TLSNotary notari allkirjastamisvõtme deklaratsioon

Teenus: `pavoltravnik.witness.directcase.ai` · **Dokumendi versioon:** 1.0 · **Kuupäev:** 26. september 2026

> **TESTREŽIIM.** Teenus on eksperimentaalne ja seda osutatakse ilma igasuguse garantiita. Kviitungid on mõeldud üksnes testimiseks ja hindamiseks ning neid ei tohi kasutada tõendina õiguslikes, finants- ega muudes olulistes küsimustes. Allpool nimetatud võtme võib igal ajal kasutusest kõrvaldada; selle ajalugu avaldatakse aadressil `/keys.json`.

1. DEKLARANT

Ing. Mgr. Pavol Trávnik, sündinud 22. juulil 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Tšehhi Vabariik, kes tegutseb **füüsilise isikuna** ja teenuse ainsa osutajana.

2. TEENUSE SISU

Teenus on avatud lähtekoodiga protokollil TLSNotary põhinev *notar* (tõendaja, ingl *notary/verifier*). Kui kasutaja (*tõestaja*, ingl *prover*) laadib veebilehe HTTPS-i kaudu, osaleb notar TLS-seansis — mitme osapoole arvutuse (MPC-TLS) abil või proksina — ilma et tal oleks võimalik serveri andmeid võltsida. Tõestaja võib privaatsed osad varjata; seejärel allkirjastab notar **kviitungi**: krüptograafilise kinnituse (commitment) serveri identiteedi (kontrollitud selle TLS-sertifikaadi alusel) ja avalikustatud sisu kohta koos kontrollimise ajaga. Igaüks saab kviitungit hiljem kontrollida tõestajat usaldamata.

Kehtiv kviitung tõendab, et avalikustatud sisu edastas nimetatud server TLS-i kaudu märgitud ajal ja et see notar oli selle tunnistajaks. **See ei tõenda** sisu õigsust ega midagi varjatud osade kohta. Notarit käitatakse sõltumatult veebisaitidest, mida ta jälgib.

3. DEKLAREERITUD ALLKIRJASTAMISVÕTI

Võtme ID	`73a6bdba645a59e4` (avaliku võtme SHA-256 räsi esimesed 8 baiti)
Algoritm	ECDSA, kõver secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Avalik võti (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
Avaliku võtme SHA-256	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktiivne alates	2026-09-25T21:52:43Z

Kinnitan, et selle võtme genereeris teenus minu ainukontrolli all, et sellega allkirjastatud kviitungid väljastab eespool kirjeldatud teenus ning et avaldan selle võtme kasutusest kõrvaldamise aadressil `/keys.json`.

4. KVIITUNGI KONTROLLIMINE

1. Kontrollige, et käesolev PDF kannab deklarandi kehtivat eIDAS-allkirja (nt EU DSS valideerijaga).
2. Võtke kviitung `{alg, key_id, payload, signature}` ja veenduge, et `key_id` ja avalik võti vastavad punktile 3.
3. Kontrollige ECDSA allkirja (64-baidine `r‖s`, hex) välja `payload` täpsete UTF-8 baitide SHA-256 räsi suhtes või saatke kviitung aadressile `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Kontrollige, et välja `payload` väärtus `verified_at` jääb võtme aktiivsusperioodi piiresse.