Erklärung zu einem Signaturschlüssel eines TLSNotary-Notars

Dienst: `pavoltravnik.witness.directcase.ai` · **Dokumentversion:** 1.0 · **Datum:** 26. September 2026

> **TESTMODUS.** Der Dienst ist experimentell und wird ohne Gewähr bereitgestellt. Belege sind ausschließlich für Test- und Evaluierungszwecke bestimmt und dürfen in rechtlichen, finanziellen oder sonstigen kritischen Angelegenheiten nicht als Beweismittel herangezogen werden. Der nachstehende Schlüssel kann jederzeit außer Betrieb genommen werden; seine Historie wird unter `/keys.json` veröffentlicht.

1. ERKLÄRENDER

Ing. Mgr. Pavol Trávnik, geboren am 22. Juli 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Tschechische Republik, handelnd als **natürliche Person** und alleiniger Betreiber des Dienstes.

2. FUNKTIONSWEISE DES DIENSTES

Der Dienst ist ein *Notar* (Notary, Verifier) auf Grundlage des quelloffenen Protokolls TLSNotary. Lädt ein Nutzer (der *Beweisführer*, Prover) eine Webseite über HTTPS, nimmt der Notar an der TLS-Sitzung teil – durch Mehrparteienberechnung (MPC-TLS) oder als Proxy –, ohne die Daten des Servers fälschen zu können. Der Beweisführer kann private Teile schwärzen; der Notar signiert sodann einen **Beleg**: eine Festlegung (Commitment) auf die Identität des Servers (geprüft anhand seines TLS-Zertifikats) und auf den offengelegten Inhalt, samt Zeitpunkt der Prüfung. Jeder kann den Beleg später prüfen, ohne dem Beweisführer zu vertrauen.

Ein gültiger Beleg beweist, dass der offengelegte Inhalt zum angegebenen Zeitpunkt vom genannten Server über TLS ausgeliefert wurde und dieser Notar dies bezeugt hat. **Er beweist nicht**, dass der Inhalt wahr ist, und nichts über geschwärzte Teile. Der Notar wird unabhängig von den von ihm beobachteten Websites betrieben.

3. ERKLÄRTER SIGNATURSCHLÜSSEL

Schlüssel-ID	`73a6bdba645a59e4` (erste 8 Byte des SHA-256 des öffentlichen Schlüssels)
Algorithmus	ECDSA, Kurve secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Öff. Schlüssel (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 des öff. Schlüssels	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktiv seit	2026-09-25T21:52:43Z

Ich erkläre, dass dieser Schlüssel vom Dienst unter meiner alleinigen Kontrolle erzeugt wurde, dass damit signierte Belege von dem oben beschriebenen Dienst ausgestellt werden und dass ich die Außerbetriebnahme dieses Schlüssels unter `/keys.json` veröffentlichen werde.

4. PRÜFUNG EINES BELEGS

1. Prüfen Sie, dass dieses PDF eine gültige eIDAS-Signatur des Erklärenden trägt (z. B. mit dem EU DSS Validator).
2. Nehmen Sie den Beleg `{alg, key_id, payload, signature}` und bestätigen Sie, dass `key_id` und der öffentliche Schlüssel mit Abschnitt 3 übereinstimmen.
3. Prüfen Sie die ECDSA-Signatur (64 Byte `r‖s`, hex) über SHA-256 der exakten UTF-8-Bytes von `payload` oder senden Sie den Beleg an `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Prüfen Sie, dass `verified_at` im Payload innerhalb des Gültigkeitszeitraums des Schlüssels liegt.

Vom Erklärenden elektronisch unterzeichnet mit einer elektronischen Signatur gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS).