pursuant to AgID Resolution no. 63/2014 (in this case, the additional Policy OID is **1.3.76.16.3**).

Any **usage limits** may be specified in certificates using the **userNotice** attribute of the CertificatePolicies extension. In particular, certificates for *automatic signatures* are a particular kind of certificate for remote signatures, and they contain a specific usage limitation established by AgID (see http://www.agid.gov.it/sites/default/files/circolari/limiti_uso_nei_cq_2014_v.1.pdf)

Any **limitations on the value** of transactions (under which the certificate may be used) may be specified in the qCStatements extension of certificates by way of the **QcEuLimitValue** item.

1.5 CPS administration

1.5.1 Version of the CPS and organization in charge

This document is version 1.9 of Aruba PEC S.p.A.'s CPS and has been drawn up, published and updated by Aruba PEC S.p.A. .

The individual responsible for this operating manual within Aruba PEC is:

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

Requests for information or explanations regarding this CPS and/or the certificate policy (CP) set forth herein may be sent by e-mail to the following address: CPS-requests@ca.arubapec.it.

1.5.2 Approving parties

This CPS is approved by the CA Services Department, following verification by the company departments involved and taking account of the provisions of §6.1 of the ETSI EN 319 401 standard.

1.5.3 Approval procedure

The drawing up and approval of the CPS follows the procedure set forth in the company's Quality Management System. This CPS is reviewed and, if necessary, updated at least annually.

1.6 Definitions and acronyms

1.6.1 Definitions

Agenzia per l'Italia Digitale (AgID)	National Body for the digitization of the Public Administration (formerly DIGITPA and CNIPA).
Qualified electronic seal certificate	An electronic seal certificate that is issued by a qualified trust service provider and complies with the requirements set out in Annex III of the eIDAS Regulation.

Qualified certificate of electronic signature	An electronic signature certificate that is issued by a qualified trust service provider and complies with the requirements set out in Annex I of the eIDAS Regulation.
Private Key	The element of the asymmetric key pair, used by the Holder, through which the qualified electronic signature is affixed to the IT document.
Public key	The element of the asymmetric key pair intended to be made public, with which the qualified electronic signature affixed to the IT document by the Holder is verified.
Emergency code	Security code delivered to the Holder to request the suspension or revocation of the certificate.
Digital signature	A particular type of advanced electronic signature based on a qualified certificate and on a system of cryptographic keys, one public and one private, related to each other, which allows the Holder through the private key and the recipient through the public key, respectively, to make manifest and to verify the origin and integrity of an IT document or a set of IT documents.
Electronic signature	Data in electronic form, enclosed or connected by logical association to other electronic data and used by the signatory to sign.
Qualified electronic signature	An advanced electronic signature created by a qualified electronic signature creation device based on a qualified certificate for electronic signatures.
OTP - One Time Password	A One-Time Password is a password that is valid only for a single transaction. The OTP is generated and made available to the Owner immediately prior to the affixing of the qualified electronic signature. It can be based on hardware devices or software procedures.
Revocation or suspension of a certificate	It is the operation with which the CA cancels the validity of the certificate before its natural expiration.
Applicant	It is the person who is requesting Aruba PEC S.p.A. the issuance of a certificate.
Qualified electronic seal	An advanced electronic seal created by a qualified electronic seal creation device based on a qualified certificate for electronic seals
Holder	It is the owner of the service.

1.6.2 Acronyms

CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Digital Administration Code (Legislative Decree no. 82/2005)
CP	Certificate Policy
CRL	Certificate Revocation List
CDRL	Local Registration Centre
CSP	Certification Practice Statement

FQDN	Fully-Qualified Domain Name
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identification and Authorization
IR	Identification Manager
OCSP	On-line Certificate Status Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
QSCD	Qualified Signature-Creation Device
QSealC	Qualified Electronic Seal Certificate
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority
TLS	Transport Layer Security
TSL	Trust Service Status List
TSP	Trust Service Provider

1.7 Riferimenti normativi

[BR] CA/Browser Forum, “Baseline Requirements Certificate Policy for the Issuance and Manage-ment of Publicly-Trusted Certificates”. (https://cabforum.org/baseline-requirements-documents/)

[EVGL] CA/Browser Forum, “Guidelines For The Issuance And Management Of Extended Validation Certificates”. (https://cabforum.org/extended-validation/)

2. PUBLICATIONS AND REPOSITORY

2.1 Repository

The term "repository" means the on-line archive by way of which the CA makes public and freely accessible the necessary information to the parties participating in the PKI (Applicants, Holders, delegated RAs, RPs, etc.), in compliance with this CPS.

The Aruba PEC repository is made up mainly of the CA website (https://www.pec.it) and other websites referenced by it. For some needs, a directory server may also be used.

The CA manages the repository on its own behalf and is directly responsible for it.

The repository is normally accessible continuously (24/7).

2.2 Information published on certificates

The CA publishes at least the following information on its website:

- Certification Practice Statement (CPS)
- PKI Disclosure Statement (PDS)
- General Contract Conditions

- CA Certificates
- Forms

In addition, lists of suspended and revoked certificates (CRL) are also published.

2.3 Time periods or frequency of publications

This CPS and the attached documentation are published on the CA website upon each update.

Regarding the publication of the CRLs, refer to §4.9.7.

2.4 Access control

Access to the repository in "read-only" form is completely unrestricted for anyone.

Access to the repository in "writing", that is, for the publication of new or updated information, is only granted to Aruba PEC.

3. IDENTIFICATION AND AUTHENTICATION (I&A)

3.1 Name of holders

3.1.1 Types of names

The Holder is identified in the certificate by way of a Distinguished Name (DN), in the Subject field, in accordance with the ITU-T X.500 standard (ISO/IEC 9594). The rules for assigning a value to the DN attributes comply with the requirements and recommendations of the applicable ETSI EN standards, concerning the profiles for issuing certificates to natural persons and legal entities, and the consequent RFC 5280 specifications. In particular, certificates issued in accordance with this CPS comply with the following standards:

- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

3.1.2 Need for the name to be significant

The identification details of the Holder (natural person or legal entity) of the certificate are inserted clearly in the Subject field, without prejudice to the provisions of §3.1.3.

In the case of certificates issued to a natural person, the Subject field contains at least the following attributes:

- countryName (OID: 2.5.4.6)
- givenName (OID: 2.5.4.42)
- surname (OID: 2.5.4.4)
- commonName (OID: 2.5.4.3)
- serialNumber (OID: 2.5.4.5)

In addition, the title attribute (OID 2.5.4.12) may be present, which is used to specify the title and professional qualification of the Holder.

In the case of certificates issued to a natural person associated with an organization, the Subject field always contains the following additional attributes, in addition to those stated above:

- organizationName (OID: 2.5.4.10)

- organizationIdentifier (OID: 2.5.4.97)

If the title attribute is also present, it may indicate the titles, duties or company position held by the Holder in the organization.

As to certificates issued to a legal entity, the Subject field contains at least the following attributes:

- countryName (OID: 2.5.4.6)
- organizationName (OID: 2.5.4.10)
- organizationIdentifier (OID: 2.5.4.97)
- commonName (OID: 2.5.4.3)

In all cases, the Subject field also contains the dnQualifier attribute (OID 2.5.4.46).

In addition, for QWAC certificates, all requirements set out in the [BR] and [EVGL] must be met. In particular, certificates must contain one or more elements in the Subject Alternative Name (SAN) extension, in which each element must be a fully qualified domain name (FQDN).
In the electronic seal certificates to be used for the purposes set forth in AgID [Agency for Digital Italy] Resolution No. 157/2020, the Subject Alternative Name (SAN) extension, populated as required by the aforementioned resolution, is also always present.
In the electronic seal certificates, the countryName attribute (OID: 2.5.4.6) specifies the country in which the legal person (registered office) is established.

3.1.3 Anonymity and pseudonyms of holders

In the event that the request is made to insert a pseudonym in the certificate, instead of the applicant's real data, the CA reserves the right to evaluate the admissibility of the request on a case-by-case basis.

If a pseudonym is used, this is clearly identified as such in the certificate by way of the specific pseudonym attribute (OID 2.5.4.65) in the Subject field. In this case, the givenName, surname and serialNumber are omitted from the Subject field.

Pseudonyms are not allowed in QWAC certificates, which for compliance with the [BR] and [EVGL] must contain the official (i.e. registered) name of the Holder or a verified "Doing Business As" (DBA).

3.1.4 Rules for interpreting names

Regarding the rules for interpreting names, the ITU-T standard relating to directory services is followed (ITU-T X.500 or ISO/IEC 9594), also taking into account the [BR] and [EVGL] as far as QWAC certificates are concerned.

3.1.5 Uniqueness of names

In order to ensure the distinctiveness of the certificate's Subject field (Holder's identification), in compliance with ETSI EN 319 412 guidelines concerning certificate issue profiles, the Subject field contains specific identification attributes based on the nature of the respective Holder.

If the holder is a natural person, distinctiveness is guaranteed by entering the **serialNumber** attribute (OID: 2.5.4.5) in the certificate's Subject field. Normally, this attribute contains the natural person's national ID number **(TIN)** and the ISO 3166 code of the country that issued it. *If the holder does not*

possess a national ID number, the holder's **passport** or **identification card** (ID) number may be used in its place. In any case, the **serialNumber** attribute is encoded in accordance with the ETSI EN 319 412-1 standard.

If the holder is a legal entity or is associated with a legal entity, its uniqueness is ensured by entering the **organizationIdentifier** attribute (OID: 2.5.4.97) in the Subject field. Normally, the **organizationIdentifier** attribute contains the legal entity's **VAT number** and the ISO 3166 code of the country that issued it. If the legal entity does not have a tax identification number, a different, unique identification code for the organization may be used in its place. In any case, the **organizationIdentifier** attribute is encoded in accordance with the ETSI EN 319 412-1 standard, i.e. as required by AgID Notice no. 18/2021.

In the particular case of QWAC certificates, which are issued to legal entities, the uniqueness of the holder organization's name is obtained by inserting the **serialNumber** attribute of the Subject in compliance with the [EVGL], while the **organizationIdentifier** is encoded as stipulated in AgID Notice No. 18/2021, except where otherwise stipulated in other regulations.

For qualified electronic seal certificates (QSealC) or qualified website authentication certificates (QWAC) intended for payment service providers pursuant to the PSD2 Directive, the **organizationIdentifier** attribute is always present and is populated in accordance with the ETSI TS 119 495 standard.

3.1.6 Recognition, authentication and role of registered trademarks

The CA does not carry out checks on the use of trademarks and registered trademarks, which are the exclusive property of the respective holders.

Certificate applicants represent and guarantee that their submission to the CA and use of information relating to the certificate request do not interfere with or harm the rights of any third party, in any jurisdiction, concerning the trademarks, service marks, trade names, corporate names and any other intellectual property right, and that they shall not attempt to use the certificate (and the information contained therein) for illegal purposes, including therein unlawful interference to the company's contractual or potential advantages, unfair competition, actions intended to damage the reputation of another person, misleading advertising and actions that create confusion regarding individuals or legal entities. Certificate holders and applicants agree to hold the CA harmless and compensate it for any loss or damage resulting from such interference or violation.

3.2 Initial identity validation

This section describes the procedures for initial identification of the requesting party´s identity (natural person or legal entity) upon applying for a qualified certificate.

Some of the following paragraphs apply only to *qualified website certificates* (QWAC), in which case the CA complies with the requirements of the ETSI EN 319 411-2 standard, with particular reference to the provisions of the [EVGL] referred to in the same standard.

3.2.1 Demonstration of possession of the private key

The demonstration of the Applicant's possession of the private key (corresponding to the public key to be inserted in the certificate) is based on verification of the CSR (Certificate Signing Request). In fact, the Applicant's public key must be sent to the CA as a CSR in PKCS#10 format (RFC 2314). See also section 4.1. The CA verifies that the electronic signature contained in the CSR is valid before accepting the CSR.

3.2.2 Validation of the identity of organizations

3.2.2.1 Identity

In the case of electronic signature or electronic seal certificates, the following shall apply:

- The request to issue a qualified certificate for a legal entity (certificate for electronic seal) falls under the responsibility of the natural person representing the legal entity, who is identified in accordance with the same procedures specified for natural persons (see § 3.2.3).
- The legal entity's powers of representation, as declared by the requesting natural person, must be demonstrated by providing the CA (or the RA) with appropriate documentation issued by an official database (e.g. Companies Registry).

In the case of website certificates (QWAC), the following shall apply:

- The CA verifies the identity of the requesting organization, its correct name and its unique identification code (e.g. VAT number where applicable or the business registration number in the relevant companies registry in other cases), as well as the physical address of its head office, by consulting reliable independent sources.
- The request for the issuance of the certificate must be signed by a "Contract Signer" authorized by the Requesting Organization; such authorization may be self-declared by the signer in accordance with the [EVGL]. The signer does not need to be a legal representative of the Requesting Organization. The individual identity of the contract signer is verified in accordance with the procedures set out under §3.2.3.

3.2.2.2 DBA or Tradename

In the case of website certificates (QWAC), if the Subject of the certificate must include a "Doing Business As" (DBA) or a trade name, the CA shall verify the Requesting Party´s right to use such DBA or trade name through one of the methods set forth in the [EVGL].

3.2.2.3 Country Verification

In the case of website certificates (QWAC), the CA shall verify that the country declared by the Requesting Party is correct through one of the methods set forth in the [EVGL].

3.2.2.4 Domain Control Verification

In the case of website certificates (QWAC), the CA verifies that all FQDNs to be included in the certificate are owned or physically controlled by the Requesting Party or one of its affiliates (for example, a parent company or subsidiary). This verification is carried out using at least one of the methods permitted by the Baseline Requirements of the CAB Forum [BR].

3.2.2.5 Further verifications

In the case of website certificates (QWAC), before issuing the certificate, the CA carries out - in addition to that mentioned in the previous sections – all the additional verifications set forth in the [EVGL], as required by the ETSI EN 319 411-1 standard.

3.2.3 Validation of individual identities

Before proceeding with the issue of the requested certificate, the CA must ascertain the applicant's identity. In order for the CA service to be more widespread in the country and to simplify it, if possible, by way of remote identification mechanisms, the identification and authentication functions may be performed using various procedures:

- "visual" (or "in-person") identification carried out directly by the CA, by external appointed parties (RAs) or by a Public Official (**Procedure 1**);
- remote identification, in compliance with anti-money laundering laws, based on identification carried out by a Financial Intermediary or by another Financial Activity Practitioner (**Procedure 2**);
- remote identification by way of a qualified electronic signature or based on identification undertaken by another Qualified Trust Services Provider (**Procedure 3**);
- remote identification by means of a Health Insurance Card/National Service Card (TS-CNS), National Service Card (CNS) or National Identity Card (CIE), or based on the identification process carried out by the corresponding Issuing Body, or identification by means of a national electronic identification (e-ID) scheme, or as notified by a Member State in accordance with article 9 of the eIDAS regulation (**Procedure 4**);
- remote identification by video conference, carried out by the CA or by appointed parties (**Procedure 5**);
- identification of the employee/collaborator/agent/etc. through the identification already carried out by the employer during the hiring and contract stipulation phase (**Procedure 6**).

The various I&A procedures mentioned above are described below. In the descriptions below, the term, "Applicant", refers to the party (natural person) who is requesting the certificate on his or her own behalf or on behalf of the organization that he or she represents.

For Italian citizens and foreign citizens resident in Italy, at least the following identity and recognition documents equivalent to each other are admitted, as provided by art. 35 of Presidential Decree no. 445 of December 28, 2000[1]:

- identification card
- passport
- driving licence
- ATe and BT cards issued by the Public Administration.

Applicants with citizenship other than Italian, for identification purposes, must show one of the documents expressly permitted by the Annex to this SPC called "Approved identity documents".

[2] In the event that the same requesting party has multiple certificates (for example, for different roles or for service reliability reasons), this code will be different for each certificate.

Procedure 1

Identification requires the physical presence of the Applicant, who must be at least 18 years old, before a party authorized to perform identification, which undertakes to ascertain the identity thereof through a formal and substantial check of a complete, valid identification document, displayed in original form by the Party him or herself.

