TLSNotary notāra parakstīšanas atslēgas deklarācija

Pakalpojums: `pavoltravnik.witness.directcase.ai` · **Dokumenta versija:** 1.0 · **Datums:** 2026. gada 26. septembris

> **TESTA REŽĪMS.** Pakalpojums ir eksperimentāls un tiek sniegts bez jebkādām garantijām. Kvītis ir paredzētas tikai testēšanai un novērtēšanai, un uz tām nedrīkst paļauties kā uz pierādījumu juridiskos, finanšu vai citos būtiskos jautājumos. Turpmāk norādīto atslēgu var jebkurā laikā izņemt no lietošanas; tās vēsture tiek publicēta `/keys.json`.

1. DEKLARĒTĀJS

Ing. Mgr. Pavol Trávnik, dzimis 1991. gada 22. jūlijā, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Čehijas Republika, kas rīkojas kā **fiziska persona** un vienīgais pakalpojuma operators.

2. PAKALPOJUMA BŪTĪBA

Pakalpojums ir *notārs* (verificētājs, angl. *notary/verifier*), kas balstīts uz atvērtā koda protokolu TLSNotary. Kad lietotājs (*pierādītājs*, angl. *prover*) ielādē tīmekļa lapu, izmantojot HTTPS, notārs piedalās TLS sesijā — ar daudzpusēju skaitļošanu (MPC-TLS) vai kā starpniekserveris —, nespējot viltot servera datus. Pierādītājs var aizklāt privātās daļas; pēc tam notārs paraksta **kvīti**: kriptogrāfisku saistību (commitment) attiecībā uz servera identitāti (pārbaudītu pēc tā TLS sertifikāta) un atklāto saturu, norādot verifikācijas laiku. Ikviens vēlāk var pārbaudīt kvīti, neuzticoties pierādītājam.

Derīga kvīts pierāda, ka atklāto saturu norādītajā laikā, izmantojot TLS, ir nosūtījis nosauktais serveris un ka šis notārs to ir apliecinājis. **Tā nepierāda**, ka saturs ir patiess, ne arī neko par aizklātajām daļām. Notārs darbojas neatkarīgi no tīmekļa vietnēm, kuras tas novēro.

3. DEKLARĒTĀ PARAKSTĪŠANAS ATSLĒGA

Atslēgas ID	`73a6bdba645a59e4` (publiskās atslēgas SHA-256 pirmie 8 baiti)
Algoritms	ECDSA, līkne secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Publiskā atslēga (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
Publiskās atslēgas SHA-256	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktīva kopš	2026-09-25T21:52:43Z

Es apliecinu, ka šo atslēgu ir ģenerējis pakalpojums manā vienpersoniskā kontrolē, ka ar to parakstītās kvītis izsniedz iepriekš aprakstītais pakalpojums un ka šīs atslēgas izņemšanu no lietošanas es publicēšu `/keys.json`.

4. KĀ PĀRBAUDĪT KVĪTI

1. Pārbaudiet, vai šim PDF ir derīgs deklarētāja eIDAS paraksts (piem., ar EU DSS validatoru).
2. Ņemiet kvīti `{alg, key_id, payload, signature}` un pārliecinieties, ka `key_id` un publiskā atslēga atbilst 3. sadaļai.
3. Pārbaudiet ECDSA parakstu (64 baitu `r‖s`, hex) attiecībā pret lauka `payload` precīzo UTF-8 baitu SHA-256 vai nosūtiet kvīti uz `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Pārbaudiet, vai lauka `payload` vērtība `verified_at` ietilpst atslēgas aktivitātes periodā.