Izjava o podpisnem ključu overitelja TLSNotary

Storitev: `pavoltravnik.witness.directcase.ai` · **Različica dokumenta:** 1.0 · **Datum:** 26. septembra 2026

> **TESTNI NAČIN.** Storitev je poskusna in se zagotavlja brez kakršnega koli jamstva. Potrdila so namenjena izključno preizkušanju in ocenjevanju in se nanje ni mogoče zanašati kot na dokaz v pravnih, finančnih ali drugih ključnih zadevah. Spodnji ključ se lahko kadar koli umakne; njegova zgodovina je objavljena na `/keys.json`.

1. IZJAVITELJ

Ing. Mgr. Pavol Trávnik, rojen 22. julija 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Češka republika, ki deluje kot **fizična oseba** in edini upravljavec storitve.

2. KAJ STORITEV POČNE

Storitev je *overitelj* (notary, verifier), zgrajen na odprtokodnem protokolu TLSNotary. Ko uporabnik (*dokazovalec*, prover) naloži spletno stran prek HTTPS, overitelj sodeluje v seji TLS — z večstranskim izračunom (MPC-TLS) ali kot posrednik (proxy) — ne da bi lahko ponaredil podatke strežnika. Dokazovalec lahko zasebne dele prikrije; overitelj nato podpiše **potrdilo**: zavezo (commitment) k identiteti strežnika (preverjeni na podlagi njegovega potrdila TLS) in k razkriti vsebini, skupaj s časom preverjanja. Vsakdo lahko potrdilo pozneje preveri, ne da bi moral zaupati dokazovalcu.

Veljavno potrdilo dokazuje, da je navedeni strežnik razkrito vsebino ob navedenem času posredoval prek TLS in da je bil ta overitelj temu priča. **Ne dokazuje** resničnosti vsebine niti ničesar o prikritih delih. Overitelj deluje neodvisno od spletnih mest, ki jih opazuje.

3. PRIJAVLJENI PODPISNI KLJUČ

ID ključa	`73a6bdba645a59e4` (prvih 8 bajtov SHA-256 javnega ključa)
Algoritem	ECDSA, krivulja secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Javni ključ (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 javnega ključa	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktiven od	2026-09-25T21:52:43Z

Izjavljam, da je ta ključ ustvarila storitev pod mojim izključnim nadzorom, da potrdila, podpisana z njim, izdaja zgoraj opisana storitev in da bom umik tega ključa objavil na `/keys.json`.

4. KAKO PREVERITI POTRDILO

1. Preverite, ali ta dokument PDF nosi veljaven podpis eIDAS izjavitelja (npr. z validatorjem EU DSS).
2. Vzemite potrdilo `{alg, key_id, payload, signature}` in potrdite, da se `key_id` in javni ključ ujemata z razdelkom 3.
3. Preverite podpis ECDSA (64 bajtov `r‖s`, hex) nad SHA-256 točnih bajtov UTF-8 vrednosti `payload` ali potrdilo pošljite na `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Preverite, ali `verified_at` v `payload` spada v obdobje aktivnosti ključa.