Dichiarazione di Pratiche e Politiche del Servizio Elettronico di Recapito Certificato Qualificato

Servizi affidabili

Evicertia
Giugno de 2024

Indice

1 Introduzione

1.1 Presentazione

Evicertia, SLU (Evicertia) è un Fornitore di Servizi di Qualificazione (CSP) che fornisce "Servizi di Consegna Elettronica Certificata Qualificata" (QERDS) ai sensi dell'Articolo 7 del REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in data identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

1.2 Nome e identificazione del documento

Il presente documento costituisce la "Dichiarazione di Pratiche e Politiche del Servizio Elettronico di Recapito Certificato Qualificato" di Evicertia di seguito "DPPSERCQ".

Il presente documento deve essere letto congiuntamente all'Evicertia Practice Statement (DPC), al quale è subordinato. Nel presente DPPSERCQ si fa rinvio alle sezioni del medesimo DPC che servono a completare il presente documento.

1.3 Partecipanti ai servizi di certificazione

Esamina questa sezione nel DPC di Evicertia.

1.4 Partecipanti ai servizi di certificazione

1.4.1 Esamina questa sezione nel DPC di Evicertia.

Il servizio di recapito qualificato genera ed emette affidavits[1] al fine di dimostrare che una serie di dati riferiti alla comunicazione tra mittente e destinatario è esistita e non è stata alterata da un determinato momento nel tempo. Il suo utilizzo è limitato alle applicazioni e/o ai sistemi dei clienti (persone fisiche o giuridiche) che hanno contrattato questi servizi.

1.4.2 Limiti e divieti di utilizzo

Il Servizio Elettronico di Recapito Certificato Qualificato non verrà utilizzato per scopi diversi da quelli specificati nel presente documento. Allo stesso modo, il servizio deve essere utilizzato solo in conformità con le normative applicabili.

[1] *Affidavit*: documento legale che serve come testimonianza o dichiarazione giurata davanti a un tribunale, o come garanzia. © Diccionario panhispánico del español jurídico.

1.5 Amministrazione delle politiche

1.5.1 Organizzazione che gestisce il documento

I dettagli dell'azienda sono i seguenti:

- Evicertia, S.L.U. (Evicertia).
- Codice Fiscale: ESB86021839.
- Registro delle Imprese di Madrid Volume: 28127, Libro: 0, Foglio 11, Sezione 8, Foglio M-506734, Iscrizione 1.

1.5.2 Dettagli di contatto dell'organizzazione

I dati di contatto di Evicertia, S.L.U. sono i seguenti:

- Pagina web: https://www.evicertia.com.
- E-mail: info@evicertia.com.
- Telefono: +34914237080.
- Fax: +34911410144.
- Indirizzo postale: C/Lagasca, 95. 28006, Madrid.

1.5.3 Procedure di gestione dei documenti

Il sistema documentale e organizzativo di Evicertia garantisce, attraverso l'esistenza e l'applicazione delle relative procedure, la corretta gestione del presente documento e delle specifiche di servizio ad esso relative.

2 Controllo delle versioni

Versione.	Data	Osservazioni
1.5	18/06/2024	• La prima versione di questo documento è approvata. È numerato come 1.5 per avere la stessa numerazione degli altri documenti linguistici.

3 Pubblicazione e conservazione

3.1 Depositare

Evicertia conserva in modo sicuro tutte gli affidavit generati per un minimo di 15 anni. Allo stesso modo, dispone di un Deposito, in cui sono pubblicate le informazioni relative al Servizio Elettronico di Recapito Certificato Qualificato. Il Deposito è consultabile all'indirizzo https://www.evicertia.com/.

Questo servizio è disponibile 24 ore su 24, 7 giorni su 7 e, in caso di guasto del sistema fuori dal controllo di Evicertia, questa farà del suo meglio per rendere nuovamente disponibile il servizio nel rispetto delle scadenze e delle procedure stabilite in materia di continuità operativa.

