PKI Disclosure Statement

1 Introduction

This document is the PKI Disclosure Statement, as required by European standard ETSI EN 319 411-1, related to the certification service offered by the Trust Service Provider **ArubaPEC S.p.A.**, an Italian company with VAT number IT-01879020517 (in the following, just "ArubaPEC").

In the following, the certification service is also referred to by "CA service" (Certification Authority). The REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 "on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" is referred to by "eIDAS Regulation".

This document does not substitute or replace the Terms and Conditions of the CA service nor the Certification Practice Statement (CPS) published on the CA website (see further on).

2 CA contact information

The CA can be contacted at the following address:

Servizio di Certificazione
Aruba PEC S.p.A
Via San Clemente 53
I-24036 Ponte S. Pietro (BG)
ITALIA

Web site: https://www.pec.it
Info mail: info@arubapec.it
Tel. +39 0575 0500
Fax +39 0575 862.020

For any queries regarding this PKI Disclosure Statement or other documents of the ArubaPEC's CA service, please send email to CPS-requests@ca.arubapec.it.

To request revocation of a certificate, follow the on-line procedure described in the CPS (requires the credentials provided at certificate issuance time). Alternatively, contact the ArubaPEC customer support team at fax number +39 0575.0504 or send an email to assistenza@ca.arubapec.it. For further information, refer to the CPS published on the CA website.

3 Certificate types, validation procedures and usage

ArubaPEC issues **qualified certificates** according to European standard ETSI EN 319 411 and other related standards. Certificates are offered to the general public (private companies, public entities, professionals, private persons, etc.), at the conditions published on the CA website.

All certificates are signed with hashing function SHA-256. For further information on the supported certificate policies (e.g. their respective OIDs and other features) see the documentation published on the CA website at https://www.pec.it/DocumentazioneFirmaDigitale.aspx.

The certificates of ArubaPEC's issuing CAs are published on the CA website and on the website of AgID (Agenzia per l'Italia Digitale) at www.agid.gov.it (see the List of Trust Service Providers).

To allow validation of certificates, the CA makes available both the Certificate Revocations List (CRL) and an on-line status checking service based on the OCSP standard. The URLs of both are included in all certificates, respectively in the CRLDistributionPoints and AuthorityInformationAccess extensions.

4 Reliance limits

Certificates are issued for advanced and qualified electronic signatures and electronic seals.

Limitations on the use of certificates may be specified within certificates themselves, in the UserNotice attribute of the CertificatePolicies extension.

Limitations on the value of transactions in which the certificate can be used may be specified in certificates, within the qCStatements certificate extension, by means of the QcEuLimitValue item.

All records pertaining to the life-cycle of certificates, as well as all the CA service audit logs, are retained by ArubaPEC for 20 years.

5 Obligations of subscribers

The certificate subscriber must:

- provide complete, accurate and truthful information to the CA at the time of certificate request;
- use its private keys only for the purposes and in the ways allowed by the CPS;
- adopt suitable measures to prevent any non-authorized use of its private keys;
- (for certificates that require use of a signature device) if it generates its private key by itself, generate it within a signature device approved by the CA;
- up to the date of certificate expiration, promptly inform the CA in the following cases:

  - its signature device gets lost, is stolen or gets damaged;
  - it has lost the exclusive control of its private key, e.g. because of compromise of the activation data (e.g. PIN) of its signature device;
  - some information contained in its certificate is inaccurate or no longer valid:
- in the case of compromise of its private key (e.g. because the PIN of its signature device gets lost or disclosed to non-authorized people), immediately cease any use of such private key and make sure that it will no longer be used.

For further information, please refer to the CPS.

6 Certificate status checking obligations of relying parties

All those who rely on the information contained in certificates (in short, “Relying Parties”) must verify that certificates are not suspended or revoked. Such verification can be performed by consulting the list of revoked certificates (CRL) published by the CA or by querying the OCSP service provided by the CA, at the addresses (URLs) contained in certificate themselves.

7 Limited warranty and disclaimer/limitation of liability

For warranty and liability limitations, please refer to the Terms and Conditions of the Qualified CA service published on the ArubaPEC website at https://www.pec.it/DocumentazioneFirmaDigitale.aspx.

8 Applicable agreements, CPS, CP

The agreements and conditions applying to the CA service are found in the following documents, published on the ArubaPEC website at https://www.pec.it/DocumentazioneFirmaDigitale.aspx:

- Certification Practice Statement (CPS) of the Qualified CA service
- General Terms and Conditions of the Qualified CA service

The supported Certificate Policies (CP) are described in the CPS; see also section 3 above.

9 Privacy policy

ArubaPEC complies with Italian law on privacy (D.Lgs. 196/2003), with EU Regulation No. 679/2016, and with the recommendations and provisions of the Italian Data Protection Authority. For further information, refer to the general Terms and Conditions of the Qualified CA Service published on the ArubaPEC website at https://www.pec.it/DocumentazioneFirmaDigitale.aspx.

All records relating to qualified certificates issued by ArubaPEC (e.g. evidence of the identity of subscribers; certificate issuance requests, including acceptance of the Terms and Conditions; certificate revocation requests; etc.) are retained by ArubaPEC for 20 years.

10 Refund policy

For the refund policy, please refer to the general Terms and Conditions of the Qualified CA service published on the ArubaPEC website at https://www.pec.it/DocumentazioneFirmaDigitale.aspx.

11 Applicable laws, complaints and dispute resolution

The CA service provided by ArubaPEC is subject to Italian and European law. The applicability, execution, interpretation and validity of the CPS are governed by Italian law and by directly applicable European laws, irrespective of the contract or other choice of legal provisions and without the need to establish a commercial contact point in Italy. This choice is intended to ensure uniformity of procedures and interpretations for all users, regardless of where they reside or use the service.

For all legal disputes related to the ArubaPEC's CA service, where ArubaPEC is plaintiff or defendant, the Court of Bergamo shall have exclusive jurisdiction, with the exclusion of any other court and excluding any hypothesis wherein the law provides for the competence of Consumer's court.

12 TSP and repository licenses, trust marks, and audit

Since December 6, 2007, ArubaPEC is a Certification Service Provided (Certification Authority) enlisted in the public registry of accredited CAs maintained by Agenzia per l'Italia Digitale (AgID).

As of July 1st, 2016, ArubaPEC is a Trust Service Provider of certification and electronic time-stamping services according to the eIDAS Regulation, and therefore enlisted in the Italian List of Trust Service Providers (TSL) published by AgID.

ArubaPEC's CA service is subject to conformity assessment every two years, according to European norms ETSI EN 319 411-1 and ETSI 319 411-2, by an independent, qualified and accredited auditor, as required by the eIDAS Regulation.

* * *