Identification operations (and respective registration) of Applicants are carried out, based on the reference organizational model, by one of the following authorized parties for identification purposes:

- directly by the CA;
- by a third party referred to as the Local Registration Centre (CDRL) before an appointee of the CDRL referred to as the Registration Operator (OdR);
- by a third party referred to as the Identification Manager (IR);
- by a Public Official based on the provisions of the legislation governing their activity, including the provisions of Italian Decree Law no. 143 of 3 May 1991, as subsequently modified and amended

The CDRLs may operate after stipulating a mandate with the CA in which the third party indicates its own personnel, which will be referred to as the Registration Operator (OdR) and will be required to operate within the context of the operational registration practices. The authorization and subsequently the qualification of the OdRs as fit for identification, registration and issue purposes, takes place by means of a training course and by passing a written test. After signing by the respective legal representatives of the CA and of the CDRL, and after qualification of the OdRs, the CA makes available to the OdRs the secure electronic tools to enable identification, registration and issue of certificates. The rights of access to the secure electronic tools and the operations of the OdRs are under the constant control of the CA.

The IRs may operate after the conclusion of a mandate directly with the CA, or through the appointment of a CDRL, within the context of the operational practices defined by the CA and limited to the performance of identification and registration activities.

Procedure 2

The identification procedure is carried out by a Financial Intermediary or a Financial Activity Practitioner which, in compliance with current anti-money laundering laws, in application of Directive 2005/60/EC, is required to correctly identify customers; the Applicant's identification details, which are provided under its own responsibility in accordance with Italian Legislative Decree 231/07 and subsequent amendments (with specific reference to Italy) and which are collected by the Practitioner upon identification, are used directly for issuing certificates subject to the following (to be completed by the Applicant):

- acceptance of the contractual conditions for the issue of the certificate and any tools for signing;
- approval and confirmation of registered personal data.

Practitioners, which are subject to identification and due diligence obligations, shall acquire data in accordance with independently established procedures in compliance with anti-money laundering laws in force on the date of identification. This identification procedure requires that the Practitioner

operates as a delegated third party (CDRL) based on specific agreements made with the CA, in accordance with this CPS and any specific instructions contained therein. In particular, the Applicants, who have already been contracted by the Recipient of the obligations or in any case involved in the contracting process itself, must:

- be identified in accordance with current Anti-Money Laundering laws;
- they are monitored on an ongoing basis;
- have strong authentication tools with two or more factors for accessing online services provided by the Practitioner, or have two or more personal contact channels guaranteed by the Practitioner for communications and activation and authentication procedures for the Signature Service, to be verified by the Practitioner as part of the aforementioned identification and control phases;

as such, in order to register the request to issue the qualified certificate, the identification data already acquired by the same Practitioner during the aforementioned identification procedure of the Applicant may be used.

In accordance with the provisions of the internal procedures and the anti-money laundering legislation in force, the Practitioner carries out all the operations necessary for the correct identification and registration of the Applicant, verifying their identity through checks on the documents and personal data provided by them, and carrying out specific checks on them such as consistency, authenticity and acceptability on the main databases for the purposes of the continuation of the entire process.

Procedure 3

Identification is based on the identification (already) undertaken by another Qualified Trust Service Provider for the issue of a qualified certificate in accordance with eIDAS Regulation. The Applicant's identity is ascertained through electronic identification procedures based on obtaining an application form or another data set in electronic form (nevertheless, submitted by the CA), electronically signed with a still valid qualified certificate, contained on the secure device (QSCD) in possession of the respective Party.

Procedure 4

Identification is carried out by means of electronic identification and authentication tools issued as part of an electronic identification scheme included on the list published by the Commission, in accordance with article 9 of the eIDAS Regulation; with specific reference to Italy, identity verification of the Applicant requesting a qualified certificate shall use an SPID authentication procedure with level 2 or level 3 credentials in accordance with the measures and specifications outlined by the Agency (AgID) on a case-by-case basis.

Procedure 5

in accordance with these procedures, identification is carried out by means of a video conference system, requiring the Applicant, who must be at least 18 years old, to have a webcam properly connected to a PC with a functioning audio system.

Identification operations (and respective registration) of Applicants are performed, based on the organizational model of reference, by one of the following authorized parties for identification purposes (hereinafter, Operator):

- directly by the CA;
- by a party appointed by the CA, referred to as the Local Registration Centre (CDRL);
- by a party appointed by the CA, referred to as the Identification Manager (IR).

The Operator follows specific procedures - which for security reasons are restricted - intended to ensure the authenticity of the course of the video conference session. Among other things, the Operator asks the Applicant to produce a valid identification document from among those indicated in Procedures 1. The Operator may refuse the admissibility of the document presented by the Applicant if it is judged that it lacks the listed characteristics. The Operator may also suspend, or not initiate, the identification process in the event that the audio/video is of poor quality or deemed in adequate for meeting the requirements of Art. 24 of EU Regulation No. 910/2014 or art. 32, paragraph 3, letter a) of the CAD.

At the time of identification, the Applicant must confirm:

- acceptance of the contractual conditions and personal data processing for the activation of the signature service and for the issue of the digital certificate;
- the registered identification and personal data that will also be used for issuing certificates.

The videoconference session is recorded in full (audio + video). To ensure the protection and processing of personal data in accordance with the related applicable legislation, Aruba adopts appropriate measures and tools to protect data subjects and makes the information that defines the data processing methods available.

The registration data, consisting of the audio-video file and structured metadata in electronic format, are stored as specified in §5.5 of this CPS.

Procedure 6

Through this method of identification, the Certification Authority takes advantage of the identification procedure already performed by the employer for the signing of the contract, after verifying the operational identification and authentication procedures used by the company/organisation. Similarly, is considered valid in accordance with the following procedure of identification if performed by the employer in the context of an agency relations' activation, verifying the operational identification authentication procedures used by the employer. This procedure provides for the granting by the CA a mandate with representation to the employer, which then acts as RA. The Certificates issued according to this method of identification can be used for the purposes specified by the employer and reported accordingly in the specific limit of use of the certificate. The registration data for this mode of identification are stored by the CA in analog or electronic format.

3.2.4 Unverified information

Some information ancillary to activation and account management procedures, such as the email address and mobile phone number, are generally not verified by the CA, which assumes no responsibility in the event that such information is provided incorrectly.

3.2.5 Verifying the authorization of requests

All information specified in §3.2.5 and §4.2.1 may be subject to verification by the CA, which reserves the right - if the submitted documentation features irregularities - to reject the request. In the event of rejection of the request, the CA informs the Applicant at once, stating the reasons for the rejection. An Applicant whose request has been rejected may make a new request. In any case, the CA remains exempt from any liability, loss and/or damage, whether direct and/or indirect, that may result from such rejection.
In the case of website certificates (QWAC), the CA shall verify the name, title and authority (representation) of the Contract Signer - and the Certificate Approver, if a different person - in accordance with the [EVGL]. For the purposes of this verification, Aruba PEC normally requires a specific declaration by the Contract Signer, which must be signed using the methods indicated in section 4.1.2.

3.2.5.1 Professional qualifications, title and organization

Pursuant to art. 28 of the CAD, the Holder may obtain, independently or with the consent of any "Third Party", the inclusion in the certificate of information on their qualifications, such as membership of professional associations or boards, the status of public official, registration in lists or possession of other professional qualifications, or representation powers. This information, if applicable, is entered in the **title** attribute of the Subject field of the certificate (see §3.1.2).

In this case, unless otherwise agreed by the CA and the Board to which an entity belongs (if applicable), in addition to the documentation and the necessary identification information (see §4.2.1), the Applicant must also produce appropriate documentation to prove the actual existence of the specific title (or professional qualification), possibly certifying it through *self-certification* pursuant to art. 46 of Presidential Decree no. 445/2000. This documentation must not be earlier than 10 (ten) days before the registration date.
Pursuant to AgID Resolution no. 121/2019, in the event that the title is *self-certified* by the Applicant, information about the organization with which the Applicant may be associated will not be included in the certificate. The name and the identification code (e.g. VAT number) of the organization will instead be included in the certificate if the organization has specifically requested or authorized the issue of the certificate, even if no specific title has been indicated. In this case, the CA carries out a check on the formal validity of the documentation submitted by the Applicant.

The CA reserves the right to make the inclusion in the certificate of the information falling in this category conditional upon the signing of specific agreements with the individual entities, which are responsible for managing and holding professional registers, lists and/or rosters, due to the rules on procedures for confirming the Holder's Title and for fulfilment of what is expected of them as an "Interested Third Party".

3.2.5.2 Usage limits and value limits

Pursuant to art. 28 of the CAD and Art. 13 of the eiDAS Regulation, the Holder may ask the CA to include in the certificate the value limit of unilateral acts and contracts for which this certificate may be used. This information is entered in the **QcStatements** extension of the certificate (see §7.1.2). The desired value limit must be expressed as a whole number, with the indication of the currency (e.g. "EUR").

Pursuant to the CAD, the CA is not liable for damages resulting from the use of a qualified certificate that exceeds the limits set by it or resulting from exceeding the limit value.

With regard to the limits on use, pursuant to art. 28 of the CAD, the CA guarantees the issue of certificates with the following limitations on use:

- "I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued".
- "Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signatures".
- "L'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto). The certificate may be used only for relations with the (state the subject)".

Here again the CA is not liable for damages resulting from the use of a certificate that does not comply with the usage limits stated in the certificate itself.

A request to insert usage limitations different from those indicated above will be assessed by the CA on a case-by-case basis with referent to the law, technical aspects and interoperability. In any case, the text of the usage limitation may not exceed 200 characters (including spaces and punctuation) and must be expressed in both Italian and English (only English is allowed in the case of closed groups of users who only use English).

The qualified certificate issued by means of SPID digital identity contains OID 1.3.76.16.5, registered by the Agency, with the following description: "Certificate issued through the Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity." Any qualified certificate issued following a request signed with a qualified electronic signature for such qualified certificate will, for their part, contain the aforementioned OID.

3.2.6 Interoperability criteria

Aruba PEC reserves the right to enter into agreements with other Trust Services Providers, limited to specific contexts, provided that these Providers are Qualified pursuant to EU Regulation no. 910/2014.

3.3 Identification and authentication of renewal requests

3.3.1 Identification and authentication for ordinary renewal of keys

The procedure followed for the renewal of the certificate (see §4.6) is substantially identical to that followed for the issue of the first certificate. If the holder is already registered, however, a new registration is not required unless changes have been made to his or her data (changes that the Holder is nevertheless required to report promptly to the CA).

As of from 2 months before the certificate expires, the Holder receives (at the email address provided to the CA or RA during registration), an expiration notice e-mail, containing instructions to start the certificate renewal procedure.

With regards to electronic signature or electronic seal certificates, based on the means made available by the CA, the renewal procedure requires, among other things, the Holder to sign digitally a renewal request form using the private key corresponding to the certificate to be renewed.

In the case of website certificates (QWAC), the CA may require the Holder to follow the same identification and authentication procedures used for the initial issuance of the certificate, depending on the age of the validation data used for the initial issuance (in accordance with the [EVGL]).

A request to renew a certificate for electronic seal falls under the responsibility of the natural person representing the legal entity holding the seal (see § 3.2.2).

3.3.2 Identification and authentication for renewal of keys following revocation

After the revocation or expiration of the certificate, the renewal of the certificate is not possible: the certificate must be issued from scratch in accordance with the procedures described for issuing the first certificate.

3.4 Identification and authentication for revocation requests

Suspension or revocation of the certificate takes place in accordance with the methods and procedures described in §4.9.

The revocation (or suspension) of the certificate may be requested by means of an on-line procedure or by forwarding to the CA (or to an RA thereof) a formal request by e-mail (off-line request) or by contacting the RA who issued the certificate. In the former case, the Holder is identified by entering his or her national ID number (or another personal identification code for foreign citizens not possessing a national ID number) and is authenticated by entering the confidential emergency code ("user code") that was provided to him or her upon registration or issue of the certificate. In the second case, the request must be signed with the Applicant's digital or handwritten signature and (in the case of a handwritten signature) accompanied by a scan of the identity document; in the case of a digital signature, both the advanced electronic signature and the qualified electronic signature are accepted in accordance with the eiDAS Regulation. In the third case, the Applicant may follow the procedure defined in more detail in Chapter 4.9.

4. OPERATIONAL REQUIREMENTS FOR CERTIFICATE MANAGEMENT

4.1 Certificate request

4.1.1 Who may request certificates

A qualified certificate for a natural person may be requested by the interested party (future Holder) by applying directly to the CA (https://www.pec.it) or to one of its RAs (CDRL).

A request may also include an "interested third party", i.e. the party that consents to the inclusion of a title in the certificate (as required by art. 32 of the CAD) or the organization that requests or authorizes the issuance of the holder's certificate (see the AgID Resolution no. 121/2019).

A qualified certificate for a legal entity may be requested by the natural person representing the legal entity, by applying directly to the CA or to an RA.

4.1.2 Request process and responsibility

In general, a request for a qualified certificate always involves the following steps:

- a formal request from the Applicant, with simultaneous acceptance of the General terms and conditions of the CA and of this CPS;

- identification and authentication (I&A) of the Applicant by the RA operator (it may be an external RA, i.e. a CDRL: see below);
- registration of the request on the CA's systems, by the RA operator;
- the generation of the key pair for the Applicant (future Holder); (this operation may also take place at an earlier time)
- sending the public key to the CA in the established format (see §3.2.1), by the Applicant himself or herself or the RA, through secure channels established by the CA.

The technical and operational details may vary in accordance with the I&A procedures (see chap. 3), in accordance with the sending channels and IT tools used for registration and in accordance with the context of use of the requested certificates.

In all cases, at the request stage the Applicant needs to:

a) confirm having viewed this CPS and having understood and accepted it;

b) accept explicitly the obligations established by current laws and by the contract with the CA;

c) consent to the processing of personal data in compliance with current legislation.

In order to extend the operational possibilities, the registration functions may also be carried out by designated third parties, with offices throughout the country, on the basis of specific agreements entered into with the CA (see §1.3.4). These third parties (also referred to as "Local Registration Centres", abbreviated to CDRL) operate in accordance with procedures agreed with the CA.

The CDRLs are accountable to the CA for the correct and secure identification of the applicants, as well as for processing their data in full compliance with privacy legislation and digital signature legislation. In turn, the CA remains fully responsible, for the applicant identification and registration operations, whether it carries them out or they are carried out by the CDRLs.

In the case of website certificates (QWAC), the following additional roles of the Requesting Party, as defined in the [EVGL], are required and applied as part of the request process:

- Certificate Requester (the natural person submitting the request to the CA)
- Certificate Approver (the natural person approving the request on behalf of the Requesting Party)
- Contract Signer (the natural person signing the Service Agreement or Subscriber Agreement)

The Requesting Party may authorize one person to hold two or more of the above roles and/or may authorize more than one person to hold the same role.

For website certificates (QWAC), the certificate request must be submitted by an authorized Certificate Requester (or "technical contact person") and must be approved by an appropriate Certificate Approver, in accordance with the [EVGL]. The certificate request must be accompanied by a Service Agreement (or Subscriber Agreement) signed by an appropriate Contract Signer pursuant to the

[EVGL], as set forth above in Chapter 3. The Service Agreement must be signed by the Contract Signer in one of the following ways:

- by handwritten signature in the presence of an Aruba PEC representative (who countersigns as a witness);
- by handwritten signature authenticated by a public official (e.g. a notary); (*)
- by means of a valid qualified electronic signature, in accordance with European regulations.

(*) In this case, the authenticated copy of the Service Agreement sent to the CA must be the original. The certificate request shall not be processed until Aruba PEC has received and verified this original.

4.1.2.1 Information that the Applicant must provide

A request for registration and certificate issue is formalized by way of a "Registration and Certificate Request Form" (the exact name of the form may vary) available on the CA website or through its sales channels. For the sake of brevity, this document is referred to hereinafter as the "application form".

In some cases, the application form is generated in PDF format by the RA electronic system and completed in advance with the Applicant's personal data, then made available to the Applicant and to the RA operator for both of them to sign.

