Dichiarazione di Trasparenza della CA

1 Introduzione

Questo documento è la Dichiarazione di Trasparenza (PKI Disclosure Statement), ai sensi dalla norma europea ETSI EN 319 411-1, relativa al servizio di certificazione erogato dal Prestatore di Servizi Fiduciari (Trust Service Provider) Aruba PEC S.p.A., impresa Italiana con CF e P.IVA 01879020517 (in seguito "ArubaPEC").
Nel seguito, il servizio di certificazione è anche detto "servizio di CA" (Certification Authority). Con "Regolamento eIDAS" si intende il "REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE".
Questo documento non sostituisce le Condizioni Generali del servizio di CA né le previsioni del Certification Practice Statement (CPS) pubblicate sul sito web della CA (vedere più avanti).

2 Informazioni di contatto

La TSA è contattabile al seguente indirizzo:

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

Per ogni necessità di chiarimento su questo od altri documenti relativi al servizio di CA di ArubaPEC, si prega di inviare posta elettronica all'indirizzo CPS-requests@ca.arubapec.it.
Per richiedere la revoca dei certificati, il titolare può utilizzare la procedura on-line disponibile sul portale della CA all'indirizzo https://gestionecertificati.firmadigitale.it/, autenticandosi con le credenziali che gli sono state fornite al momento del rilascio del certificati.
La revoca dei certificati può essere richiesta mediante un messaggio posta elettronica all'indirizzo revoche.firma@arubapec.it che contenga:

- i dati identificativi del richiedente (nome, cognome, codice fiscale, telefono, indirizzo di email, indirizzo postale, eventuale organizzazione di appartenenza e/o poteri di rappresentanza);
- i dati sufficienti per l'individuazione del certificato che si chiede di revocare (per es. numero di serie e data di inizio validità);
- la motivazione della richiesta di revoca;

- data e firma del richiedente;
- la scansione del documento di identità del richiedente, a meno che la richiesta non sia firmata digitalmente.

Per maggiori informazioni si rimanda al CPS pubblicato sul sito della CA.

3 Tipi di certificati, relativo utilizzo e procedure di validazione

ArubaPEC eroga **certificati qualificati** in conformità alla norma europea ETSI EN 319 411 e alle norme ad essa collegate. I certificati sono emessi al pubblico generale (aziende private, enti pubblici, professionisti, privati cittadini, ecc.), alle condizioni pubblicate sul sito web della CA. Salvo diversa richiesta degli interessati, i certificati elettronici sono inoltre emessi secondo la piena applicazione delle raccomandazioni emanate dall'AgID e volte a garantire maggiormente l'interoperabilità e la fruizione dei servizi in rete nel contesto italiano.
Tutti i certificati normalmente sono firmati con la funzione di hashing SHA-256. Per maggiori informazioni sulle policy supportate (per es. i relativi OID ed altre caratteristiche) si rimanda alla documentazione pubblicata all'indirizzo https://www.pec.it/DocumentazioneFirmaDigitale.aspx.
I certificati delle chiavi di certificazione (CA emittenti) di ArubaPEC sono pubblicati sul sito web della CA e sul sito web dell'AgID (elenco dei Prestatori di Servizi Fiduciari).
Per la validazione dei certificati, la CA rende disponibili la Lista dei Certificati Revocati (CRL) ed un servizio di interrogazione in standard OCSP. Gli indirizzi (URL) della CRL e del servizio OCSP sono contenuti nei certificati stessi, rispettivamente nelle estensioni *CRLDistributionPoints* e *AuthorityInformationAccess*.

4 Limitazioni di fiducia

I certificati qualificati sono emessi per l'apposizione di sigilli e firme elettroniche avanzate e qualificate.
Ulteriori limitazioni d'uso possono essere specificate nei singoli certificati mediante l'attributo *UserNotice* dell'estensione *CertificatePolicies*.
Eventuali limitazioni sul valore delle transazioni in cui il certificato può essere usato sono specificate all'interno dei singoli certificati attraverso l'estensione *qCStatements*, mediante la voce *QcEuLimitValue*.
Le informazioni di registrazione dei titolari ed il giornale degli eventi (event log) relativi al servizio di CA sono conservati da ArubaPEC per 20 anni.

5 Obblighi dei titolari

Il titolari del certificato ha l'obbligo di:

- fornire alla CA informazioni complete, veritiere ed esatte nella fase di richiesta del certificato;
- utilizzare la propria chiave privata unicamente per gli scopi previsti dal CPS;
- adottare misure di sicurezza atte a prevenire l'uso non autorizzato della propria chiave privata;
- (per i certificati che richiedono l'uso di un dispositivo di firma) nel caso in cui generi da sé la propria coppia di chiavi, generarla all'interno di un dispositivo di firma approvato dalla CA;
- fino alla data di scadenza del certificato, informare prontamente la CA nel caso in cui:

  - il proprio dispositivo di firma sia andato perso, sia stato sottratto o si sia danneggiato;
  - abbia perso il controllo esclusivo della propria chiave privata, per es. a causa della compromissione dei dati di attivazione (es. PIN) del proprio dispositivo sicuro di firma;
  - le informazioni contenute nel certificato siano inesatte oppure non più valide;
- nel caso di compromissione della propria chiave privata (per es. a causa dello smarrimento del PIN del dispositivo di firma o della sua rivelazione a terzi non autorizzata), cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata.