3.2 Pubblicazione delle informazioni da parte del fornitore di servizi di certificazione

Evicertia pubblicherà nel proprio Deposito le seguenti informazioni:

- La Dichiarazione sulle pratiche di certificazione Evicertia.
- Le dichiarazioni di divulgazione corrispondenti, di seguito “DD” del Servizio Elettronico di Recapito Certificato Qualificato.
- chiavi pubbliche dei certificati utilizzati per firmare gli affidavit
- In anticipo, e quando possibile, qualsiasi informazione che riguardi i partecipanti ai servizi di certificazione.

3.3 Frequenza di pubblicazione

Le informazioni del PSC, compresi il DD, il DPC e il presente DPPSERCQ, vengono pubblicate non appena disponibili.

Le modifiche al DPPSERCQ sono disciplinate da quanto stabilito nella procedura di gestione del presente documento ed in conformità alla normativa applicabile.

3.4 Controllo di accesso

Esamina questa sezione nel DPC di Evicertia.

4 Identificazione e autenticazione

4.1 Identificazione

Per poter utilizzare i servizi di recapito qualificato di Evicertia, sarà necessario che sia il mittente che il destinatario delle comunicazioni abbiano superato il processo di verifica dell'identità di Evicertia ed entrambe le parti siano abbonate al servizio.

Il processo di verifica dell'identità degli abbonati avverrà attraverso uno qualsiasi dei metodi di identificazione inclusi nell'articolo 24 del Regolamento eIDAS, purché Evicertia lo includa nelle sue procedure interne di verifica dell'identità:

- Presenza fisica in uno qualsiasi degli uffici delle Autorità di registrazione Evicertia.
- A distanza, utilizzando mezzi di identificazione elettronica per i quali è stata garantita la presenza della persona fisica o di un rappresentante autorizzato della persona giuridica.
- Mediante un certificato di firma elettronica qualificata o un sigillo elettronico qualificato.

- Utilizzare altri metodi di identificazione riconosciuti a livello nazionale che forniscano una sicurezza equivalente in termini di affidabilità alla presenza fisica.

Sarà necessario consegnare la documentazione (Carta d'identità, passaporto, contratto firmato elettronicamente con certificato o sigillo qualificato, ...) che dimostri che la persona è chi dice di essere, o il legale rappresentante (atto pubblico o procura) in caso di persona giuridica (società, enti, società di capitali, ...).

Una volta verificata l'identità della persona, per tale utente verranno attivate le corrispondenti funzionalità del servizio di consegna qualificata Evicertia.

4.2 Autenticazione dell'emittente

L'autenticazione del mittente per inviare comunicazioni verrà effettuata tramite nome utente (collegato alla sua email) e password, fornendo il servizio, mezzi con cui applicare politiche di password complesse e proteggere le modifiche della password.

4.3 Autenticazione del destinatario

L'autenticazione del destinatario viene effettuata utilizzando un doppio fattore di autenticazione con un URL temporaneo casuale e una OTP (One-Time Password) che verrà inviata all'e-mail o al cellulare del destinatario.

5 Requisiti operativi

5.1 Accesso al servizio

L'accesso alle diverse URL del Servizio Elettronico di Recapito Certificato Qualificato avverrà sempre tramite protocolli sicuri e comunicazioni crittografate.

5.2 Eventi e prove

Come indicato nell'articolo 3.36 del regolamento eIDAS, il servizio di recapito elettronico qualificato è <<un servizio che consente la trasmissione di dati tra terzi con mezzi elettronici e fornisce prove relative alla gestione dei dati trasmessi, inclusa la prova dell'invio e della ricezione dei dati, e che protegge i dati trasmessi contro i rischi di perdita, furto, deterioramento o alterazione non autorizzata;>>, pertanto il servizio Evicertia consente la raccolta di prove per garantire che i messaggi elettronici del mittente siano consegnati al destinatario degli stessi, garantendo l'integrità delle prove e la loro veridicità.

Il soggetto preposto a garantire tale integrità e veridicità è il PSC stesso, attraverso una serie di processi crittografici come l'apposizione di firme elettroniche e marche temporali qualificate. Sia i processi di firma che le marche temporali sono forniti da PSC qualificati secondo la normativa eIDAS.