During registration, the Applicant must provide with at least the following documentation:

a) The application form completed in all its mandatory parts;

b) only in the case of a request for a certificate which is also meant to contain the title or professional qualifications of the holder (e.g. lawyer, engineer, doctor, etc.), or the position held in third-party organizations, the documentation proving possession of the professional qualifications or of the position held, powers of representation, etc.;

c) only in the case of a request for a certificate for an electronic seal, the documentation necessary for proving the identity of the legal entity (which will become the Holder of the certificate) and that relating to the existence of the powers of representation of the natural person requesting the issue thereof.

The application form must be signed by the Applicant, with a handwritten or electronic signature . In the case of an electronic signature, the CA accepts the following types of electronic signature:

1) advanced electronic signature based on a qualified certificate or qualified in accordance with the eIDAS Regulation (with a certificate not necessarily issued by this CA);

2) simple electronic signature affixed by means of the authentication certificate on the Applicant's CIE/CNS/CRS (Electonic Identity Card/National or Regional Services Card) card;

3) electronic signature based on confidential data known only by the Applicant, as well as by the CA (for example a dynamic password (OTP) that the CA sends to the Applicant's mobile phone (by SMS or other means);

4) electronic signature affixed by means of graphometric techniques;

5) other forms of electronic signatures or advanced electronic signatures in accordance with the laws currently in force.

With regard to point 5, the CA reserves the right to accept electronic signatures only in such cases in which it ascertains the integrity and security of the specific procedures authorised and implemented within the identification process, or when the acceptance or signing procedure is made available by the CA itself.
In cases of visual identification of the Applicant, the recognition appointee shall digitally countersign the form (or provide other reliable electronic evidence attesting to the identity of the operator that undertook recognition). In such case, the form also includes the appointee's declaration that the Applicant's electronic signing occurred in his/her presence.

If a qualified certificate is requested for a **natural person**, the Applicant must provide the following information:

- given name and surname (*)
- date of birth
- municipality, province and country of birth
- national ID number or similar identification code (see §3.1.5)
- address of residence, possibly abroad
- e-mail address (for sending communications)
- details of the identification document presented for identification: type, number, issuing body and issue date thereof
- mobile phone number (mandatory only for some procedures)
- any professional qualifications (*)
- any powers of representation (*)
- any pseudonym, to be inserted in the certificate in place of the given name and surname

(*) All details marked with an asterisk are included in the certificate, except in the case of the use of a pseudonym (see §3.1.3).

In the event of a request for a qualified certificate for a **legal entity**, the Applicant (legal representative or person possessing a power of attorney from the legal entity) must provide the following information:

- name of the legal entity (*)
- country where the legal entity has its registered office (*)
- VAT number or Tax Code (*) for Italian organizations, or VAT code or other unique identification code of the organization for foreign Parties (*) (see §3.1.5)
- applicant's given name and surname
- applicant's national ID number or similar identification code (see §3.1.5)
- the applicant's e-mail address (for sending communications)

- details of the applicant's identification document: type, number, issuing body and issue date thereof;
- mobile phone number (mandatory for some procedures).

(*) All details marked with an asterisk are included in the certificate.

4.2 Processing of the request

4.2.1 Fulfilment of the Identification and authentication functions

For the procedures for carrying out the I&A functions, refer to sections §3.2 and §4.1.2.

During the registration and certificate application phase, some confidential personal codes that are necessary for the following may be provided to the Applicant by the RA operator:

- activating and unlocking the signature device (PIN and PUK codes)
- activating the remote signature procedure (e.g. password, OTP)
- requesting the suspension or revocation of the certificate ("user code")

These codes may be provided to the Holder in physical form (e.g. printed on halftone paper in a sealed envelope, or as a scratch-card), separately from the signature device, or in electronic form (e.g. sent by SMS or e-mail). In some cases, (e.g. remote signature) some of these codes may be set by the Holder. As applicable, except as provided for in Appendix D of this document, the certificate suspension or revocation code may also be provided to the Holder during generation of the certificate (see §4.3.1).

4.2.2 Approval or rejection of requests

The CA or the delegated third party (RA/CDRL) may reject the request in the event that the information provided by the Applicant is deemed unreliable, inaccurate, incomplete or inconsistent; in the event

of doubts about the identity of the Applicant (or of the legal person presumably represented by him or her) or for any other reason that constitutes non-compliance with this CPS.

4.2.3 Request processing times

The request processing times, from Applicant registration to the issuance of the certificate, depend on the request procedures as followed (see §3.2.3), on any need for more detail concerning the information provided by the Applicant and on the need to deliver the signature device physically (if applicable, and in accordance with the type of device) and/or to activate it.

4.3 Certificate issuance

4.3.1 CA actions during the issue of the certificate

The issue of the certificate follows an appropriate request made as described in sections 3.2 and 4.1. Generation of the certificate takes place in compliance with current laws and with the ETSI standards of reference, using a process organized in different phases and based on secure communication channels.
During the certificate issuing process, following identification and authentication (I&A) of the Applicant, the CA carries out the following actions (under which "CA" means not only the certificate generation system but also the systems and/or websites that interconnect the RA and/or the Applicants):

1) where provided, it activates a procedure that generates a pair of keys within the Applicant's signature device (or within an HSM in the case of a certificate request by remote signature) and the corresponding CSR, which is automatically sent to the CA;
2) through a secure (encrypted and authenticated) channel, it receives the Applicant's CSR;
3) it verifies the Applicant's possession of the private key and the correct functioning of the key pair, through cryptographic verification of the CSR;

4) it generates a unique identification code[2], within its own database, which will be inserted in the dnQualifier attribute (OID: 2.5.4.46) of the certificate's Subject field (see §3.1.5);
5) it generates the certificate (*) using the public key extracted from the CSR and the Holder's identification data (previously collected and stored during registration);
6) it stores the certificate in its database, recording the event in the audit log;
7) if required, it publishes the certificate in the specific repository, recording the event in the audit log;
8) it sends the certificate to the Holder (or to the RA) or directly to the signature device (if any) through an (encrypted and authenticated) secure channel; if the Holder's private key is on a signature device, at the same time a procedure is activated that installs the certificate on the device (or within the HSM in the case of a certificate for remote signature); the customization of the device is thus completed (event recorded in the audit log). In the case of a personal signature device (e.g. smartcard), this procedure can also involve modifying the PIN and PUK codes of the device by setting them to the established values (see §4.2.1);
9) in the case of signature keys generated by the holder within HSM, it associates the strong authentication credentials already held by the Owner and used during the generation of the key pair (for example OTP or biometric data) with the Holder. Access to the key pair is also subject to the knowledge of a username and password previously chosen by the owner (in the case of the OTP) or to the physical presence of the holder before an appointee of the CA (in the case of identification based on biometric techniques);
10) if necessary (or if not already undertaken during registration), it generates a confidential emergency code to be used to authenticate any certificate suspension or revocation request (pursuant to current laws);
11) it provides the Holder with personal codes and the emergency code through secure procedures that depend on the type of signature device used (if any), on how the Holder's keys are generated and on the Holder registration procedures:
    a) in the case of keys generated by the CA, the personal codes and the emergency code are provided to the Holder by sending a closed, sealed envelope (or scratch-card) containing this information or through codes transmitted via SMS and/or, email;
    b) in the case of keys generated by the CDRL, the personal codes and the emergency code are provided to the Holder by delivering a closed, sealed envelope (or scratch-card) containing this information or through codes transmitted via SMS and/or, email;

[2] In the event that the same requesting party has multiple certificates (for example, for different roles or for service reliability reasons), this code will be different for each certificate.

c) in the case of keys, under the control of the Holder, generated within an HSM, there are two possibilities:

- The personal codes for activation of the secure device and the emergency code are already in the possession of the Holder. The username and password are set by the Holder during generation of the key pair. The OTP credentials and the emergency code have already been delivered to the Owner at the time of identification thereof.
- the personal activation codes for the signature device will be transmitted to the user, who must change them the first time he/she logs in (see step 8). The holder is also notified of the emergency code through secure procedures.

(*) In the case of signature keys generated by the CA in bulk, the certificate is issued in a suspended state and must be activated subsequently through a temporary OTP code sent to the Holder's mobile phone.

If conditions are met that prevent the generation of the certificate, the system rejects the request and signals the event to the RA operator or to the Applicant.

4.3.2 Certificate issue notification for the holder

The issuing of the certificate is notified to the registration operator (CA appointee or OdR) or directly to the Holder, in accordance with the request procedures; in the first case, the operator reports the issue to the Holder upon delivery of the personalized signature device (i.e. containing the certificate). In some cases, the Holder may be notified by e-mail at the e-mail address provided at the time of registration.

4.4 Certificate acceptance

4.4.1 Actions that constitute acceptance of the certificate

Use of the private key constitutes acceptance of the certificate. In addition, the certificate is considered accepted at the time of its installation on the Holder's signature device if the contract expressly provides for this.

4.4.2 Publication of the certificate by the CA

Publication of the certificate, if expressly requested, includes the following steps:

- the certificate is published in the certificates repository; the moment (date/time) of publication is confirmed by a reliable time reference;
- publication of the certificate is recorded in the audit log.

Publication of the certificate is not a standard part of the CA service described here and does not happen "by default". Mere consent to publication by the applicant does not necessarily lead to the publication of the certificate, unless it is provided for in specific agreements with a particular customer.

4.4.3 Notification of certificate issue to other parties

No provision.

4.5 Use of the key pair and certificate

4.5.1 Use of the key pair and certificate by the holder

The Holder of the signature certificate is required to adopt all the appropriate organizational and technical measures to avoid harm to others and to keep and use his or her private key and his or her signature device (if any) with reasonable care. The Holder is therefore required to protect the privacy of his or her private key, avoiding disclosure to third parties of the personal identification code (e.g. PIN) for activation thereof, providing to enter it in ways that do not allow viewing by other parties and keeping it in a safe place from where the signature device is kept (if any). The same care must be devoted to strong authentication devices (e.g. OTP code generators) in the case of signature keys stored within an HSM (i.e. keys for remote signature). The private key, for which the certificate was issued, is strictly personal and may never, under any circumstances, be sold or granted to third parties for use. For further details on the Holder's obligations, refer to §9.6.

4.5.2 Use of the key pair and certificate by Relying Parties

All those who rely on information contained in certificates (these subjects are referred to, for short, as "Relying Parties": RPs) have the obligation to verify that the certificate has not expired, been suspended or been revoked. The verification must be carried out on the status of the certificate at the relevant date/time for the RP, in accordance with the particular context (e.g. the current date/time, or rather the date/time of signing if this can be ascertained or inferred).

RPs may be exempt from carrying out the above-mentioned verifications only in the case of a "verified signature" certificate, in accordance with the AgID Resolution no. 63 / 2014; the examination of the certificate's CertificatePolicies extension allows the RP to determine whether it is a certificate of this type (see §1.4).

For further details on the obligations of RPs, refer to §9.6.

4.6 Certificate renewal

The renewal of the certificate applies to certificates that have not yet expired (and are not revoked) and consists of the generation of a new key pair (by the Applicant) and the issuing of a new certificate (by the CA) with a period of validity normally equal to the period of validity of the expiring certificate and with the same Holder's identifying data.

4.6.1 Circumstances for certificate renewal

The renewal process must be initiated at least 30 days before the expiry date of the current certificate. Failure to comply with this deadline requires the initiation of non-standard procedures with consequent possible delays that cannot be quantified a priori.
When requesting the certificate and accepting the contract conditions, if the Holder expresses his/her consent to the tacit renewal of the certificate, the renewal procedure is automatically initiated based on the procedures described below:

- As a result of the consent given, the Holder will receive communications (at the email address provided to the CA or RA), relating to the management of the tacit renewal (e.g. informative communications close in time to the tacit renewal and confirmation of the renewal that has occurred). At any time, the Holder may revoke consent to the tacit renewal provided through the procedures made available by the CA, for example, by accessing the Service management panel;
- the generated keys are kept within the same secure device (§ 1.4) and the same security elements are maintained.

4.6.2 Who may request renewal

Renewal may be requested by the Holder of the expiring certificate (or by its representative, if the Holder is a legal entity). Based on this CPS, only certificates issued by this CA are renewable.
The Holder may also consent to tacit renewal of the certificate during the certificate application and acceptance of the terms and conditions. Based on this CPS, only certificates issued by this CA are renewable.

4.6.3 Processing of renewal requests

As stated above in §3.3, the procedure followed for renewal is very similar to that followed for the issue of the first certificate; the Holder (or Applicant, in the case of certificates issued to a legal entity) must in any case contact the reference RA (CDRL) or the CA.

The main steps of the renewal process are:

1) completion of the certificate request form and subsequent digital signing thereof, by the Holder or by the Applicant, by means of the expiring certificate which must not be suspended or revoked;
2) sending of the aforementioned form to the reference CA or RA (CDRL);
3) the CA's verification of the correctness of the data contained in the form and of the validity of the associated digital signature;
4) generation of the Holder's new key pair and sending of the CSR to the CA;
5) sending of a corresponding new certificate by the CA;
6) sending of the new certificate to the Holder, by the CA, and its installation on the Holder's signature device (if any).

The renewal procedure is performed by the CDRL (as if it were a new issue) or directly by the user Holder through a service made available by the CA, within the scope of commercial and contractual relations established with the Holder or with the RA (CDRL), if any; also for the renewal, interaction with the Holder takes place through secure communication channels (encrypted and authenticated).
In the event of consent to tacit renewal by the Holder, the CA shall carry out the procedure provided for in point 4 of this paragraph.

4.6.4 Notification to the holder of the new issue of the certificate

The provisions of §4.3.2 apply.

4.6.5 Actions that constitute acceptance of the renewed certificate

The provisions of §4.4.1 apply.

4.6.6 Publication of the renewed certificate by the CA

The provisions of §4.4.2 apply.

4.6.7 Notification to other parties of the new issue of the certificate

The provisions of §4.4.3 apply.

4.7 Key regeneration

The regeneration of the key, not intended as renewal (i.e. replacement of keys before their natural expiration) but applicable following the expiration or revocation of the certificate, is managed as a completely new issue; therefore refer to sections 4.1 to 4.5.

4.8 Certificate modification

The modification of the certificate, not intended as renewal (i.e. replacement of keys before their natural expiration) but applicable in cases in which the Holder's identification details change, such as name, title or organization, etc., is managed as a completely new issue; therefore refer to sections 4.1 to 4.5.

4.9 Certificate suspension and revocation

Suspension and revocation of the certificate take place in compliance with the laws in force and with other applicable legislation, even if technical, in accordance with the procedures and means described below.

The revocation of a certificate causes the early and final termination of its validity.

Suspension temporarily interrupts the validity of a certificate and allows the subsequent recovery (reactivation) or the final revocation after a predefined period of time that may vary in accordance with the agreements of the CA with the Customer.

The revocation or suspension of the certificate takes place by entering the certificate's serial number in a new List of Revoked Certificates (**CRL**), which is published in such a way that all interested parties may observe the certificate status by downloading and consulting it. The same information is also made available with the **OCSP** protocol. For further details, refer to §4.10.

4.9.1 Circumstances for revocation

The CA revokes the certificate in the following circumstances:

- explicit request by the Holder and/or his or her representative, for any reason;
- explicit request by an "interested third party" in the established cases (see below);
- the certificate has not been issued in compliance with this CPS and current laws; (*)
- the Holder's identifying information contained in the certificate is no longer valid; (*)
- early termination of the contract between the CA and the Holder;
- violation of the certificate Holder's contractual obligations;
- evidence of material errors, abuses or falsifications during registration; (*)
- compromise of the secrecy of the holder's private key or of the data on activation thereof (e.g. PIN, password, OTP or other similar codes); (*)

- The QSCD on which the Holder's private key is stored loses the certification referred to in §1.4. In particular:
  if the CA becomes aware of the loss of the QSCD certification status for the certificate bearing the esi4-qcStatement-4 statement as referred to in §1.4, before the end of the

validity period of the digital certificate, it shall automatically revoke it or take measures to prevent the established use of the certificate.

Specifically, if the CA ascertains that the keys have been physically cancelled, it may reissue the certificate on another QSCD referred to in §1.4 and deliver it to the Holder via the security procedures governed by this Manual.

- loss, theft or damage of the signature device; (*)
- non-recoverable loss of the private key; (*)
- improper use of the certificate by the Holder;
- request by the Courts.

(*) In these cases, when the circumstance is detected by the Holder, the Holder **must** request the revocation of the certificate on his or her own initiative and as soon as possible; for further details on the Holder's obligations, refer to §9.6.3.

An "interested third party" may request the revocation of the certificate (in accordance with the offline procedure described in §4.9.3) only when the party's relationship with the Holder ceases or changes in such a way as to invalidate the information contained in the certificate. For example, in the event that the "interested third party" is an organization (institution, company, association, etc.) that purchased certificates intended for its employees, such organization may request the revocation of a certificate when (non-exhaustive list)

- the contracts between the organization and the certificate Holder have changed or terminated;
- there have been cases of fraud and/or disloyalty by the employee who holds the certificate;
- the title, position or corporate title of the holder (e.g. representative powers or professional qualifications) indicated in the certificate itself has lapsed.

In the case of seal certificates, the Holder and RPs acknowledge that the CA does not have any obligation, after the issuing of the certificate, to verify the continued satisfaction over time of the requirements that allowed it to be issued with respect to the legal entity.

4.9.2 Who may request revocation

Revocation of the certificate may be requested:

- by the Holder of the certificate (in the case of a certificate registered to a natural person);
- by the natural person who represents the Holder (in the case of seal certificates);
- by the "interested third party" (in accordance with current laws);
- by the CA itself, if the need arises; in particular, in the case of a seal certificate, if a third party notifies the CA of termination, for whatever reason and/or cause, and/or of the existence of insolvency proceedings and/or other circumstances relating to the legal entity holding it, as a result of which the information contained therein is no longer current;
- by the Courts.

4.9.3 Procedure for revocation

The revocation of the certificate may be requested in the two ways described below.

Procedure 1: on-line

The online revocation request procedure, available 7 days a week and twenty-four hours a day, includes the following steps:

- the Holder connects to the website, https://gestionecertificati.firmadigitale.it, and is authenticated by entering his or her national ID number (or another personal identification code for foreign citizens who do not have a national ID number) and the confidential emergency code (*);
- if authentication is successful, the site shows the most significant data in the Holder's active certificates and makes it possible to select one to request its revocation (or suspension);
- following confirmation of the operation and insertion of the reason (optional), the request for suspension or revocation is immediately accepted and executed (automatically) as soon as possible, in any case within the maximum established timeframe (see §4.9.5).

(*) This is the "user code" delivered to the Holder, in accordance with the laws in force, during registration or delivery of the signature device, in any case, before the Holder takes possession of the signature instruments, fully operational.

Procedure 2: off-line

Revocation of the certificate may also be requested through a formal request sent to the CA by (simple or certified) e-mail, to be sent to the email address revoche.firma@arubapec.it which must contain:

- identification details of the applicant (given name, surname, national ID number, telephone number, e-mail address, postal address, any organization to which he/she belongs and/or his/her powers of representation);
- sufficient details for the identification of the certificate requested to be revoked (e.g. serial number and effective date);
- the reason for the revocation request (see §4.9.1);
- date and applicant's signature (see §3.4 for accepted forms of signing);
- scan of the applicant's identity document, unless the request is digitally signed (see §3.4).

In addition, the form for requesting revocation of a signature certificate can be found in the aruba.it guides on Digital Signatures, which are published online at https://guide.pec.it/soluzioni-firma-digitale/firma-digitale.aspx.

Revocation requests made in this manner will not be accepted if they do not contain all the necessary information listed above.

The CA verifies the authenticity of the request and proceeds to revoke the certificate by inserting it on a revocation and suspension list (**CRL**), which is then published as described in §4.10. The moment (date and time) of the certificate revocation and publication of the CRL is recorded in the audit log. The status of the certificate is also made available through the **OCSP** service (see §4.10).

In both the (on-line and off-line) request procedures, an email is sent to the Holder confirming revocation, if the request has been accepted.

In the case of a request by the "interested third party", the CA informs the certificate Holder of the request for revocation submitted by the "interested third party". The CA may reject the request if it deems it to be unauthentic, inaccurate or incomplete and will notify the requesting "interested third party".

In the case of revocation at the initiative of the CA, the latter notifies the Holder of the reasons for the revocation, as well as the date and time from which the revocation will be effective.

4.9.4 In the event that a revocation is requested and it is not possible to ascertain the authenticity of the request in a timely manner, the CA proceeds with suspension of the certificate.Grace period for a revocation request

In the case of ascertained or even suspected compromise of the respective private key or of respective signature device, the Holder must inform the CA (or RA) of this as soon as possible, requesting the suspension or revocation of the certificate.

4.9.5 Time within which the CA must undertake the revocation

The revocation request is processed within 24 hours of receipt, provided that the request is made in accordance with the established procedures (see §4.9.3) and that there are no doubts as to the authenticity thereof.

In the event that the reason for the revocation (or suspension) request is suspected or proven compromise of the private key, the CA will process the request as soon as possible.

4.9.6 Revocation verification requirements for Relying Parties

Refer to sections §4.5.2 and §9.6.4.

4.9.7 Frequency at which the CRL is issued

The CRL is regenerated and published periodically at least every 24 hours, even in the absence of new requests for suspension or revocation.

4.9.8 Maximum CRL latency

The CRLs are published immediately after being generated. The latency between when generated and when published depends on the computer workload. Usually the latency is a few minutes, and in any case it does not exceed 60 minutes, allowing for unforeseen circumstances.

4.9.9 Availability of on-line services for revocation verification

In addition to publication of the CRLs, the CA also makes available an on-line certificate status verification service based on the OCSP protocol (RFC 6960). The OCSP service is freely accessible by anyone who needs it and is available seven days a week, twenty four hours a day. For further details, refer to §4.10.

4.9.10 Requirements for the on-line verification of revocation

There are no special requirements for the on-line verification of revocation. Only the use of an OCSP client conforming to the RFC 6960 standard is required.

4.9.11 Other forms of publicizing revocation

No provision.

4.9.12 Special requirements in the event of a compromised key

In the event of ascertained impairment of the private key or of the device that contains it (e.g. in the case of established theft), the Holder is required to report this at once to the CA, which will suspend the certificate if the Holder is not able to prove his/her identity and/or does not have the appropriate emergency codes.

4.9.13 Circumstances for suspension

The suspension may take place in the following circumstances:

- explicit request by the Holder of the certificate or by his or her representative (in the case of
  a Holder that is a legal entity);
- unauthenticated revocation request (e.g. due to the fact that the applicant is not able to provide the required confidential code: see §4.2.1);
- explicit request by the "interested third party";
- doubts have arisen regarding the security of the signature device or the confidential data necessary the activation of the key (e.g. PIN, password, OTP);
- doubts have arisen regarding the correctness of the data contained in the certificate.

In the case of seal certificates, the Holder and Relying Parties acknowledge that the CA does not have any obligation, after the electronic seal certificate has been issued, to verify the continued satisfaction of the requirements that allowed it to be issued to the legal entity.

See also the following sections for further details.

4.9.14 Who may request suspension

Suspension of the certificate may be requested:

- by the certificate Holder (in the case of a Holder that is a natural person);
- by the natural person who requested the certificate (in the case of a Holder that is a legal entity);
- by the "interested third party" (if applicable);
- from the CA itself, if the need arises.

4.9.15 Procedure for suspension

The suspension procedure takes place in the same manner as described for revocation in §4.9.3.

4.9.16 Limits on the suspension period

On expiry of a pre-established time period of 120 days from the suspension date, a suspended certificate is automatically revoked by the CA. Here too the CA sends notification to the Holder of the revocation.

4.10 Information services on the certificate status

4.10.1 Operating features

The status of certificates (active, suspended or revoked) is made available to all interested parties by publishing the Certificate Revocation List (**CRL**) using the format set forth in the RFC 5280 specification. The CRL is freely accessible, at least using the HTTP protocol. The CRL address (URL) is contained in the CRLDistributionPoints (CDP) extension of the certificate itself. The serial numbers of revoked certificates *remain in the CRL even after the* certificate expires.

In addition to the CRL, an on-line verification service is also available based on the **OCSP** (On-line Certificate Status Protocol) protocol and in accordance with the RFC 6960 specification. The address (URL) of the OCSP responder is contained in the AuthorityInformationAccess (AIA) extension of the certificate itself.

4.10.2 Service availability

Access to the CRL and to the OCSP service is available continuously (24 x 7).

4.10.3 Optional features

No provision.

4.11 Contract termination

The contract between the CA and the holder is regarded as terminated when the certificate expires or is revoked, unless otherwise specified in contracts with certain customers.

4.12 Security deposit and recovery of the private key

As part of the certification service described here, there is no provision for a security deposit ("key escrow") for Holders' keys. Therefore, it is not possible to recover the Holder's private key ("key recovery"). Regarding CA keys, on the other hand, provisions is made for recovery (see §6.2.4).

5. PHYSICAL AND OPERATIONAL SECURITY MEASURES

5.1 Physical security

Aruba PEC uses data center management services (with ISO/IEC 27001 certificates) provided by the group's parent company, Aruba S.p.A., which is responsible for housing, Internet connectivity and for the physical security of the processing systems used to support the CA service. Aruba guarantees to Aruba PEC:

- physical access control;
- continuity of power supply;
- fire prevention and anti-flooding systems;
- optimal ventilation and air conditioning;
- redundant Internet connectivity and at least twice the minimum capacity required;
- a Network Operation Centre (NOC), manned 24/7 for 365 days a year by qualified systems personnel, which ensures constant monitoring of the infrastructure and services and timely intervention if needed.

5.1.1 Location and building characteristics of the operating site

The CA services, like other trust services provided by Aruba PEC S.p.A., are based on redundant computing infrastructures, designed and built in order to ensure utmost reliability and continuity of service; therefore, several data centers owned by the Aruba Group are used:

- **primary** operating data center ("IT1") located in Arezzo, at via P. Gobetti 96;
- **secondary** operating data center ("IT2") located in Arezzo, at via S. Ramelli 8;
- **disaster recovery** data center ("IT3") located in Ponte S. Pietro (BG), at via S. Clemente 53.

The "IT1" data center, designed and built in accordance with the Rating 4 (ex Tier 4) level specifications of the ANSI/TIA 942-B standard, features the following characteristics:

- Dimensions: 5000 m2
- Capacity: over 40,000 physical servers.
- Type of building: reinforced concrete
- High density
- Maximum floor load (Kg/m2): 1000
- Maximum height of the floating floor (mm): 500
- Height between raised floor and false ceiling (m): 3
- Unpacking room
- External battery areas

The data center ("IT2") has the following characteristics:

- Dimensions: 2000 m2
- Capacity: over 10,000 physical servers
- Type of building: reinforced concrete
- High density
- Maximum floor load (Kg/m2): 500
- Maximum height of the floating floor (mm): 500
- Height between raised floor and false ceiling (m): 3
- Unpacking room
- External battery areas

The ("IT3") data center, also designed and built in accordance with the Rating 4 (ex Tier 4) level specifications of the ANSI/TIA 942-B standard, features the following characteristics:

- Dimensions: 90,000 m2 dedicated to the data center, out of a total area of 200,000 m2
- Capacity: 3600 racks (165,000 physical servers)
- Type of building: reinforced concrete
- Double multi-modular power centre with UPS featuring 2N + 1 redundancy
- Redundant emergency generators with 48-hour full-load autonomy
- Data hall made up entirely of firewalls and ceiling with double insulation
- Autonomous production of hydroelectric and photovoltaic energy
- Incredibly efficient geothermal cooling system
- Storage and office space available to customers

There is also armed surveillance in this data center.

The following Figure 1 depicts the geographical location of the three sites; the "IT3" site (disaster recovery) in Ponte S. Pietro (BG), near Milan, is about 300 km from the primary and secondary sites in Arezzo:

Figure 1: Location of CA operating sites

Further information on data centers may be found on the website, https://www.datacenter.it.

5.1.2 Physical access

The following is in place at all data centers:

- a **physical access control** system, so that access to the building is possible only for those who actually need it, after signing in at reception, and that access to the technical rooms is permitted only for authorized personnel, following identification with a badge and relative PIN;
- **passive anti-intrusion systems**, such as grilles, bulletproof glass, armoured doors, motorized gates, and **intrusion detection systems**, such as CCTV and VMD.

For the specific details of the individual data centers, refer to section 5.1.1.

5.1.3 Power supply and air conditioning;

All data centers are equipped with:

- redundant **power supply** systems at all levels (substations, power centres, UPS, generator sets, switchboards, etc.) to guarantee continuity of power supply in any foreseeable condition;
- **ventilation** and **air conditioning** (HVAC) systems capable of ensuring optimal climatic conditions for the smooth operation of servers hosted at the data center.

For the specific details of the individual data centers, refer to section 5.1.1.

5.1.4 Prevention and protection from flooding

All data centers are equipped with flooding detection systems:

For the specific details of the individual data centers, refer to section 5.1.1.

5.1.5 Fire prevention and protection

A **fire-fighting system** is in place at all data centers, in compliance with the law and the technical standards of reference; sensors for **fire detection** are also present on all floors of the building. For the specific details of the individual data centers, refer to section 5.1.1.

5.1.6 Preservation of storage media

Regarding storage media preservation, the procedures established by the company's information security management system (ISMS) apply.

5.1.7 Waste disposal

Regarding waste disposal, the CA applies the provisions found in current laws.

5.1.8 Off-site backup

In general, backups are stored at a different location from the original data site, thereby ensuring the possibility of restoration under any foreseeable circumstances.

5.2 Operational security

5.2.1 Roles of trust

The organizational structure is established in compliance with the ETSI EN 319 401 and ETSI EN 319 411-1 standards and in compliance with current laws.

The roles of trust 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 CA 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 roles of trust / individuals in positions of responsibility as part of the CA service:

- Security Officer: with overall responsibility for implementing and managing security procedures.
- System Administrator: responsible for the installation, configuration and maintenance of CA systems. The System Administrators include the role of the "Supervisor of Technical Operation of Systems" in accordance with current laws.
- System Operator: responsible for the day-to-day operation of the CA systems.
- System Auditor: responsible for checking the archives and audit logs of CA systems.
- Registration & Revocation Officer: responsible for verifying the information needed to issue certificates and approve certificate requests; also responsible for changing the status of the certificates (e.g. suspension/revocation).

In accordance with art. 38 of the Prime Ministerial Decree (DPCM) of 22 February 2013, the following individuals in positions of responsibility are appointed at Aruba PEC, in addition to those cited above:

- Supervisor of the certification and time validation service;
- Supervisor of technical and logistical services;
- Supervisor of audits and inspections (auditing);
- Security Manager.

5.2.2 Number of people required to perform procedures

For the management of the CA private keys (key generation, backup, restoration, deletion, etc.) at least two parties assigned to roles of trust ("dual control") are required.

The other procedures may be performed by a single person.

5.2.3 Identification and authentication for each role

All the roles of trust specified in section 5.2.1 and Aruba PEC personnel in general use appropriate identification and authentication systems before accessing Aruba PEC information systems.

In particular, with regard to physical access to data rooms and cabinets that contain the CA systems, identification and authentication take place via personal badge with PIN.

On the other hand, as regards logical access to the CA systems, identification is carried out using the personal account and relative password or by means of two-factor authentication (e.g. smartcard with PIN) for the activities or systems that require it.

5.2.4 Roles that require the separation of tasks

The personnel holding one of the roles of trust referred to in section 5.2.1 may not hold additional roles as part of the CA service.

5.3 Personnel security

5.3.1 Required qualifications, experience and authorizations

Aruba PEC ensures that the members of personnel allocated to the CA service are adequately skilled for the tasks assigned to them, on the basis of appropriate education, training, instruction, abilities and experience, and free from conflicts of interest that may compromise necessary impartiality and compliance with the procedures. In particular, with reference to the roles of trust, the required characteristics and skills are described in the company's "job description" document.

In the case of new recruits, Aruba PEC always reserves the right to assess what type of training is necessary with respect to the tasks to be allocated, the existing qualifications and experience, and where necessary makes provision for the inclusion of the person in a training plan.

