Vakuutus TLSNotary-notaarin allekirjoitusavaimesta

Palvelu: `pavoltravnik.witness.directcase.ai` · **Asiakirjan versio:** 1.0 · **Päivämäärä:** 26. syyskuuta 2026

> **TESTITILA.** Palvelu on kokeellinen, ja se tarjotaan ilman minkäänlaista takuuta. Kuitit on tarkoitettu vain testaukseen ja arviointiin, eikä niihin saa vedota todisteena oikeudellisissa, taloudellisissa tai muissa kriittisissä asioissa. Jäljempänä mainittu avain voidaan poistaa käytöstä milloin tahansa; sen historia julkaistaan osoitteessa `/keys.json`.

1. VAKUUTTAJA

Ing. Mgr. Pavol Trávnik, syntynyt 22. heinäkuuta 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Tšekin tasavalta, joka toimii **luonnollisena henkilönä** ja palvelun ainoana ylläpitäjänä.

2. PALVELUN TOIMINTA

Palvelu on avoimen lähdekoodin TLSNotary-protokollaan perustuva *notaari* (todentaja, engl. *notary/verifier*). Kun käyttäjä (*todistaja*, engl. *prover*) lataa verkkosivun HTTPS-yhteydellä, notaari osallistuu TLS-istuntoon — monen osapuolen laskennalla (MPC-TLS) tai välityspalvelimena — ilman että se voi väärentää palvelimen tietoja. Todistaja voi peittää yksityiset osat; sen jälkeen notaari allekirjoittaa **kuitin**: kryptografisen sitoumuksen (commitment) palvelimen identiteettiin (tarkistettu sen TLS-varmenteesta) ja paljastettuun sisältöön sekä todentamisen ajankohdan. Kuka tahansa voi myöhemmin tarkistaa kuitin luottamatta todistajaan.

Pätevä kuitti todistaa, että nimetty palvelin toimitti paljastetun sisällön TLS-yhteydellä ilmoitettuna ajankohtana ja että tämä notaari havaitsi sen. **Se ei todista** sisällön paikkansapitävyyttä eikä mitään peitetyistä osista. Notaaria ylläpidetään riippumattomasti sen havainnoimista verkkosivustoista.

3. ILMOITETTU ALLEKIRJOITUSAVAIN

Avaimen tunniste	`73a6bdba645a59e4` (julkisen avaimen SHA-256-tiivisteen 8 ensimmäistä tavua)
Algoritmi	ECDSA, käyrä secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Julkinen avain (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
Julkisen avaimen SHA-256	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Käytössä alkaen	2026-09-25T21:52:43Z

Vakuutan, että palvelu on luonut tämän avaimen yksinomaisessa hallinnassani, että sillä allekirjoitetut kuitit myöntää edellä kuvattu palvelu ja että julkaisen tämän avaimen käytöstä poistamisen osoitteessa `/keys.json`.

4. KUITIN TARKISTAMINEN

1. Tarkista, että tässä PDF-tiedostossa on vakuuttajan pätevä eIDAS-allekirjoitus (esim. EU DSS -validaattorilla).
2. Ota kuitti `{alg, key_id, payload, signature}` ja varmista, että `key_id` ja julkinen avain vastaavat kohtaa 3.
3. Tarkista ECDSA-allekirjoitus (64 tavun `r‖s`, hex) kentän `payload` tarkkojen UTF-8-tavujen SHA-256-tiivisteestä tai lähetä kuitti osoitteeseen `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Tarkista, että kentän `payload` arvo `verified_at` osuu avaimen voimassaoloaikaan.