Försäkran om en signeringsnyckel för en TLSNotary-notarie

Tjänst: `pavoltravnik.witness.directcase.ai` · **Dokumentversion:** 1.0 · **Datum:** 26 september 2026

> **TESTLÄGE.** Tjänsten är experimentell och tillhandahålls utan garanti. Kvitton är endast avsedda för test och utvärdering och får inte åberopas som bevis i rättsliga, finansiella eller andra kritiska angelägenheter. Nyckeln nedan kan när som helst tas ur bruk; dess historik publiceras på `/keys.json`.

1. UTFÄRDARE AV FÖRSÄKRAN

Ing. Mgr. Pavol Trávnik, född den 22 juli 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Tjeckien, som agerar som **fysisk person** och ensam operatör av tjänsten.

2. VAD TJÄNSTEN GÖR

Tjänsten är en *notarie* (notary, verifierare) byggd på protokollet TLSNotary med öppen källkod. När en användare (*bevisaren*, prover) läser in en webbsida via HTTPS, deltar notarien i TLS-sessionen – genom flerpartsberäkning (MPC-TLS) eller som proxy – utan att kunna förfalska serverns data. Bevisaren kan dölja privata delar; notarien signerar därefter ett **kvitto**: ett åtagande (commitment) avseende serverns identitet (kontrollerad mot dess TLS-certifikat) och det röjda innehållet, med tidpunkten för verifieringen. Vem som helst kan senare kontrollera kvittot utan att behöva lita på bevisaren.

Ett giltigt kvitto bevisar att det röjda innehållet levererades över TLS av den angivna servern vid den angivna tidpunkten och att denna notarie bevittnade det. **Det bevisar inte** att innehållet är sant, och inte heller något om dolda delar. Notarien drivs oberoende av de webbplatser den observerar.

3. FÖRSÄKRAD SIGNERINGSNYCKEL

Nyckel-id	`73a6bdba645a59e4` (de första 8 byten av SHA-256 av den publika nyckeln)
Algoritm	ECDSA, kurva secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Publik nyckel (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 av publik nyckel	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktiv sedan	2026-09-25T21:52:43Z

Jag försäkrar att denna nyckel har genererats av tjänsten under min ensamma kontroll, att kvitton signerade med den utfärdas av den tjänst som beskrivs ovan och att jag kommer att publicera att nyckeln tagits ur bruk på `/keys.json`.

4. SÅ VERIFIERAS ETT KVITTO

1. Kontrollera att denna PDF bär en giltig eIDAS-underskrift av utfärdaren (t.ex. med EU DSS-validatorn).
2. Ta kvittot `{alg, key_id, payload, signature}` och bekräfta att `key_id` och den publika nyckeln stämmer med avsnitt 3.
3. Verifiera ECDSA-signaturen (64 byte `r‖s`, hex) över SHA-256 av exakt de UTF-8-byte som utgör `payload`, eller skicka kvittot till `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Kontrollera att `verified_at` i nyttolasten ligger inom nyckelns aktiva period.

Elektroniskt undertecknad av utfärdaren med en elektronisk underskrift enligt förordning (EU) nr 910/2014 (eIDAS).