5.3.2 Background check

In order to define the shortlist of candidates, Aruba PEC uses the CVs sent directly to the company through the appropriate channels (e.g. its website) and the collaboration of companies specializing in recruitment, both in technical and administrative terms. For each candidate, the veracity of the information contained in the C.V. (qualifications, masters, diplomas, specific qualification courses, etc.) is checked. The professional companies appointed by Aruba PEC also have an obligation to request references, possibly for each potential candidate, before submission to Aruba PEC.

5.3.3 Training requirements

The staff allocated to CA services is adequately trained, in accordance with the tasks performed. Aruba PEC provides staff with initial training at the start of their employment, which may also take the form of courses provided by external teachers when deemed necessary, and workplace training ("on-the-job training").

5.3.4 Training refresher frequency

For all personnel working as part of the CA service, the need for new training is assessed at least once a year (or sooner in the case of new developments / services), so as to ensure that all personnel are always able to perform their duties satisfactorily and competently. Furthermore, training for all staff on information security issues is held annually.

5.3.5 Rotation of duties

No provision.

5.3.6 Penalties for unauthorized actions

In the event of unauthorized actions and/or violations of company or Group policies and/or procedures, Aruba PEC reserves the right to apply the disciplinary procedure established in the collective bargaining agreement, after assessing the nature and the seriousness of the violation and its impact on company activities, whether this is the first such instance, whether the employee was adequately trained, etc.

5.3.7 Checks on non-employed personnel

Non-employed personnel (e.g. consultants) must sign a confidentiality agreement (NDA) before they start working with Aruba PEC and when accessing any confidential data. Non-employed personnel must also comply with corporate security policies.

5.3.8 Documentation provided to personnel

Aruba PEC ensures the availability of all the documentation necessary for the proper performance of their duties for all personnel employed in the context of the CA service (this CPS, operating procedures, forms, guides, security policies, etc.).

5.4 Audit log management

The Audit Log is the secure archive in which records of the most relevant events for the security of the CA service are kept.

5.4.1 Types of events recorded

At least the following events are recorded:

- events relating to the management of the life cycle of certificates, in particular requests for
  certificate issue and requests for suspension, reactivation and revocation;
- events relating to the personalization of signature devices;
- access to the system for issuing and managing certificates;
- entry and exit from protected CA premises.

Regarding each event, the type, date and time of occurrence and, if available, other information useful for identifying the those involved in the event, the systems involved, and the outcome of the operations are recorded.

5.4.2 Audit log processing frequency

The relevant events are collected by the systems that generate them and are sent to the centralized management system within a few minutes.
In the Audit Control management system events are automatically classified and stored locally in order to allow them to be consulted.

On a daily basis, local data is copied to the long-term storage system (see section 5.4.4).

5.4.3 Audit log storage period

The Audit Log is kept for 20 years.

5.4.4 Audit log protection

The Audit Log is stored on WORM (Write-Once-Read-Many) storage.

5.4.5 Audit log back-up procedures

The WORM storage on which the Audit Log is stored is replicated at two data centes.

5.4.6 Audit log storage system

Refer to section 5.4.4.

5.4.7 Notifications in case of detection of suspicious events

No provision.

5.4.8 Vulnerability checks

No provision.

5.5 Archiving of records

5.5.1 Type of information archived

Pursuant to the CAD [2], the CA keeps all the information concerning the qualified certificates issued, from the moment they are issued, also in order to provide proof of certification in any court proceedings. Information regarding requests for the suspension or revocation of certificates is also kept.
In particular, the following is archived:

- the certificate application forms, including acceptance of the contract conditions of the CA and any attachments (e.g. applicant's identity document if any, etc.);
- the certificate suspension or revocation request forms.

The contracts stipulated with the Registration Authorities (RA) are held by the Aruba PEC legal department.

Regarding the logs of the CA's processing systems, refer to section 5.4.

5.5.2 Archive retention period

Archives are kept for at least 20 years, in accordance with the CAD [2].

5.5.3 Archive protection

Records are archived and protected in different ways, depending on whether they were originally on paper or digital, as described below:

5.5.3.1 Paper archives

For this scenario, Aruba PEC has entered into a contract with a leading company in the field of archiving and storing documents and in dematerialization processes. This contract provides for a physical archive management service that includes the following activities:

- removal of paper forms from the Aruba archive and delivery to the designated site;
- flows in and out of the archive, using an IT procedure designed specifically for the management of paper archives,
- storage of documents at its Archiving Centre satisfying the security requirements and standards below,
- search and consultation service for paper material with specified SLAs,
- pulping service once the statutory storage period has expired,
- final collection service in the event that Aruba PEC later decides to make use of other suppliers or to manage such documentation on its own.

The site responsible for archiving is equipped with the necessary facilities, the necessary authorizations and the respective certifications for the storage of paper material. In fact, the supplier meets the design requirements laid down by the Archival Superintendencies in matters of custody and management of historical and government agency archives (Italian Legislative Decree no. 490 of 29/10/99 - G.U. [Official Gazette] no. 302 of 27/12/99). Moreover, the same company was entrusted with the task of dematerializing the forms by scanning them, indexing the agreed fields using OCR and periodically transferring images and indexes on servers made available by Aruba PEC.

5.5.3.2 Digital archives

In the case of forms or digital documentation two different approaches are provided for:

- if the documentation is handled manually, such as, for example, digitally signed certificate request forms or revocation requests, once the verified documents have been checked, operators proceed to upload them to the standards-compliant storage system made available by Aruba PEC;
- in the event that the documentation is the result of application processes, it is normally stored on systems that are under the control of the CA and, after applying a time stamp, they are copied onto special systems with restricted access, ensuring that they are maintained for the period required by law.

5.5.4 Archive backup procedure

As detailed in §5.5.3.1, paper archives filed and stored with an external supplier are scanned and a copy is filed on CA systems.

Regarding digital archives, as described in §5.5.3.2, backup is guaranteed either by the storage system, which by nature makes a double copy, or by a replication system that makes a second copy in an area with limited and controlled access.

5.5.5 Time-stamping of archives

Time-stamping is used exclusively for digital documentation produced through automatic procedures: in this case, each document is time-stamped as the last act of the application process.

In the case of the documentation kept in accordance with the law, the time reference is guaranteed by the storage process itself.

5.5.6 Archiving system

Records as per section 5.5.1 all are digitized and then stored in a document management system and kept on the systems in accordance with the procedures described in section 5.5.3.

Digital documents and scanned copies of paper documents are all kept in the Aruba group's data centers.

5.5.7 Procedure for retrieving and verifying archived information

For the quick retrieval of stored information, it is useful to know the procedures used to issue the specific certificate to which the searched information refers; to do this, there are various ways, including the consultation of the CA databases or websites/portals that connect Applicants and RAs. However, it is possible to put into action several search channels in parallel mode if the issue procedure is not known in advance. In general, there are two ways of searching:

1) in the case of paper documentation, the contract with the external supplier includes the search and consultation service in accordance with guaranteed SLAs and in compliance with regulatory and business requirements;
2) in the case of digital documentation, it is possible to carry out searches on the storage system, through the main metadata, or in the archiving area of the documentation not yet placed in storage in compliance with the law.

5.6 CA key renewal

At least 5 years before the end of the period of validity of the current certification key (CA key), Aruba PEC generates a new CA key pair and sends the corresponding self-signed certificate to AgID (as the

national body responsible for supervising the Trust Services Providers). After the new CA certificate has been added to the trusted list (TSL) published by AgID, Aruba PEC begins to sign new certificates and corresponding CRLs with the new CA key.

5.7 Impairment and disaster recovery

5.7.1 Incident and impairment management procedures

The Aruba PEC Corporate Information Security Management System (ISMS), compliant with the ISO/IEC 27001 standard, also provides for incident and compromise management procedures.

The management of an information security incident is handled through a multi-step procedure, each stage of which has a specific purpose, coordinated by an internal committee (Committee for Security and Crisis Management, hereinafter "Committee") comprised of persons with various responsibilities and members of the Management. The phases in which the process is organized are described below:

- Detection: phase in which any person (employee, collaborator or any interested party) who detects a possible incident communicates it to the Committee. The Committee ensures that the report is as detailed as possible and that those who encountered the problem do not take any action independently.
- Identification and analysis: the Committee accepts the report and assesses whether it is actually a security incident. If so, it evaluates its seriousness and proceeds with the following phases. If not, it just closes the incident.
- Containment: in this phase, as far as possible, the harmful effects caused by the incident are limited in order to prevent them from spreading to other areas of the organization.
- Evidence collection: phase in which the evidence is sought and collected in order to attach it to the documentation of the incident in case of possible legal consequences or if it is necessary to proceed with more in-depth investigations. All the evidence is collected following guidelines which aim to guarantee correct and reliable collection.
- Removal and Restoration: phase in which the cause of the damage is removed and, through the restoration procedures, the systems involved in the incident are reactivated, allowing the systems and users to return to work.
- Incident Closure and Notification: once the restoration phase is over, the incident is deemed to be closed. At this stage, the closure is notified to the various managers involved.

5.7.2 Corruption or loss of computers, software and/or data

Aruba PEC implements a Business Continuity plan for the CA service in order to ensure that even a case of corruption or loss of one or more computers cannot cause any disruption to the CA platform. In particular, all critical components of the system are redundant both locally in the single data center and in the two IT1 and IT2 data centers. Aruba PEC also implements specific backup plans to ensure that there is no loss of software and/or data.

5.7.3 Procedures in the event that the CA is compromised

The CA key is the single most critical CA resource and as such is protected by a set of multi-layered security measures, as well as other critical CA resources.

In the event that the CA key is compromised (loss of confidentiality), after the incident has been assessed, Aruba PEC will implement the following plan:

- sending information to the national supervision body (AgID);
- sending information to the conformity assessment body (CAB);
- publication of an information note on the CA website;
- sending an information note to all the RAs and other interested parties;
- revocation of all certificates issued with the compromised key.

Finally, unless the CA is to be discontinued, new CA keys will be generated and the public key will be distributed in the manner set forth in section 6.1.4.

5.7.4 Operational continuity in the event of a disaster

Operational continuity in the event of a disaster is guaranteed by the DR site located in the IT3 data center about 300 km away from the IT1 and IT2 data centers (refer to section 5.1 for further details).

5.8 End of the CA or RAs

Below is a description of the activities that will be carried out if Aruba PEC decides, for any reason, to cease its certification service.

Before the actual end:

- at least 60 days before the scheduled termination date, information will be sent to all customers of the CA service (and other services that include the CA services), as well as to the supervisory body (AgID) and the conformity assessment body (CAB);
- with at least 60 days' notice, an information note will be published in a manner that stands out on the CA website, in order that information is also made available to Relying Parties;
- with at least 60 days' notice, the CA will send a notice to all possible subcontractors and delegated third parties (RAs, informing them that upon expiration of the deadline they will no longer be authorized to perform activities related to the certificate issuing service;
- the responsibility for storing evidence (certificate requests, audit logs, etc.) will be transferred to another trustworthy entity that can guarantee its storage for an adequate time period. Responsibility for publishing the terminated public CA key on its website will also be transferred to this party;
- the destruction of private certification keys as well as that of the attached encryption material allowing restoration thereof will be planned.

Upon the termination date:

- the private certification keys as well as the attached material (if any) allowing restoration thereof will be destroyed (by logic deletion), thereby recording the operation.

6. TECHNICAL SECURITY MEASURES

6.1 Generating and installing keys

6.1.1 Generation of the key pair

6.1.1.1 CA keys

The generation of certification keys (CA keys) takes place in a protected environment, within a secure encryption device (see section 0), by following a procedure that requires the joint action of at least two people ("dual control"). The procedure is performed in the presence of the Head of Internal Inspections and is recorded in a report kept by the CA Security Supervisor.

6.1.1.2 Holders' Keys

In the case of keys that must be placed on a secure device (see section 1.4), the key pair is generated inside the device in accordance with procedures compatible with the security target of the device itself, generally through the software libraries provided by the device manufacturer.
In the case of keys that must not be placed in a secure device (see section 1.4), the key pair is generated by software procedures approved by the CA.

6.1.2 Delivery of the private key to the holder

6.1.2.1 Keys that must be placed on a secure device

In the case of certificates relating to keys that must be placed on a secure device (see section 1.4), the device is generally supplied to the holder by the CA or by the RA already customized (i.e. already containing the private key and the corresponding certificate); in some issue processes, the keys may instead be generated directly by the holder through the tools and procedures made available by the CA. The private key is protected by the device's PIN. In the event that the device is not delivered directly to the holder, but is sent to the holder by post, confidential PIN and PUK codes are sent separately, except in cases where the keys' certificates are delivered with a suspended status (providing the holder with the tools and procedures necessary for their activation).

In the case of keys for remote signature, the private key is not delivered to the holder (because it is inside a remote encryption device) but rather put under the exclusive control thereof through a strong (two-factor) authentication system.

6.1.2.2 Keys that must not be placed on a secure device

In this case, the keys are generated by the holder him or herself, in accordance with procedures approved by the CA, or are generated by the CA and supplied to the holder through secure channels.

6.1.3 Delivery of the public key to the CA

The public key of the party requesting the certificate (future Holder) is provided to the CA in the form of a Certificate Signing Request (CSR) in compliance with the PKCS#10 standard (RFC 2986).

6.1.4 Dissemination of the CA's public key

The CA's public key, necessary for the verification of all the certificates issued by it, is disseminated in the form of a self-signed certificate at least in accordance with the following procedures:

- through publication on the CA website;
- through publication on the CA's server directory;
- through the Trust-service Status List (TSL) published on the AgID website.

6.1.5 Length of keys

Regarding the length of the keys, Aruba PEC generally applies the recommendations of the ETSI TS 119 312 specification ("Electronic Signatures and Infrastructures (ESI); Cryptographic Suites").

6.1.5.1 CA Key

The (RSA type) key of the CA has a length of 4096 bits.

6.1.5.2 Holders' Keys

The (RSA type) keys of Holders must normally have a length of 2048 bits.
Qualified certificates for keys with a length of less than 2048 bits may be issued, at the discretion of the CA, only in limited, justified cases, and for a limited period of time.

6.1.6 Generating parameters and key quality

6.1.6.1 CA Key

The CA uses a pair of cryptographic keys generated by an RSA algorithm, with a public exponent of 65537 (hexadecimal 0x10001).

6.1.6.2 Holders' Keys

Holders' keys must be generated using the RSA algorithm, with a public exponent of 65537 (hexadecimal 0x10001).

6.1.7 Key Usage (X.509 v3 extension)

6.1.7.1 CA Key

The CA's key is used solely to sign the Holders' certificates and to sign the Revoked Certificate Lists (CRL). Therefore, in the CA certificate, the KeyUsage extension contains:

- keyCertSign (certificates signature)
- cRLSign (CRL signature)

6.1.7.2 Holders' Keys

The holders' keys are used for the electronic signature or electronic seal or for website authentication. In the holder's certificate, the value of the KeyUsage extension depends on the type of certificate as follows:

Type of certificate	KeyUsage
Electronic signature, electronic seal (QSealC)	nonRepudiation

Electronic seal for "Signature SPID"	digitalSignature + keyEncipherment
Qualified website authentication certificate (QWAC)	digitalSignature + keyEncryption

6.2 Protection of the private key and security of the hardware security modules

6.2.1 Security requirements of the hardware security modules

The CA's private keys are generated and used on high-quality, secure cryptographic hardware (HSM), possessing Level-3 FIPS PUB 140-2 certification and EAL4-level or higher ISO 15408 (Common Criteria) certification.

In the event that the use of a secure signature device is required (see section 1.4), the holder 's private key is placed inside a cryptographic hardware device with EAL4-level or higher ISO 15408 (Common Criteria) certification, on the basis of a Security Target appropriate for the intended use of the keys, in compliance with current laws.

6.2.2 Multi-person control (N out of M) of the private key

No provision.

6.2.3 Security deposit of the private key

Not applicable.

6.2.4 Backup of the private key

In order to ensure the continuity of the service, Aruba PEC keeps backup copies of its private certification keys (CA keys), in encrypted form.

6.2.5 Archiving of the private key

Backup copies of the CA's private keys are kept in a safe place.

6.2.6 Transfer of the private key from/to the cryptographic module

Backup and recovery operations concerning CA keys require the joint action of at least two different people ("dual control").

