Erklæring om en signeringsnøgle for en TLSNotary-notar

Tjeneste: `pavoltravnik.witness.directcase.ai` · **Dokumentversion:** 1.0 · **Dato:** 26. september 2026

> **TESTTILSTAND.** Tjenesten er eksperimentel og stilles til rådighed uden garanti. Kvitteringer er udelukkende beregnet til test og evaluering og må ikke lægges til grund som bevis i juridiske, finansielle eller andre kritiske anliggender. Nøglen nedenfor kan til enhver tid tages ud af drift; dens historik offentliggøres på `/keys.json`.

1. ERKLÆRINGSGIVER

Ing. Mgr. Pavol Trávnik, født den 22. juli 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Den Tjekkiske Republik, der handler som **fysisk person** og eneste operatør af tjenesten.

2. HVAD TJENESTEN GØR

Tjenesten er en *notar* (notary, verifikator) bygget på open source-protokollen TLSNotary. Når en bruger (*bevisføreren*, prover) indlæser en webside via HTTPS, deltager notaren i TLS-sessionen – ved flerpartsberegning (MPC-TLS) eller som proxy – uden at kunne forfalske serverens data. Bevisføreren kan skjule private dele; notaren signerer derefter en **kvittering**: en forpligtelse (commitment) på serverens identitet (kontrolleret mod dens TLS-certifikat) og på det offentliggjorte indhold, med tidspunktet for verifikationen. Enhver kan senere kontrollere kvitteringen uden at skulle have tillid til bevisføreren.

En gyldig kvittering beviser, at det offentliggjorte indhold blev leveret via TLS af den angivne server på det anførte tidspunkt, og at denne notar overværede det. **Den beviser ikke**, at indholdet er sandt, eller noget om skjulte dele. Notaren drives uafhængigt af de websteder, den observerer.

3. ERKLÆRET SIGNERINGSNØGLE

Nøgle-id	`73a6bdba645a59e4` (de første 8 bytes af SHA-256 af den offentlige nøgle)
Algoritme	ECDSA, kurve secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Offentlig nøgle (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 af offentlig nøgle	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktiv siden	2026-09-25T21:52:43Z

Jeg erklærer, at denne nøgle er genereret af tjenesten under min eneste kontrol, at kvitteringer signeret med den udstedes af den ovenfor beskrevne tjeneste, og at jeg vil offentliggøre udfasningen af denne nøgle på `/keys.json`.

4. SÅDAN VERIFICERES EN KVITTERING

1. Kontrollér, at denne PDF bærer en gyldig eIDAS-signatur fra erklæringsgiveren (f.eks. med EU DSS-validatoren).
2. Tag kvitteringen `{alg, key_id, payload, signature}` og bekræft, at `key_id` og den offentlige nøgle svarer til afsnit 3.
3. Verificér ECDSA-signaturen (64 bytes `r‖s`, hex) over SHA-256 af de nøjagtige UTF-8-bytes i `payload`, eller send kvitteringen til `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Kontrollér, at `verified_at` i payloaden ligger inden for nøglens aktive periode.