TLSNotary notaro pasirašymo rakto deklaracija

Paslauga: `pavoltravnik.witness.directcase.ai` · **Dokumento versija:** 1.0 · **Data:** 2026 m. rugsėjo 26 d.

> **BANDOMASIS REŽIMAS.** Paslauga yra eksperimentinė ir teikiama be jokių garantijų. Kvitai skirti tik testavimui ir vertinimui, jais negalima remtis kaip įrodymais teisiniais, finansiniais ar kitais svarbiais klausimais. Toliau nurodytas raktas gali būti bet kada išimtas iš naudojimo; jo istorija skelbiama `/keys.json`.

1. DEKLARANTAS

Ing. Mgr. Pavol Trávnik, gimęs 1991 m. liepos 22 d., Zborovská 124/68, Malá Strana, 150 00 Praha 5, Čekijos Respublika, veikiantis kaip **fizinis asmuo** ir vienintelis paslaugos operatorius.

2. KĄ ATLIEKA PASLAUGA

Paslauga yra atvirojo kodo protokolu TLSNotary pagrįstas *notaras* (tikrintojas, angl. *notary/verifier*). Kai naudotojas (*įrodinėtojas*, angl. *prover*) įkelia tinklalapį per HTTPS, notaras dalyvauja TLS seanse — daugiašalio skaičiavimo būdu (MPC-TLS) arba kaip tarpinis serveris —, negalėdamas suklastoti serverio duomenų. Įrodinėtojas gali paslėpti privačias dalis; tuomet notaras pasirašo **kvitą**: kriptografinį įsipareigojimą (commitment) dėl serverio tapatybės (patikrintos pagal jo TLS sertifikatą) ir atskleisto turinio, nurodant patikrinimo laiką. Bet kas vėliau gali patikrinti kvitą nepasitikėdamas įrodinėtoju.

Galiojantis kvitas įrodo, kad atskleistą turinį nurodytu laiku per TLS pateikė įvardytas serveris ir kad šis notaras tai paliudijo. **Jis neįrodo**, kad turinys yra teisingas, nei nieko apie paslėptas dalis. Notaras veikia nepriklausomai nuo svetainių, kurias stebi.

3. DEKLARUOJAMAS PASIRAŠYMO RAKTAS

Rakto ID	`73a6bdba645a59e4` (pirmieji 8 viešojo rakto SHA-256 baitai)
Algoritmas	ECDSA, kreivė secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Viešasis raktas (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
Viešojo rakto SHA-256	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktyvus nuo	2026-09-25T21:52:43Z

Pareiškiu, kad šį raktą sugeneravo paslauga, esant mano išimtinei kontrolei, kad juo pasirašytus kvitus išduoda pirmiau aprašyta paslauga ir kad šio rakto išėmimą iš naudojimo paskelbsiu `/keys.json`.

4. KAIP PATIKRINTI KVITĄ

1. Patikrinkite, ar šiame PDF yra galiojantis deklaranto eIDAS parašas (pvz., naudojant EU DSS tikrinimo priemonę).
2. Paimkite kvitą `{alg, key_id, payload, signature}` ir įsitikinkite, kad `key_id` ir viešasis raktas atitinka 3 skirsnį.
3. Patikrinkite ECDSA parašą (64 baitų `r‖s`, hex) pagal tikslių lauko `payload` UTF-8 baitų SHA-256 arba nusiųskite kvitą adresu `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Patikrinkite, ar lauke `payload` esanti `verified_at` reikšmė patenka į rakto aktyvumo laikotarpį.