6.2.7 Storage of the private key on the hardware security module

The CA's private key is generated exclusively on the hardware security module (HSM), where it remains, and is protected from risks of loss, alteration, unauthorized use, unsafe export, etc., thanks to the specific security mechanisms of the HSM (see also section 6.2.1).

6.2.8 Private key activation procedures

Activation of the private key takes place in compliance with the procedures established by the HSM supplier and in accordance with the related security certification (also see section 6.2.1).

6.2.9 Private key deactivation procedures

No provision.

6.2.10 Private key destruction procedures

For the destruction of the CA's private key, if necessary (for example in the case of complete termination of the service or the disposal of a single CA key), the procedure recommended by the HSM supplier is followed.

6.2.11 Classification of hardware security modules

See section 6.2.1

6.3 Other aspects concerning the management of key pairs

6.3.1 Archiving of the public key

No provision.

6.3.2 Operational duration of certificates and keys

Pursuant to current laws, the CA determines the expiry date of the certificate and the period of validity of the keys in accordance with the length of the keys and the services to which they are assigned, also taking into account the recommendations contained in the ETSI TS 119 312 technical specification.

Certificates issued under this CPS normally have a duration of 3 years. The CA evaluates case by case the appropriateness of issuing certificates with a different duration, taking into account the above. In any case, the maximum duration of a certificate is 10 years.

Website certificates (QWAC) have a maximum duration of 2 years.

The period of validity of the keys is considered to coincide with the period of validity of the corresponding certificates.

6.4 Activation data

6.4.1 Generation of activation data

The generation of key activation data takes place in compliance with best security practices and (if applicable) with the procedures recommended by the device suppliers.

6.4.2 Protection of activation data

6.4.2.1 CA Key

The activation data of CA keys are protected in a manner consistent with the corporate security policy and with the "dual control" requirement referred to in section 6.1.1.1.

6.4.2.2 Holders' keys

The activation data of the holder's private key are protected, by the holder him or herself, in such a way as to prevent their disclosure to unauthorized third parties. For further important clarifications in this regard, refer to section 9.6.3.

6.4.3 Other aspects relating to activation data

No provision

6.5 Computer security

6.5.1 Computer security requirements

The computers used in the CA services use operating systems of proven quality and reliability, configured in such a way as to prevent unauthorized use and/or use of resources (data, applications, communication channels, etc.) in a manner not permitted by the provisions.
If possible and if such feature is not already built into the operating system, anti-malware systems are installed in order to mitigate the risk of "infections" and security attacks. Furthermore, for the same reason, security patches recommended from time to time by suppliers are installed.

The processors are subjected to a "hardening" procedure aimed at removing or disabling unsolicited features, specifically on each computer in accordance with the role it holds in the infrastructure.

Privileged access to computers (i.e. as system "Administrator") is limited to personnel who actually need it and who have been appointed as "system administrator" in compliance with current legislation.

6.5.2 Computer security rating

No provision.

6.6 Life cycle security

6.6.1 System development security

The development of software systems to support the trust services provided by Aruba PEC, including the CA service, performed by Aruba PEC or on behalf of Aruba PEC, takes place in compliance with the company's Quality Management System (QMS), in accordance with the UNI EN ISO 9001:2015 standard.

6.6.2 Security Management System

Aruba PEC has established and put in place an ISMS (Information Security Management System) that complies with the ISO/IEC 27001:2013 standard covering all company areas, including those involved in the development and provision of the CA service.

6.6.3 Life cycle management

The life cycle of the systems is subject to the corporate change management procedures.

6.7 Network security

Access to the CA's on-line hosts is protected by high-quality firewalls that ensure adequate filtering of connections. Before firewalls, the batch of routers that implement appropriate ACLs (Access Control List) is an additional protective barrier. On CA service servers, all unnecessary communication ports are disabled. Only agents that support the protocols and functions necessary for the operation of the service are active.

To strengthen communication filtering, the whole certification system is divided into an external area, an internal area and a DMZ.

At least quarterly, Aruba PEC commissions a Vulnerability Assessment (VA) to see whether there are any network vulnerabilities, using independent specialists.

6.8 Time reference

The time reference used by Aruba PEC, with which the CA processing systems are kept synchronized, is obtained from a high-precision device that guarantees a difference of no more than one second with respect to the UTC time scale.

7. PROFILE OF CERTIFICATES, CRL, OCSP

7.1 Profile of certificates

The certificates issued in accordance with this CPS comply with the RFC 5280 public specification, based on the ITU-T X.509 v3 standard (i.e. ISO/IEC 9594-8:2005), as well as the European ETSI EN 319 411 and ETSI EN 391 412 standards (parts 1-4).

Unless otherwise requested by the interested parties, qualified certificates according to the eIDAS regulation also comply with the AgID recommendations aimed at fostering the interoperability and use of online services in the Italian context (AgID Determination n.121/2019, and subsequent amendments and additions). The following assumes full compliance with these recommendations.

7.1.1 Version number

The certificate version is v3 (2).

7.1.2 Extensions inserted in certificates

Certificates issued under this CPS contain the following extensions:

- **KeyUsage** (OID 2.5.29.15) marked as **critical**
- **CertificatePolicies** (OID 2.5.29.32)
- **CRLDistributionPoints** (OID 2.5.29.31)
- **AuthorityKeyIdentifier** (OID 2.5.29.35)
- **SubjectKeyIdentifier** (OID 2.5.29.14)
- **AuthorityInformationAccess** (OID 1.3.6.1.5.5.7.1.1)
- **qCStatements** (OID 1.3.6.1.5.5.7.1.3)

The **CertificatePolicies** extension contains the identifiers of the certificate policies of reference (see section 1.4 for further information) and any qualifiers thereof.

The **CRLDistributionPoints** extension contains the **CRL** address (for more information, see sections 0 and 7.2).

The **AuthorityInformationAccess** extension contains:

- the address of the OCSP service (for more information, refer to sections 0 and 7.3);
- the address (URL) from which the certificate of the issuing CA may be downloaded.

For qualified website authentication certificates, (QWAC), there is also the **SubjectAlternativeNames** extension which contains one or more **FQDNs** (Fully Qualified Domain Names) controlled by the holder. This includes the FQDN contained in the commonName (CN) attribute for the Subject field.

The **qCStatements** extension contains the following elements:

- **QcCompliance** (OID 0.4.0.1862.1.1)
- **QcRetentionPeriod** (OID 0.4.0.1862.1.3)
- **QcSSCD** (0.4.0.1862.1.4) – present only in certificates related to keys placed on secure device (see section 1.4)
- **QcType** (0.4.0.1862.1.6)
- **QcPDS** (OID 0.4.0.1862.1.5)
- **etsi-psd2-qcStatement** (OID 0.4.0.19495.2) – solo nel caso di certificati per sigillo elettronico o per sito web da utilizzare nell'ambito di servizi di pagamento conformi alla direttiva comunitaria PSD2.

In the event that use of the certificate is limited to transactions that do not exceed a certain value, the **QcStatements** extension also includes the **QcLimitValue** element (OID 0.4.0.1862.1.2).

In the seal certificates to be used for the purposes of AgID Determination n.157/2020, there is also the ExtendedKeyUsage (EKU) extension containing the id-kp-clientAuth element.

7.1.3 Algorithm identifiers

All certificates issued in accordance with this CPS are signed with the **sha256WithRSAEncryption** algorithm identified by OID 1.2.840.113549.1.1.11.

7.1.4 Forms of names

The Subject (holder) field of the certificate contains a **Distinguished Name** consisting of attributes defined in the public RFC 5280 specification and complies with ETSI EN 319 412 standard (parts 1-4).

7.1.5 Limitations on names

Not applicable.

7.1.6 Policy identifiers

For the list of supported policies and their identifiers (OID), refer to section 1.4.
Qualified website authentication certificates (QWAC) also include, in the CertificatePolicies extension, the certificate's standard class EV OID.

7.1.7 Limitations on policies

The PolicyConstraints extension is not used.

7.1.8 Syntax and meaning of policy qualifiers

In the **CertificatePolicies** extension, the **cPSuri** qualifier is always inserted containing the (URL) address of this CPS published on the CA website.

The **userNotice** qualifier may also be present, containing a text describing any limitations on the use of the certificate.

7.1.9 Established treatment of critical policies

Not applicable.

7.2 Profile of CRLs

The CRLs issued by the CA comply with the public RFC 5280 specification.

In the base-fields, in addition to the mandatory data, the **nextUpdate** field is also inserted (scheduled date for the next CRL issue).

The CRL is signed with the **sha256WithRSAEncryption** algorithm (OID 1.2.840.113549.1.1.11).

7.2.1 Version number

The Version field of the CRL contains the value 2 as required by the RFC 5280 specification.

7.2.2 CRL Extensions

The CRL contains the **cRLNumber** extension (consecutive number of the CRL).

The individual entries of the CRL also contain the **reasonCode** extension, **which indicates** the reason for the suspension or revocation.

7.3 OCSP Profile

The OCSP service provided by Aruba PEC complies with the public RFC 6960 specification. In particular, the OCSP response complies with the "pkix-ocsp-basic" profile (OID 1.3.6.1.5.5.7.48.1.1).

7.3.1 Version number

The version of the OCSP response is v1 (0).

7.3.2 OCSP Extensions

The OCSP response contains the Nonce extension (OID OID 1.3.6.1.5.5.7.48.1.2).

8. COMPLIANCE CHECKS

8.1 Frequency and circumstances of checks

Compliance of Aruba PEC's CA services with this CPS, with Regulation (EU) no. 910/2014 ("eIDAS") and with the applicable ETSI standards is verified on an annual basis by an accredited Assessment Body (Conformity Assessment Body, CAB).

Moreover, always on an annual basis, internal auditing is performed on the CA services that also takes into account aspects related to information security, applicable data protection laws and internal policies and procedures.

Aruba PEC may delegate to external companies the task of performing audits on parties that carry out any activities on behalf of Aruba PEC within the context of CA services, for example external RAs (CDRL). For these second-party audits there is no pre-established frequency.

8.1.1 Checks on the CA

The purpose of the audits is to ascertain that the CA's activities comply with all the requirements of the applicable ETSI EN standards and the eIDAS regulation and that they are implemented effectively.

8.1.2 Checks on the RAs

The purpose of the audits is to make sure that the external RAs' activities comply with all the requirements of the applicable ETSI EN standards and the eIDAS regulation and that they are implemented effectively. In the case of external RAs, this is generally achieved by compliance with contractual obligations, such that verification may relate in particular to these aspects.

8.2 Identity and qualifications of auditors

Compliance checks (audits) on the CA are carried out by an accredited Assessment Body (CAB) in compliance with Regulation (EC) no. 765/2008, through qualified and competent personnel on the subject of conformity assessments, in accordance with the ETSI EN 319 403 standard, of the Trust Services Providers and the related trust services provided pursuant to the eIDAS Regulation.

8.3 Relations between the CA and auditors

The Assessment Bodies (CAB) that perform audits on the CA service, and possibly on the external RAs that collaborate with the CA, have no relation with Aruba PEC.

The internal auditor does not belong to the unit that oversees CA activities.

8.4 Topics covered by the checks

The checks concern in particular the correct operation of the CA with reference to the activities of: identification and authentication of the parties requesting the certificates; management of related documentation; certificate issuing; key management; suspension, reactivation and revocation of certificates; updating the list of revoked certificates (CRL). Implementation of the established physical, technical and operational security measures is also verified; the safety of personnel. More generally, compliance with this CPS and with other documents applicable to the CA service (e.g. internal operating procedures) is verified.

8.5 Actions resulting from non-compliance

The actions resulting from any non-compliance detected during audits (failure to meet the requirements defined in the regulations, standards, applicable procedures) depend on the nature and severity of the detected non-compliance, the rules for the management of non-compliance defined by the Supervisory Board and/or internal non-conformity management procedures.

8.6 Communication of the results of checks

The result of the audit carried out by the Supervisory Board (Conformity assessment Body - CAB) is communicated to the company Management and to the heads of the organizational unit in charge of providing the CA service. The result of the audit is also communicated to the National Supervisory Body (AgID) by sending the report produced by the Conformity assessment Body - CAB.

The result of the internal audit or the second-party audit is communicated to the company Management, to the heads of the organizational unit in charge of providing the CA service and, if applicable, to the external entity/organization involved.

9. GENERAL CONDITIONS

9.1 Service fees

9.1.1 Fees for issuing or renewing the certificate

The maximum fees for the service are published on the CA website www.pec.it.

Different economic conditions may be negotiated on a personalized basis, depending on the volumes requested.

9.1.2 Fees for certificate access

Access to published certificates is free of charge and unrestricted.

9.1.3 Fees for access to certificate status information

Access to information services (CRL, OCSP) on the status of certificates is free of charge and unrestricted.

9.1.4 Fees for other services

No provision.

9.1.5 Refund Policy

Refer to the General Supply Conditions published on the CA website.

9.2 Financial responsibility

9.2.1 Insurance coverage

Aruba PEC has taken out specific insurance with a first-rate insurance company to cover the risks resulting from the provision of the certification service and other trust services. In particular, the insurance provides for an indemnity limit per claim and per insurance period of €15,000,000 (fifteen million euros).

9.2.2 Other assets

No provision.

9.2.3 Guarantee or insurance coverage for end users

Refer to section 9.2.1.

9.3 Confidentiality of processed information

9.3.1 Scope of application of confidential information

The following information is treated as confidential:

- in general, all data obtained from Applicants (future certificate Holders), with the exception of information that must be included in the certificates or that for other reasons is considered as non-confidential (see section 9.3.2);
- requests for the issue of certificates, whether in paper or electronic form;
- requests for the suspension or revocation of certificates, whether in paper or electronic form;

- the communications exchanged between the CA and the RAs, and between the CA and the Applicants or Holders, regardless of the communication channel used (email, telephone, web, etc.);
- the confidential codes of Applicants or Holders (e.g. credentials for accessing the CA's websites, activation data of private keys, etc.) if they are generated by the CA or pass through the CA systems;
- Holders' private keys if generated by the CA;
- the logs of the CA's processing systems;
- contracts with external RAs.

9.3.2 Information considered to be non-confidential

All information that must be public in compliance with the law (see section 9.15), with the technical standards of reference for certification services (e.g. RFC 5280) or by explicit request of the Holder is not considered confidential. In particular, the following information is not considered confidential:

- the certificates and information contained therein
- the lists of suspended or revoked certificates (CRL) and the information contained therein
- information on the status of certificates issued on-line by the CA (e.g. via OCSP)
- information on Holders obtainable by searching public sources
- information that the Holder him or herself has asked the CA to make public

9.3.3 Responsibility to protect confidential information

The CA ensures that confidential information is adequately protected, in terms of both hardware and software, from unauthorized access (even if read only) and from the risk of loss due to disasters (refer to section 5.7).

All confidential information is processed by the CA in compliance with applicable rules, in particular Italian Legislative Decree no. 196/03 [4] and Regulation (EU) 2016/679 2016/679 [5].

9.4 Personal data protection and processing

Aruba PEC is the controller of personal data collected when identifying and registering users requesting certificates and is therefore required to process such data with the utmost confidentiality and in accordance with the provisions of Italian Legislative Decree 196/03 [4] and Regulation (EU) 2016/679 [5].

In the event that the identification and registration of users take place at a delegated organization (RA), the latter is qualified as "Data Processor".

9.4.1 Privacy plan

Regarding privacy, the CA complies with current regulations, in particular Legislative Decree 196/03 [4] and Regulation (EU) 2016/679 [5]. The protection of personal data is part of the Aruba PEC Information Security Management System (ISMS), which is ISO/IEC 27001 certified.

9.4.2 Data that is considered personal

Refer to the definition of personal data pursuant to current regulations, in particular Regulation (EU) 2016/679 [5].

9.4.3 Data that is not considered personal

Non-personal data is considered to be that not falling within the definition referred to section 9.4.2.

9.4.4 Roles and Responsibility for processing personal data

Aruba PEC is the "Data Controller" of personal data pursuant to Legislative Decree 196/03 [4] and Regulation (EU) 2016/679 [5].

9.4.5 Information and consent to the processing of personal data

The information on the processing of personal data, pursuant to Regulation (EU) 2016/679 [5], is published on the CA website.
A request for a certificate involves the processing of the Data Subject's personal data by the CA, in accordance with the information issued thereto prior to signing the Contract.