Le prove in Evicertia si chiamano affidavit e sono documenti in cui sono raccolte tutte le informazioni degli esperti per dimostrare che un evento si è verificato e non è stato modificato successivamente. Negli affidavit puoi trovare:

- Dati informativi del mittente e del destinatario dei messaggi elettronici.
- Il contenuto rilasciato, insieme ai documenti allegati elaborati, comprende anche riepiloghi crittografici degli stessi.
- Negli affidavit è possibile trovare informazioni sui seguenti eventi:
    - Invio e rilascio al server di posta del destinatario.
    - Consegna al server di posta del destinatario o errore se non è stato possibile consegnarla.
    - Apertura del messaggio.
    - O azioni successive del destinatario (se si verificano).
    - Il riferimento temporale sarà indicato in Tempo Coordinato Universale (UTC).

Ogni atto sostitutivo viene firmato elettronicamente dal servizio, e viene apposta una marca temporale qualificata, al fine di garantire l'integrità del documento e che lo stesso non sia stato successivamente modificato.

L'emittente avrà accesso a tutti i suoi affidavit presso il Servizio Elettronico di Recapito Certificato Qualificato, durante il periodo di custodia contrattuale con un periodo minimo di quindici anni. Il destinatario può accedere agli affidavit attraverso il servizio di supporto o attraverso le informazioni dell'emittente. Una volta scaduto il periodo di validità del contratto, nessuna delle parti avrà accesso agli affidavit.

In caso di mancata integrità degli affidavit o di qualsiasi incidente associato all'integrità del contenuto durante il processo di consegna, il servizio di supporto di Evicertia avviserà le parti interessate.

6 Controlli di sicurezza fisica, di gestione e operativi.

Esamina questa sezione nel DPC di Evicertia.

7 Controlli tecnici di sicurezza

Evicertia utilizza sistemi e prodotti affidabili, protetti da qualsiasi alterazione e che garantiscono la sicurezza tecnica e crittografica dei processi di certificazione che supportano.

7.1 Generazione e installazione della coppia di chiavi

7.1.1 Generazione di coppie di chiavi

I certificati elettronici qualificati del servizio di consegna saranno generati da fornitori di servizi qualificati eIDAS come Firma Profesional (www.firmaprofesional.com) e Uanataca

(www.uanataca.com), in conformità con la sua Dichiarazione sulle pratiche di certificazione e il suo Testo informativo, essendo disponibili sul loro sito web.

Allo stesso modo, sono state seguite le procedure chiave della cerimonia di Evicertia, all'interno del perimetro di alta sicurezza previsto per questo compito. Le attività svolte durante la cerimonia di generazione delle chiavi sono state registrate, datate e firmate da tutti i soggetti che vi hanno partecipato. Tali registrazioni vengono conservate a fini di audit e monitoraggio per un periodo adeguato determinato da Evicertia.

Per la generazione delle chiavi dei certificati elettronici qualificati del servizio di consegna vengono utilizzati dispositivi con certificazione FIPS 140-2 livello 3 o Common Criteria EAL4+.

Le chiavi vengono generate utilizzando l'algoritmo a chiave pubblica RSA, con una lunghezza minima di 2048 bit.

Certificati elettronici qualificati del servizio di consegna	2.048 bit	Fino a 5 anni

7.1.2 Invio della chiave pubblica all'emittente del certificato

I metodi per inviare la chiave pubblica al fornitore di servizi elettronici di fiducia sono PKCS#10, un'altra prova crittografica equivalente o qualsiasi altro metodo approvato da Evicertia.

7.1.3 Distribuzione della chiave pubblica del fornitore di servizi di certificazione

Le chiavi pubbliche di Evicertia vengono comunicate a terzi che si fidano dei certificati, garantendo l'integrità della chiave e autenticandone l'origine, pubblicandola nel Deposito.

Gli utenti possono accedere al Deposito per ottenere chiavi pubbliche e inoltre, nelle applicazioni S/MIME, il messaggio di dati può contenere una catena di certificati, che vengono distribuiti agli utenti in questo modo.

Il certificato delle autorità di certificazione radice e subordinate sarà disponibile per gli utenti sul sito web di Evicertia.

