CEDACRI

Procedura PKI Disclosure Statement

17-06-2025

Unrestricted

Legal Notices

Contenuti

Scopo e ambito di applicazione

Scopo

Questo documento è la Dichiarazione di Trasparenza (PKI Disclosure Statement), ai sensi dalla norma europea ETSI EN 319_401, ETSI EN 319_411-2 e ETSI EN 319_411-1 relativa al servizio di Firma elettronica Qualificata del Prestatore di Servizi Fiduciari Qualificati (Qualified Trust Service Provider- QTSP) nel seguito anche Cedacri S.p.A. con sede legale in Milano (Milano) Corso Monforte n. 30, C.F. – P.IVA 00432960342, 0521 8071, Fax: 0521 807901.

Cedacri S.p.A. opera in conformità alla normativa vigente in materia sia europea (Regolamento UE n.910/2014 - eIDAS) che nazionale (D.Lgs 7 marzo 2005, n. 82 e successive modificazioni – Codice dell'amministrazione digitale).

Questo documento non sostituisce le Condizioni Generali del servizio né il Manuale Operativo della Firma Elettronica Qualificata - CP e CPS (di seguito "Manuale Operativo") pubblicate sul sito web www.cedacricert.it

Ambito di applicazione

Il presente documento ha validità per Cedacri S.p.A.

1 Definizioni e abbreviazioni

Oltre a quanto riportato nel “Glossario” (rif. PR00018A2 – Glossario, allegato alla Procedura di Gestione della Documentazione) che contiene le definizioni e abbreviazioni applicabili a tutta la documentazione interna aziendale, si riportano qui di seguito le definizioni e abbreviazioni specifiche che troveranno applicazione solo per il presente documento.

- Nessuna definizione

2 Informazioni del contatto

Cedacri S.p.A.
Corso Monforte, 30
20122 Milano (Milano)
Tel. +039 0521 8071 (centralino)
Fax.+039 0521 807372
Web site: www.cedacricert.it
Info mail: servizifiduciari-cedacri@iongroup.com

È attivo un servizio di call center indirizzato all'utenza del servizio per qualsiasi tipo di informazione riguardo le procedure descritte nel presente manuale. Il servizio è attivo tutti i giorni, festivi compresi, con orario continuativo nelle 24 ore, al numero 840 033033.

3 Tipi di certificati, relativo utilizzo e procedure di validazione

Il servizio comprende l'emissione di un certificato qualificato riferito alla chiave pubblica del soggetto titolare (di seguito "soggetto") e la sua pubblicazione secondo le modalità indicate nel manuale operativo.

I certificati sono emessi a persone fisiche alle condizioni pubblicate sul sito sul sito web www.cedacricert.it sezione download.

Per le chiavi del soggetto, l'algoritmo di crittografia asimmetrica utilizzato è l'RSA e la lunghezza delle chiavi è non inferiore a 2048 bit.

Per maggiori informazioni sulle policy supportate (per es. i relativi OID ed altre caratteristiche) si rimanda alla documentazione pubblicata all'indirizzo sopra indicato sezione documentazione.

Il processo di rilascio del certificato prevede le due seguenti casistiche:

- chiavi generate su token USB;
- chiavi generate su HSM e destinate all'utilizzo per la sottoscrizione automatica.

Il certificato qualificato emesso ha validità di 1095 giorni salvo revoca.

Qualora richiesto, il QTSP consegna direttamente al sggetto, previa corresponsione del relativo costo, un dispositivo sicuro di creazione della firma in grado di conservare la chiave privata dello stesso e generare al proprio interno le firme digitali.

Sull'emissione di un certificato digitale, che avviene solo dopo l'identificazione e registrazione certa del richiedente. Cedacri gestisce l'intero ciclo di vita del certificato compresa la sospensione temporanea della sua validità o la sua revoca definitiva.

4 Limitazioni di utilizzo

I certificati qualificati sono emessi per l'apposizione di firme elettroniche qualificate.

Ulteriori limitazioni d'uso possono essere specificate nei singoli certificati mediante l'attributo "User Notice" dell'estensione "Certificate Policies".

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 Cedacri per 20 anni.

5 Obblighi dei titolari

Il soggetto è responsabile della veridicità dei dati comunicati nella richiesta di attivazione.

Qualora lo stesso, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto, o, comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, egli sarà considerato responsabile di tutti i danni derivanti al QTSP e/o a terzi dall'inesattezza delle informazioni contenute nel certificato, con obbligo di garantire e manlevare il QSTP per eventuali richieste di risarcimento danni.

Il soggetto è altresì responsabile dei danni derivanti al QSTP e/o a terzi nel caso di ritardo di attivazione da parte sua delle procedure previste dai manuali operativi per la revoca e/o la sospensione del certificato.

Il soggetto, in considerazione della circostanza che l'utilizzo di una firma digitale per cui sia stato emesso un certificato qualificato comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua persona, è obbligato ad osservare la massima diligenza nell'utilizzo, conservazione e protezione della chiave privata, del dispositivo di firma e del codice di attivazione ad esso associato (PIN).

In particolare, il soggetto è obbligato, ai sensi dell'art. 32 del Codice dell'Amministrazione Digitale, ad adottare tutte le misure tecniche ed organizzative idonee ad evitare che, dall'utilizzo del sistema di chiavi asimmetriche o della firma digitale, derivi danno ad altri.