9.4.6 Disclosure of data following a request from the courts

The personal data of the Data Controller may be communicated to the police, courts, information and security agencies or other government entities, pursuant to Regulation (EU) 2016/679 [5], in the event that this is required for the purposes of defence or security of the State or for preventing, detecting or fighting crimes.

9.4.7 Other circumstances of possible personal data disclosure

Not applicable.

9.5 Intellectual property rights

This CPS is the intellectual property of Aruba PEC S.p.A. All rights are reserved.

9.6 Statements and warranties

9.6.1 Statements and warranties of the CA

By issuing the certificate, the CA confirms and warrants that:

- the Holder's identifying information contained in the certificate, as of the issue date of the
  certificate, was accurate and truthful;
- as of the issue date of the certificate, the Holder possessed the corresponding private key.

The CA undertakes to:

- provide the certification service in accordance with this CPS;
- provide an efficient service for the suspension or revocation of certificates;
- provide an efficient and reliable information service on the status of the certificates;
- provide clear and complete information on the requirements and conditions of the service;
- make a copy of this CPS available to anyone who requests it;

- process personal data in accordance with current laws.

The CA also undertakes to fulfil all the obligations stipulated by art. 32 of the CAD and in particular:

- to adopt all the appropriate organizational and technical measures to avoid harm to third parties;
- when dealing with requests to issue qualified certificates:
  - to ascertain, with certainty, the identity of the individual requesting the certification;
  - to release and publish the electronic certificate in the ways and cases stipulated in the technical rules referred to in article 71, pursuant to Legislative Decree no. 196 of 30 June 2003, and subsequent modifications;
  - to specify, in the certificate that has been qualified at the request of the body, and with the consent of the interested third party, the powers of representation or other qualifications relating to professional activities or positions held, after verifying the documentation presented by the applicant confirming their existence;
  - to comply with the technical rules mentioned in article 71;
  - to inform applicants comprehensively and clearly about the certification procedure and the technical requirements needed to access it, as well as about the features and limitations for using signatures issued on the basis of the certification service;
  - to arrange for the timely publication of the revocation and suspension of the electronic certificate if requested by the holder or the third party from whom the holder's powers derive, if the signature device or electronic authentication tools for using the signature device is lost, if stipulated by the authority, if it is discovered that there are circumstances limiting the holder's capacity or if there is a suspicion of abuse or falsification, as stipulated in the technical rules referred to in article 71 of the CAD;
  - to guarantee a secure and timely revocation and suspension service for electronic certificates, as well as to make sure that the lists of signature certificates issued, suspended and revoked function efficiently, punctually and securely;
  - to ensure the precise determination of the date and time of the release, revocation and suspension of electronic certificates;
  - to keep all the information concerning the qualified certificate, including electronically, from the moment of its issue for at least twenty years in order to provide proof of the certification in any court proceedings;
  - not to copy or keep private signature keys of any individual to whom the provider of qualified electronic signature services has provided the certification service;

- to prepare, on durable communication media, all the useful information for individuals who request the certification service, including in particular the precise terms and conditions relating to using the certificate, as well as any usage restrictions, the existence of an optional accreditation system and the procedures for lodging complaints and resolving disputes; this information, which may be transmitted electronically, must be written in clear language, and be provided before the agreement is concluded between the person requesting the service and the provider of electronic signature services;
- to use reliable systems for managing the register of certificates, with processes in place to guarantee that only authorized individuals can add and edit information, that the authenticity of the information can be verified, that the certificates are accessible to the public only in cases agreed to by the holder of the certificate, and that the operator is aware of any event that compromises security requirements. By request, relevant elements of the information may be made available to third parties relying on the certificate;
- to make sure that the system is working properly, ensuring its continuity, and to report any malfunctions that disrupt, suspend or interrupt the service to the AgID and any users immediately.

- to be responsible for identifying the individual who requests the qualified signature certificate, including cases in which that activity is delegated to a third party.
- process personal data in accordance with the provisions of the policy referred to in Article 13 of Regulation (EU) 2016/679. Data may not be collected or processed for any other purposes without the explicit consent of the person to whom it refers.

9.6.2 Statements and warranties of the RAs

The RAs are required to comply fully with the contract signed with the CA, in particular (but not only) as to:

- correct and secure I&A (identification and authentication) of the applicants;
- diligent storage of all the collected evidence (unless it is under the responsibility of the CA, in accordance with the specific contract stipulated with the RA), for the entire time period set forth in the contract;
- correct use of the sending tools and channels that the CA makes available to them.

9.6.3 Statements and warranties of the Holders

The certificate Holder must:

- read and accept in full this CPS before requesting the certificate;
- provide the CA with accurate, complete and truthful information when requesting the certificate;
- use his or her private key solely for the purposes set forth in this CPS;

- adopt security measures to prevent unauthorized use of his or her private key (e.g. by storing the activation data for his or her signature device, such as PIN or password, in a secure place);
- (for certificates that require the use of a signature device) in the case where it generates its own key pair, generate it on a signature device approved by the CA;
- until the expiration date or any revocation of his or her certificate, promptly inform the CA in the event that:
  - his or her signature device is lost, stolen or damaged;
  - he or she has lost the exclusive control of his or her private key, for example due to the compromising of the activation data (PIN or password) of his or her signature device;
  - some information contained in the certificate is incorrect or no longer valid;
- if his or her private key is compromised (for example due to the loss of the signature device's PIN or its disclosure to unauthorized third parties), immediately stop using it and make sure that it is no longer used.

Furthermore, the holder must:

- ensure the confidentiality of restricted codes received from the CA, for example the activation data for signature devices (PIN or password), the restricted codes for accessing the CA's on-line services (e.g. the emergency suspension code), etc.;
- promptly ask the CA to suspend the certificate in the event of the suspected compromising of his or her private key;
- if his or her private key is compromised, promptly ask the CA to revoke the certificate;
- before starting to use the private key, carefully check that the corresponding certificate obtained from Aruba PEC has the expected profile and contains correct information, including any restrictions on use;
- refrain from using the private key in the event that the corresponding certificate obtained from Aruba PEC features any discrepancy with respect to expectations.

The certificate holder must also fulfil the obligations stipulated by art. 32 of the CAD and in particular:

- to look after the signature device or electronic authentication tools for using the remote signature device, and to adopt all the appropriate organizational and technical measures to avoid harm to third parties;
- to use the signature device him or herself.

9.6.4 Statements and warranties of the Relying parties

All those who have to rely on the information contained in the certificates (in short, these parties are referred to as "Relying Parties": RPs) have the obligation, before accepting a certificate, to:

- verify that the certificate in question is complete and authentic;

- verify that the certificate in question is not suspended, revoked or expired on the reference date of the check (*);
- take due consideration of the following information, if present in the certificate: title or qualifications of the holder, organization to which the holder belongs, limits on use, limits on value;
- verify that the certificate in question is a qualified certificate (if required).

(*) Verification may be performed by consulting the CRL published by the CA or by querying the OCSP service provided by the CA, at the addresses (URLs) contained in the certificates themselves. The verification may be omitted only in the case of a "verified signature" certificate (see §4.5.2).

The RPs are also required to be familiar with this CPS; in particular, with regard to liability limitations and compensation policies.
In the case of litigation with Aruba PEC, the RPs may not make any claim if they do not fulfil the obligations set out above.

9.6.5 Statements and warranties of other parties

Pursuant to current laws (in particular, [2] and [3]), an "interested third party" is a natural person or legal entity that consents to the inclusion of a role in the certificate or an organization that requests or authorizes the issuance of the holder's certificate. In the second case, it is the organization that appears in the certificate in the **organizationName** field (if any).

The Interested Third Party is required to:

- be familiar with this CPS;
- promptly inform the CA in the event that the situation in existence at the time of issuing the certificate (e.g. the possession, by the Holder, of certain professional qualifications, his or her belonging to the aforementioned organization or his or her holding of certain positions therein) become inapplicable, requiring in this case the revocation of the certificate.

9.7 Warranty exclusion

The CA has no further obligations and guarantees nothing more than what is expressly stated in this CPS (refer to section 9.6.1) and in the General Supply Conditions and/or as required by current laws.

9.8 Limits on responsibility

Aruba PEC's obligations and responsibilities are only those defined in this document and in the Contract for providing the Service. The CA is liable for damages caused, with intent or negligence, to any natural person or legal entity in the event of failure to comply with contractual obligations and those provided for by current legislation in the cases and within the limits established by art. 13 of the Regulation..
Notwithstanding the above, apart from circumstances that are subject to a binding legal provision, in no other case, on no account and/or for no reason can Aruba PEC be held liable in relation to the Customer, or to any other individuals directly or indirectly connected or linked to the Customer, for direct or indirect damages, data loss, breaches of third-party rights, delays, malfunctions, interruptions, whether total or partial, occurring in relation to the Provision of the Service or connected directly or indirectly with, or resulting from:

a) instances of force majeure, acts of God, catastrophic events (for example but not limited to: fire, explosion, strike, rioting etc.); and/or
b) tampering or interventions affecting the Service or equipment by the Customer and/or third parties not authorized by Aruba PEC.

Aruba PEC will in no circumstances be liable for the use made of the Service in relation to critical situations including, for example, specific risks to the safety of individuals, damage to the environment, specific risks in relation to mass transport services, the management of nuclear and chemical plants and medical devices; in these circumstances, Aruba PEC will make itself available to assess and negotiate with the respective "SLAs" a specific "mission critical" agreement with the Customer.
Aruba PEC does not offer any guarantee of the validity and effects, including evidentiary, of the Service or of any piece of data, information, message, act or document associated with it or in any case issued, communicated, transferred, kept or in any way processed via that Service:

a) if the Customer intends to use them or rely on them in any countries other than Italy, apart from Certificates issued on the basis of this document for countries within the European Union ;
b) for their confidentiality and/or integrity (in the sense that any violations of the latter can normally be identified by the User or the recipient via the appropriate verification procedure).

Under no circumstances will Aruba PEC assume any responsibility for the information, data or content released or transmitted and, in any case, processed by the Customer via the Service, and in general for their use of the aforementioned Service, and reserves the right to take any measures and actions to protect its own rights and interests, including passing on to the individuals involved information that would help to identify the Customer.

9.9 Compensation

9.9.1 Compensation for contracting parties

Aruba PEC has taken out specific insurance to cover the risks of activities and of any harm resulting from the provision of the certification service (see section 9.2.1).

In the event that the certificates issued by Aruba PEC provide for limitations on use - including limitations on the value of transactions for which the certificate is valid, or limitations on the purposes for which the certificate may be used - Aruba PEC will not be liable for damages resulting from improper use.

In any case, compensation for damages to third parties may not exceed the total annual maximum amount of €1,250,000 (one million and two hundred and fifty thousand euros), including claim costs.

In the event of harm resulting from the activities covered by the Contract, the Contracting Party shall, under penalty of forfeiture:

- make a complaint to Aruba PEC within 24 hours of its occurrence, or from when it becomes aware of it (providing confirmation subsequently by registered letter with advice of receipt, or by Certified Email within the next 24 hours);
- within six months from the submission of the complaint referred to in the previous point, quantify the possible damage suffered and put forward the respective request for compensation.

9.9.2 Compensation for Aruba PEC

Without prejudice to the General Supply Conditions, the Contracting Parties are required to reimburse any damages suffered by Aruba PEC in the following cases:

- false statement (e.g. about the identity of the Applicant) in the request for the certificate;
- omitted information regarding essential documents or facts, either due to negligence or intentionally;
- failure to keep the activation data (e.g. PIN) of the respective private key;
- use of names in violation of the intellectual property rights of other parties.

9.10 Duration and termination of the contract

9.10.1 Contract duration

The Contract starts on the date of its acceptance by the Contracting Party and ends on the expiration date of the certificate issued by Aruba PEC; in the event of renewal of the certificate itself, the period of validity of the Contract is deferred until the expiry date of the renewed certificate. In any case, the validity of the Contract shall cease as a consequence of the revocation of the certificate, for whatever reason.

9.10.2 Contract termination

Refer to the General Conditions published on the CA website.

9.10.3 Effects of termination

In the case of termination of the contract, the Holder's certificate is revoked by the CA.

9.11 Notices and communications

Refer to section 1.5.1.

9.12 Revisions of the CPS

9.12.1 Revision procedures

The CA reserves the right to make changes to this CPS at any time, without notice, due to its technical or organizational requirements or as a result of changes to the laws. Each new version of the CPS cancels and replaces the previous versions.

Significant changes to the CPS, e.g. which affect the operational procedures, the profile of the certificates, etc., are agreed with the supervisory body (AgID) before being published.

9.12.2 Notification period and mechanism

This CPS is reviewed by the CA and, if necessary, updated at least once every year even in the absence of changes to the laws.

New versions of the CPS are published on the CA website.

9.12.3 Circumstances that require changing the OID

This CPS applies to various certificate policies (see section 1.4), each one identified by a specific OID. The revision of the CPS does not in itself imply the modification of these OIDs.

9.13 Jurisdiction

The Court of Arezzo shall have sole jurisdiction to settle all legal disputes in which Aruba PEC S.p.A. is the plaintiff or defendant and relating to the use of the certification service, the operating procedures and the application of the provisions of this Manual.

9.14 Applicable law

The contract is subject to Italian and European law and shall be interpreted and performed as such. For anything not expressly provided for in the contract, the CA service shall be governed by current laws.

9.15 Compliance with applicable laws

9.15.1 Regulatory Framework

The main applicable regulatory framework is shown below:

[1] Regulation (EU) 2014/910 of the European Parliament and of the Council dated 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (also "eIDAS").

[2] Italian Legislative Decree no. 82 of 7 March 2005: "Code of Digital Administration", G.U. no. 112 dated 16 May 2005, as subsequently amended and modified.

[3] Prime Ministerial Decree dated 22 February 2013: Technical rules on the generation, application and verification of advanced electronic, qualified and digital signatures...,"
G.U. no. 117 dated 21 May 2013.

[4] Legislative Decree no. 196 dated 30 June 2003" "Personal Data Protection Code", G.U. no. 174 of 29 July 2003, as subsequently amended and modified.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 on the protection of individuals with regard to the processing of personal data, as well as on the free movement of such data and repealing Directive 95/46/EC.

[6] EU Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market etc., Official Journal of the European Union L 337 of 23 December 2015.

[7] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS, which may or may not be supplemented by General Conditions or specific contracts signed specifically by the Applicant, constitutes the provisions governing the use of the certificate by the Holder and also governs the relationship between the Holder and the CA. The request for the certificate means full and unconditional acceptance of this CPS by the Holder.

9.16.2 Contract assignment

Refer to the General Conditions published on the CA website.

9.16.3 Protection

Refer to the General Conditions published on the CA website.

9.16.4 Application (legal fees and waiver of rights)

Refer to the General Conditions published on the CA website.

9.16.5 Force majeure

Aruba PEC shall not be liable for the non-fulfilment of the obligations accepted herein if such non-fulfilment is due to causes not attributable to Aruba PEC, such as - including, but not limited to - acts of God, absolutely unpredictable technical malfunctions, outside all possible control, interventions by the authorities, force majeure, natural disasters, strikes, including actions within companies - including those involving those that the parties use in the performance of activities related to the service described herein - and other causes attributable to third parties.

9.17 Other provisions

9.17.1 Service access times

For access to the CA services, the following times are guaranteed, subject to unforeseen circumstances and in case of scheduled maintenance downtime:

Service	Accessibility times
User registration and certificate issuing	From 9:00 AM to 5:00 PM from Monday to Friday excluding holidays
Suspension or revocation of certificates	24 hours a day, 7 days a week
Access to the CRLs and to the OCSP service	24 hours a day, 7 days a week

Specific service levels may be stipulated through customized contracts.

9.17.2 Recommendations

Signature applications make it possible to add digital signatures to any kind of file. The user must remember that certain formats allow you to add executable code (macros or commands) to the document without changing its binary structure, in order to activate functions that may change acts, data or facts represented within that document (Art. 4, paragraph 3 of the Prime Ministerial Decree (DPCM) of 22 February 2013).
Such files, while signed with a digital signature, do not have the same effects as those described in article 21, paragraph 2 of the CAD.