7.1.4 Dimensioni delle chiavi

La lunghezza delle chiavi dei certificati utilizzati per firmare gli affidavit sarà di almeno 2048 bit.

7.1.5 Generazione dei parametri della chiave pubblica

La chiave pubblica dei certificati utilizzati per firmare gli affidavit è preferibilmente crittografata secondo RFC 5280.

7.1.6 Controllo di qualità dei parametri della chiave pubblica

La qualità dei parametri della chiave pubblica sarà almeno:

- Lunghezza modulo = 4096 bit
- Algoritmo di generazione della chiave: rsagen1
- Funzioni crittografiche riassuntive: SHA256.

7.1.7 Generazione di chiavi in applicazioni informatiche o beni d'investimento

Tutte le chiavi vengono generate in beni strumentali, secondo quanto indicato nella sezione “Generazione delle coppie di chiavi”.

7.2 Protezione della chiave privata

Esamina questa sezione nel DPC di Evicertia.

7.3 Controlli di sicurezza informatica

Esamina questa sezione nel DPC di Evicertia.

7.4 Controlli tecnici del ciclo di vita

Esamina questa sezione nel DPC di Evicertia.

7.5 Controlli di sicurezza della rete

Esamina questa sezione nel DPC di Evicertia.

7.6 Controlli tecnici del modulo crittografico

Esamina questa sezione nel DPC di Evicertia.

7.7 Fonti orarie

Esamina questa sezione nel DPC di Evicertia.

8 Controllo di conformità

Esamina questa sezione nel DPC di Evicertia.

9 Requisiti commerciali e legali

Esamina questa sezione nel DPC di Evicertia.

10 Allegato I – Acronimi

Gli acronimi utilizzati nel presente DPC sono riportati di seguito.

- CA: *Certification Authority*.
- RA: *Registration Authority*.
- CN: *Common Name*.
- CP: *Certificate Policy*.
- CED: Centro Elaborazione Dati.
- CPS: *Certification Practice Statement*.
- CRL: *Certificate Revocation List*. Elenco dei certificati revocati.
- CSR: *Certificate Signing Request*. Richiesta de firma del certificato.
- DES: *Data Encryption Standard*. Standard di crittografia dei dati.
- DN: *Distinguished Name*. Nome distintivo all'interno del certificato digitale.
- DPC: Dichiarazione sulle Pratiche di Certificazione.
- DSA: *Digital Signature Algorithm*. Standard dell'algoritmo di firma.
- DCCF: Standard dell'algoritmo di firma.
- ETSI: *European Telecommunications Standards Institute* o Istituto europeo per le norme di telecomunicazione o Istituto europeo per le norme di telecomunicazione.
- QSCD: *Qualified Signature Creation Device*. Dispositivo qualificato per la creazione di firme.
- FIPS: *Federal Information Processing Standard Publication*.
- ISO: *International Organization for Standardization*. Organizzazione internazionale per la standardizzazione.
- LRC: Elenchi di revoche di certificati.
- LDAP: *Lightweight Directory Access Protocol*. Protocollo di accesso alla directory.
- NTP: *Network Time Protocol*.
- OCSP: *On-line Certificate Status Protocol*. Protocollo di accesso allo stato del certificato.
- OID: *Object Identifier*. Identificatore dell'oggetto.
- OTP: *One-Time Password*.
- PA: *Policy Authority*.
- PC: Politica di certificazione.
- PDS: Disclosure Statement. Testo informativo.
- PIN: Personal Identification Number. Numero di identificazione personale.
- PKCS: Public-Key Cryptography Standards.
- PKI: *Public Key Infrastructure*. Infrastruttura a chiave pubblica.
- PSC: Fornitore di servizi fiduciari/certificazione elettronica.
- RSA: *Rivest-Shimar-Adleman*. Tipo di algoritmo di crittografia.
- SHA: *Secure Hash Algorithm*. Algoritmo hash sicuro.
- SSL: *Secure Sockets Layer*.
- TCP/IP: *Transmission Control. Protocol/Internet Protocol.*
- URL: *Uniform Resource Locator* o localizzatore uniforme di risorse.