Lo stesso soggetto è tenuto a proteggere la segretezza della chiave privata non comunicando o divulgando a terzi il codice personale identificativo (PIN) di attivazione della stessa, provvedendo a digitarlo con modalità che non ne consentano la conoscenza da parte di altri soggetti e conservandolo in un luogo sicuro e diverso da quello in cui è custodito il dispositivo contenente la chiave.

La chiave privata per cui è stato rilasciato il certificato qualificato è strettamente personale. Il dispositivo sicuro di firma che la contiene non può essere per alcuna ragione ceduto o dato in uso a terzi.

Il soggetto deve autonomamente provvedere al rispetto dei requisiti hardware e software necessari per il corretto utilizzo della firma digitale.

In particolare, il soggetto provvede all'adeguamento dei suoi sistemi hardware e software alle misure di sicurezza previste dalla legislazione vigente.

Il certificato digitale può essere rilasciato al nome dello stesso soggetto che lo richiede e lo utilizza (c.d. soggetto), ovvero al nome di un soggetto, con facoltà di utilizzo da parte di soggetti diversi dal soggetto (c.d. utente-utilizzatore).

Nel caso di rilascio del certificato al nome del soggetto, con facoltà di utilizzo da parte di utenti-utilizzatori, entrambi i soggetti sono destinatari dei diritti e degli obblighi di cui al presente contratto, salvo espressa disposizione contraria.

Nel caso di compromissione della propria chiave privata (per es. a causa dello smarrimento del PIN del dispositivo sicuro di firma o della sua rivelazione a terzi non autorizzata), cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata.

6 Obblighi di verifica dello stato dei certificati

La verifica può essere fatta mediante consultazione della Lista dei Certificati Revocati (CRL) pubblicata dal QSTP o mediante interrogazione del servizio OCSP erogato dalla QSTP agli indirizzi (URL) contenuti nei certificati.

7 Limitazione di garanzia e responsabilità

Gli obblighi del QSTP sono quelli indicati dalla normativa vigente, dal manuale operativo e dalla contrattualistica tra il soggetto e il QSTP.

Il QSTP non presta alcuna garanzia sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dal soggetto, su usi diversi della chiave privata, del dispositivo sicuro di firma e del certificato qualificato rispetto a quelli previsti dalle norme italiane vigenti e dal manuale operativo, sul regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali, sulla validità e rilevanza, anche probatoria, del certificato qualificato o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il certificato è riferito nei confronti di soggetti sottoposti a legislazioni differenti da quella italiana, sulla loro segretezza e/o integrità (nel senso che eventuali violazioni di quest'ultima sono, di norma, rilevabili dal soggetto o dal destinatario attraverso l'apposita procedura di verifica).

8 Accordi applicabili CP e CPS

Gli accordi e condizioni che si applicano sono contenuti nei seguenti documenti pubblicati:

- condizioni generali del servizio disponibili sul sito web di Cedacri all'indirizzo https://www.cedacricert.it/cedacricert/it/download/Offerta.html
- Certificate Policy (CP) e Certification Practice Statement (CPS) ovvero "Manuale Operativo" disponibili sul sito https://www.cedacricert.it/cedacricert/it/documentazione/

9 Tutela sulla privacy

Cedacri rispetta le norme vigenti italiane (D.lgs. 196/2003) ed europee (Regolamento UE n.679/2016) e successive modifiche 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 secondo le indicazioni riportate nel paragrafo precedente.

10 Politiche di rimborso

I clienti sono obbligati al risarcimento dei danni eventualmente sofferti da Cedacri nei seguenti casi:

- falsa dichiarazione nella richiesta di certificazione;
- omessa informazione su atti o fatti essenziali per negligenza o con l'obiettivo di raggirare Cedacri;
- utilizzo di nomi (per es. nomi di dominio, marchi commerciali) in violazione dei diritti di proprietà intellettuale.

11 Norme applicabili, reclami e foro competente

Il servizio erogato da Cedacri è assoggettato alle leggi dell'ordinamento italiano ed europeo.

Cedacri ha messo in atto un processo di gestione degli eventuali reclami che dovessero pervenire via e-mail a "servizifiduciari-cedacri@iongroup.com" garantendo un tempo di presa in carico della richiesta di al massimo 7 gg solari.

Per tutte le eventuali controversie giudiziarie nelle quali risulti attrice o convenuta Cedacri e relative al suddetto servizio erogato da Cedacri sarà competente esclusivamente il Foro di Milano.

12 Accreditamenti, marchi di fiducia e verifiche di conformità

Cedacri è un QTSP per la firma elettronica qualificata ai sensi della normativa europea; pertanto, Cedacri è soggetta a un periodico accertamento di conformità ("vigilanza") da parte del Conformity Assessment Body (CAB).

Tale valutazione di conformità è effettuata ai sensi delle normative citate al Cap.1 secondo lo schema di valutazione eIDAS definito da ACCREDIA.

In aggiunta a quanto detto, Cedacri è conforme agli standard ISO 9001 e ISO 27001 ed il campo di applicazione comprende, tra i servizi erogati da Cedacri, anche la Firma.

La conformità alle procedure e agli standard di sicurezza è verificata tramite un processo di audit interno.

Gli audit interni sono pianificati per verificare la conformità del sistema di gestione ai requisiti di sicurezza definiti da Cedacri e dalle norme internazionali di riferimento.

13 Elenco allegati

- Non presenti.