It is the signatory's sole responsibility to use the standard functions for each product to make sure that this condition is satisfied.

Please find below a number of recommendations as examples. This list is not exhaustive:

- Do not add digital signatures to documents that contain "fields" whose values are automatically updated by the application with which the document is viewed before signing (for example, Page and Date fields in Microsoft Word™).

- Do not add digital signatures to documents that contain executable code (for example "macros" in the Microsoft Office™ suite). Where possible, disable the function before opening the document to be signed (for example in Adobe Reader™ go to Preferences to disable “Acrobat Javascript”).
- Before signing a document, make the "fields" static (for example, in Microsoft Word™ select the whole document, and then use the specific keyboard shortcut, normally CTRL+SHIFT+F9).
- Always check to see if there is executable code in the document to be signed (for example, in Microsoft Word™ use the "Macros" control panel).

Operating procedures may vary depending on the application and product version.
If you have any doubts about the reliability of the document, before adding one or more digital signatures, it is a good idea to convert the document to a different format (e.g. PDF). The conversion process in fact eliminates any elements from the document that could potentially invalidate the signature.

List of attachments to this CPS

ATTACHMENT 1: APPROVED IDENTITY DOCUMENTS

Appendix A - Certification keys

Please find listed below the CA keys currently in use by Aruba PEC and covered by this CPS. For each key, the **Subject** DN, the **Subject Key Identifier** (SKI) and the dates on which validity starts and ends dates are shown. In all cases, this is a Root CA (therefore self-signed) as required by Italian law.

Subject DN	CN = ArubaPEC EU Qualified Certificates CA G2 OU = Qualified Trust Service Provider 2.5.4.97 = VATIT-01879020517 O = ArubaPEC S.p.A. L = Ponte San Pietro C = IT
Subject Key Identifier	13 d6 fa 13 94 9f a5 e1 c1 20 62 a8 fb c2 ee 37 4d 9f ed 25
Effective date	23/09/2017
End of validity	18/09/2037

Subject DN	CN = ArubaPEC EU Qualified Certificates CA G1 OU = Qualified Trust Service Provider 2.5.4.97 = VATIT-01879020517 O = ArubaPEC S.p.A. L = Arezzo C = IT
Subject Key Identifier	c6 6f 3b 85 7b d1 26 b1 78 9a 42 a4 25 69 0c f6 ff 7a a0 67
Effective date	26/04/2017
End of validity	21/04/2037

Subject DN	CN = ArubaPEC S.p.A. NG CA 3 OU = Certification AuthorityC O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	f0 c0 45 b1 b6 35 b4 ea 5f 29 fa 83 03 4a dc 2f f5 b3 7d e8
Effective date	22/10/2010
End of validity	23/10/2030

Subject DN	CN = ArubaPEC for the Carabinieri Police Force CA 1 OU = ArubaPEC for Carabinieri 1 Certification Authority O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	1d ea a2 b9 4c b8 93 25 7f ec 3f 08 27 de 70 f2 8d 7f 83 20
Effective date	27/02/2009
End of validity	28/02/2029

Subject DN	CN = ArubaPEC for the Basilicata Region CA 1 OU = ArubaPEC for CA Basilicata Region of Qualified Signature O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	c5 db f0 51 6a a0 41 3f d1 ab 3c dd 09 54 18 72 05 ca b4 93
Effective date	21/03/2013
End of validity	22/03/2033

Subject DN	CN = ArubaPEC for CA of qualified signature OU = ArubaPEC for form. ATe qualified signature O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	eb 09 88 fb eb 3b c5 07 ba cc b8 00 11 a0 a3 f7 f8 8b a5 64.
Effective date	15/06/2016
End of validity	16/06/2036

Subject DN	CN=Qualified Signature CA for ATe Model OU=ArubaPEC for IPZS 2.5.4.97=VATIT-01879020517 O=ArubaPEC S.p.A. L=Ponte San Pietro C=IT
Subject Key Identifier	80 29 64 4e da aa da ac c5 61 24 27 a5 b3 90 75 aa 66 80 81
Effective date	28/03/2018
End of validity	23/03/2038

As of the date of revision of this CPS, qualified website authentication certificates (QWAC) are signed with the “ArubaPEC EU Qualified Certificates CA G2” key.

Appendix B – Operating procedures for generating and verifying signatures

In reference to art. 14 of the Prime Ministerial Decree (DPCM) of 22 February 2013, Aruba PEC has provided its own customers with applications that allow them to check the digital signatures added to electronic documents in the form of PKCS#7 / CAdES, PAdES and XAdES “cryptographic envelopes”. These applications allow you to check:

1. the integrity of the signed document and the signatory's details;
2. the authenticity and reliability of the signatory's certificate;
3. if applicable, the suspension or revocation status of the signatory's certificate.

The process for confirming a signature therefore requires:

- the signatory's certificate;
- the issuing certification key certificate to check the authenticity, integrity and reliability of the signatory's certificate;
- access to the CRL, or the OCSP service, of the issuing certifier to make sure the signatory's certificate has not been suspended or revoked.

Below is a summary of the user instructions for using the verification system:

1. Launch the signature and verification application.
2. Select the function for verifying signatures.
3. Choose the file to verify.
4. The software requires an Internet connection as it will attempt to access CRL and/or OCSP.
5. The software shows a video of the result of the verification. The content of the signed file can be read using programs suitable for the format of the file itself (for example: PDF files can be read with Acrobat Reader).

The same applications qualified to verify signatures allow you to:

1. Add a digital signature, generating an encrypted envelope, in standard PKCS#7 / CAdES, PAdES and XAdES formats.
2. Add multiple signatures.

A signature is generated thanks to a private key whose corresponding public key has been certified in accordance with the processes outlined in this CPS. The aforementioned private key may or may not be stored on secure signature devices (see. section 1.4) provided or qualified by Aruba PEC. The signatory's qualified certificate corresponding to the public key to be used to verify it is always attached to the digital signature.

Below is a summary of the user instructions for generating the signature:

1. Launch the signature application.

2. Select the signature function from the main menu or context menu.
3. Choose the file to be signed.
4. Enter the personal code(s) to access the (local or remote) secure signature device or other certified key container (see section 1.4).

Appendix C - Procedure for registering and activating the remote signature service with non-contextual identification

Summary

Definitions

Client	Legal person, public or private, having a contractual relationship with the CA for the provision of the services covered by this document and further defined in the dedicated contracts.

1. Introduction

This Appendix describes the conditions and rules according to which the Aruba PEC Certifier issues qualified certificates for remote subscription keys, in compliance with the current legislation on digital signature, in cases where the identification obligations of the requesting user at a later stage and in any case not contextual to the issue and first use of the certificate itself.

2. Scope, purpose and recommendations to readers

This appendix applies in those contexts in which the process of generating the certificate, identifying the applicant and affixing the signature, follows a particular flow or in any case not explicitly detailed within the CPS. The purpose of the Appendix is therefore to describe according to which methods and with which security guarantees Aruba PEC can issue certificates in these specific contexts of use.
The following integrates, where necessary, the ways in which Aruba PEC issues the remote signature certificate in the aforementioned operating context, the security measures adopted, the obligations, guarantees and responsibilities, already indicated in this Operating Manual (CPS) and / or in its Appendices. For anything not expressly indicated in the CPS, what is described in this document remains valid, to which reference should also be made for the regulatory and technical references that may not be indicated in the CPS itself.

3. Methods of issuing and using the certificates

This paragraph describes the procedures used for registering, identifying and activating the signature service for users who have not been previously or contextually identified either by the CA or by the Customer. In a typical, but not exclusive context, the requesting user is a prospect certified on the website / web portal or other IT system of the Certifier or Client, hereinafter simply System, which provides the signature service; the user in question intends, for example, to sign a contract for the

purchase of one or more services or products offered, for which remote signature of the same is required.
The scenario envisages that a user requests a remote digital signature service according to a process summarized in the following phases (the non-essential steps for the purposes of this document are omitted).

1) Recording of data - the user is certified in the designated area of the System and must enter or confirm their personal data, including those essential to the CA for its subsequent identification and for the issuance of the qualified certificate, contact attributes such as your e-mail address and your no. mobile phone, in addition to any data that the Customer may need for his own purposes (see par. 4.1.2.1 "Information that the Applicant must provide" of this CPS for more details).

2) Generation of the certificate - the user proceeds with the request for the remote signature certificate (during the process, the user receives or specifies any codes necessary for authentication during the signature phase, according to the specific procedure activated). Once the CA receives the applicant's personal data, it proceeds to issue the qualified certificate, which will be revoked if the process of verifying the identity of the holder by the CA or the subjects delegated by it is not successfully completed. This qualified certificate will have specific limitations of use and use in relation to the scenario in question.

The CA reserves the right to ask the Customer for specifics, measures and tools in the implementation of the solution, if those adopted are deemed to be inadequate or insufficient for the scenario of use of the qualified certificate, including collecting and transmitting through the specific agreed channels. evidence / attestations relating to the data and registration activities, authenticated by the subject himself or by another natural person authorized as the Client's application manager or process manager.

3) Signature of the contractual conditions - the holder digitally signs the required documentation (forms, documents and contracts of both the Customer and the CA) by entering the static and / or dynamic personal authentication codes (OTP) required by the process; the digital signature certificate, after the documents have been signed, is suspended by the CA, also at the request of the Customer, pending the conclusion of the identification process.

4) Identification of the holder (Activation / Revocation of the Certificate) - consequently, the CA or the delegated subjects (eg the Customer following its contractualization as a CDRL) proceed with the certain identification of the holder. Aruba PEC considers valid the identifications carried out using only one of the identification methods already allowed to the CA pursuant to par. 3.2.3 of this CPS and in any case agreed with Aruba PEC at the time of definition of the activities of CDRL.

There are two alternative scenarios:
- in the event that the process of verifying the identity of the holder is completed positively, thus confirming the assignment of the certificate of the holder, the CA reactivates the certificate and the latter is made available for normal use through the services provided;
- if, on the other hand, the process of verifying the identity of the holder has not ended or has ended negatively (eg by identifying significant discrepancies in the identification data provided and / or reported in the certificate), the CA will proceed with the revocation of the certificate.

The CA reserves the right to request from the Customer, even CDRL, specific evidence / at-tests relating to the outcome of these activities to validate the identity of the owner, also contractually agreeing measures and specific dates in relation to the specific ty of the context.
Nevertheless, the CA remains responsible for guaranteeing the revocation of the certificate if the maximum term provided for by this CPS on the suspension period has expired.

4. Certificate policy

The certificates issued according to the rules of this annex are identified with the following Object Identifiers (OID):

- 1.3.6.1.4.1.29741.1.7.11 = "Qualified eIDAS certificates issued with ad hoc procedures for specific projects"

Additional OIDs may be present in the certificate in relation to the intended use of the certificate, specific standards and regulations and in any case according to the indications of this CPS (par. 1.4).

5. Limits of use

Certificates are issued within a very specific application and use context, therefore provide for the inclusion of appropriate restrictions on the use of the digital signature. As required by the technical rules, this limitation will be encoded within the certificate in human readable form.
Once the remote digital signature service has been activated, according to the procedures described in the previous paragraphs, the holder will be able to use his certificate exclusively through the applied services exposed by the Customer (or by the Certifier). Therefore, the use of the certificate will be limited both through the limitations of use indicated in the certificate itself, as aforementioned, and by technical measures that make it usable exclusively through the services (typically online) provided / offered in relation to the specific scenario in question.

Appendix D - Procedure for activating and using the One Shot remote signature service

Summary

Definitions

One Shot certificate	The qualified digital certificate governed by this Appendix having a limited duration in time for a period not exceeding 30 (thirty) days from the moment of its issue
Client	Legal person, public or private, having a contractual relationship with the CA for the provision of the services covered by this document and further defined in the dedicated contracts.

1. Introduction

This appendix describes the rules, methods and operating procedures adopted by the Certi-ficator for the issue of "One Shot" certificates, that is a particular type of qualified certificate which, in the presence of certain domain constraints or areas of use , is characterized by simplicity of use and short duration.

2. Scope, purpose and recommendations to readers

Aruba PEC, in addition to the certificates having the characteristics described in the general section of this CPS, also has the right in specific contexts, attributable to limited uses of the digital signature, to issue a particular type of certificate called One Shot. The characteristic of these One Shot qualified certificates is that of having a shorter period of validity, usually not exceeding 30 (thirty) days from the time of their issue, use within 24 (twenty-four) hours from the time of issue. , and a simplified user experience.

Once the initial registration phase has been completed, the issuance of the One Shot Certificate is foreseen in a single way, ie remotely with keys generated on HSM devices (QSCD). This procedure is carried out under the responsibility of the Certifier's specialized personnel or duly authorized by the latter, in the spaces that host the HSM and the connected servers.

This appendix identifies the subjects involved in the process of issuing the aforementioned qualified One Shot remote signature certificates, the obligations and responsibilities of said subjects and users, the preconditions and methods of issuing the certificates, and those of their use. .

Where necessary, the following supplements the operating procedures already indicated in this Operating Manual (CPS) and / or in its Appendices. For anything not expressly indicated here, what is described in this document remains valid, to which reference should also be made for any regulatory and technical references not listed here.

3. How to use One Shot certificates

The CA has set up a simplified credential management system for the One Shot Certificate that requires a single IT authentication factor for the affixing of the remote signature, namely the use of a One Time Password (OTP).
The setting by the user and the insertion of the username and password are not considered mandatory for the use of the One Shot certificate as this specific type of certificate can only be used through the signature processes appointed by the Certifier or by the Client and only at the same time or within a time span close to the issue of the requested certificate; the use of the certificate is in any case subject to the initial identification of the applicant in accordance with the identification and authentication functions approved by the Certifier and indicated in this CPS.
Based on the procedures for issuing and issuing digital certificates provided for in the specific operational context, the CA avails itself of the possibility of authorizing its Customers, by means of an act of delegation, to fulfill all or part of the registration and activation, including the certain identification of the requesting subjects and the collection of the user's consent; in this case the Customer is configured as a Local Registration Center (CDRL) of the Certifier accredited by Aruba PEC.

4 Generation and management of the OTP

As mentioned above, the only authentication factor required to use this certificate is a One-Time Password (OTP).
The OTP is generated randomly by the Certifier's system at the time of activation by the Owner of the remote signature procedure.
The OTP is transmitted to the Owner or generated by the same through a hardware or software tool, chosen at the time of registration or established by the contracting parties, Aruba PEC and its Customer, with respect to the context of use. In any case, the OTP token is associated with the Holder through secure procedures that depend on the type of device used; typically the OTP is received on the mobile number declared and verified during the identification / registration phase.
With the insertion of the OTP, the owner starts the remote signature procedure by transmitting the data for the creation of the signature of his exclusive knowledge.

5. Preliminary checks and contractual obligations

Considering the need to ensure the use of the certificate by the legitimate owner, Aruba PEC, before implementing or authorizing the process that allows its delivery, verify that the solution adopted by the Customer is sustainable, adequate to its standards and compliant with this CPS.
Therefore, the Customer is contractually obliged to implement all the organizational measures and security measures that Aruba PEC will deem necessary in order to consider the solution to be implemented sufficiently safe. These particular obligations, arranged for the use of One Shot certificates, will be formalized in the contracts between the parties.

6. Use of the private key and certificate by the holder

The holder is therefore required to protect the confidentiality of his device on which he will generate or receive the OTP and then unlock the use of his private key, keeping it in a safe place and with adequate security measures in order to avoid to let third parties access.
As for all qualified certificates, even for One Shot certificates its use is strictly personal and can never, for any reason, be transferred or granted for use to third parties.

7. Certificate policy

Certificates issued according to the rules of this annex are identified with the following Object Identifier (OID): 1.3.6.1.4.1.29741.1.7.10
Additional OIDs may be present in the certificate in relation to the intended use of the certificate, to specific standards and regulations and in any case according to the indications of this CPS (par. 1.4).

8 Limits of use

Certificates are issued within a very specific application and use context, therefore providing for the inclusion of appropriate restrictions on the use of the digital signature. As required by the technical rules, this limitation will be encoded within the certificate in human readable form.

Consequently, the Holder will be able to access his/her certificate exclusively through specific application services and sign electronic documents as part of authorised processes.