Per maggiori informazioni si rimanda al CPS.

6 Obblighi di verifica dello stato dei certificati

Tutti coloro che fanno affidamento sulle informazioni contente nei certificati (in breve ci si riferisce a tali soggetti con "Relying Parties") hanno l'obbligo di verificare che il certificato non sia sospeso o revocato. La verifica può essere fatta mediante consultazione della Lista dei Certificati Revocati (CRL) pubblicata dalla CA o mediante interrogazione del servizio OCSP erogato dalla CA, agli indirizzi (URL) contenuti nei certificati stessi.

7 Limitazioni di garanzia e di responsabilità

Per quanto riguarda le limitazioni di garanzia e di responsabilità, si rimanda alle condizioni generali del servizio CA pubblicate sul sito web di ArubaPEC all'indirizzo https://www.pec.it/DocumentazioneFirmaDigitale.aspx.

8 Accordi applicabili, CPS e CP

Gli accordi e condizioni che si applicano al servizio di CA sono contenuti nei seguenti documenti pubblicati sul sito web di ArubaPEC all'indirizzo https://www.pec.it/DocumentazioneFirmaDigitale.aspx:

- Certification Practice Statement (CPS) ovvero "Manuale Operativo" del servizio di CA
- Condizioni Generali del servizio di CA

Le policy dei certificati (CP) sono indicate nel CPS, oltre che nel presente documento.

9 Tutela della privacy

ArubaPEC rispetta le norme vigenti italiane (D.lgs. 196/2003) e comunitarie (Regolamento UE n.679/2016) in tema di privacy, nonché le raccomandazioni e disposizioni del Garante per la Protezione dei Dati Personali. Per ulteriori informazioni si rimanda alle condizioni generali del servizio CA pubblicate sul sito web di ArubaPEC all'indirizzo https://www.pec.it/DocumentazioneFirmaDigitale.aspx.
Tutte le informazioni relative ai certificati qualificati emessi da ArubaPEC (le evidenze dell'identificazione dei titolari e della loro accettazione delle condizioni generali, i dati di registrazione dei titolari, le richieste di revoca, ecc.) sono conservate da ArubaPEC per 20 anni.

10 Politiche di rimborso

Per quanto riguarda la politica sui risarcimenti, si rimanda alle condizioni generali del servizio CA pubblicate sul sito web di ArubaPEC all'indirizzo https://www.pec.it/DocumentazioneFirmaDigitale.aspx.

11 Norme applicabili, reclami e foro competente

Il servizio di CA erogato da ArubaPEC è assoggettato alle leggi dell'ordinamento italiano ed europeo. L'applicabilità, l'esecuzione, l'interpretazione e la validità del CPS sono regolate dalla leggi italiane e dalle leggi europee direttamente applicabili, indipendentemente dal contratto o altre scelte di disposizioni di legge e senza la necessità di stabilire un punto di contatto commerciale in Italia. Questa scelta è volta a garantire a tutti gli utenti un'uniformità di procedure e interpretazioni, indipendentemente dal luogo in cui essi risiedono o utilizzano il servizio.

Per tutte le eventuali controversie giudiziarie nelle quali risulti attrice o convenuta ArubaPEC e relative al servizio di CA erogato da ArubaPEC sarà competente esclusivamente il Foro di Arezzo, con esclusione di qualsiasi altro foro competente e con esclusione delle ipotesi in cui la legge preveda la competenza del foro del consumatore.

12 Accreditamenti, marchi di fiducia e verifiche di conformità

Dal 6 dicembre 2007, ArubaPEC è un Certificatore (Certification Service Provider) iscritto nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale (AgID).

Dal 1° luglio 2016, ArubaPEC è un Prestatore di Servizi Fiduciari (Trust Service Provider) di Certificazione e di Validazione Temporale Elettronica ai sensi del Regolamento eIDAS e pertanto iscritto nell'Elenco dei Prestatori di Servizi Fiduciari stabiliti in Italia pubblicato dall'AgID.

Il servizio di CA erogato da ArubaPEC è sottoposto ogni due anni ad una verifica di conformità alle norme ETSI EN 319 411-1 e ETSI EN 319 411-2 da parte di un auditor esterno indipendente, qualificato ed accreditato, come richiesto dal Regolamento eIDAS.

* * *