Dichiarazione della chiave di firma del notaio TLSNotary

Servizio: `pavoltravnik.witness.directcase.ai` · **Versione del documento:** 1.0 · **Data:** 26 settembre 2026

> **MODALITÀ DI TEST.** Il servizio è sperimentale ed è fornito senza alcuna garanzia. Le ricevute sono destinate esclusivamente a scopi di collaudo e valutazione e non devono essere utilizzate come prova in questioni legali, finanziarie o altre questioni critiche. La chiave sotto indicata può essere ritirata in qualsiasi momento; la relativa cronologia è pubblicata all'indirizzo `/keys.json`.

1. DICHIARANTE

Ing. Mgr. Pavol Trávnik, nato il 22 luglio 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Repubblica ceca, che agisce in qualità di **persona fisica** e unico gestore del servizio.

2. FUNZIONAMENTO DEL SERVIZIO

Il servizio è un *notaio tecnico* (notary; verificatore) basato sul protocollo open source TLSNotary. Quando un utente (il *dimostratore*) carica una pagina web tramite HTTPS, il notaio partecipa alla sessione TLS — mediante calcolo multiparte (MPC-TLS) o come proxy — senza poter falsificare i dati del server. Il dimostratore può oscurare le parti private; il notaio firma quindi una **ricevuta**: un impegno crittografico sull'identità del server (verificata rispetto al suo certificato TLS) e sul contenuto divulgato, con l'ora della verifica. Chiunque può in seguito verificare la ricevuta senza doversi fidare del dimostratore.

Una ricevuta valida prova che il contenuto divulgato è stato fornito tramite TLS dal server indicato all'ora dichiarata, e che il presente notaio ne è stato testimone. **Non prova** che il contenuto sia veritiero, né alcunché in merito alle parti oscurate. Il notaio è gestito in modo indipendente dai siti web che osserva.

3. CHIAVE DI FIRMA DICHIARATA

ID della chiave	`73a6bdba645a59e4` (primi 8 byte dello SHA-256 della chiave pubblica)
Algoritmo	ECDSA, curva secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Chiave pubblica (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 della chiave pubblica	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Attiva dal	2026-09-25T21:52:43Z

Dichiaro che la presente chiave è stata generata dal servizio sotto il mio esclusivo controllo, che le ricevute firmate con essa sono emesse dal servizio sopra descritto e che pubblicherò il ritiro di tale chiave all'indirizzo `/keys.json`.

4. COME VERIFICARE UNA RICEVUTA

1. Verificare che il presente PDF rechi una firma eIDAS valida del dichiarante (ad es. con il validatore EU DSS).
2. Prendere la ricevuta `{alg, key_id, payload, signature}` e accertare che `key_id` e la chiave pubblica corrispondano alla sezione 3.
3. Verificare la firma ECDSA (`r‖s` di 64 byte, hex) sullo SHA-256 dei byte UTF-8 esatti di `payload`, oppure inviare la ricevuta a `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Verificare che il valore `verified_at` di `payload` rientri nel periodo di validità della chiave.

Firmato elettronicamente dal dichiarante con firma elettronica ai sensi del regolamento (UE) n. 910/2014 (eIDAS).