Izjava o ključu za potpisivanje TLSNotary ovjeritelja

Usluga: `pavoltravnik.witness.directcase.ai` · **Verzija dokumenta:** 1.0 · **Datum:** 26. rujna 2026.

> **TESTNI NAČIN RADA.** Usluga je eksperimentalna i pruža se bez ikakva jamstva. Potvrde su namijenjene isključivo testiranju i procjeni te se na njih ne smije oslanjati kao na dokaz u pravnim, financijskim ili drugim kritičnim stvarima. Ključ u nastavku može se u bilo kojem trenutku povući; njegova je povijest objavljena na `/keys.json`.

1. DAVATELJ IZJAVE

Ing. Mgr. Pavol Trávnik, rođen 22. srpnja 1991., Zborovská 124/68, Malá Strana, 150 00 Praha 5, Češka Republika, koji djeluje kao **fizička osoba** i jedini operater usluge.

2. ŠTO USLUGA RADI

Usluga je *ovjeritelj* (engl. *notary*, verifikator) izgrađen na protokolu otvorenog koda TLSNotary. Kada korisnik (*dokazivatelj*, engl. *prover*) učita web-stranicu putem HTTPS-a, ovjeritelj sudjeluje u TLS sesiji – višestranačkim izračunom (MPC-TLS) ili kao posrednik (proxy) – a da pritom ne može krivotvoriti podatke poslužitelja. Dokazivatelj može prikriti privatne dijelove; ovjeritelj zatim potpisuje **potvrdu**: obvezu (commitment) na identitet poslužitelja (provjeren prema njegovu TLS certifikatu) i na otkriveni sadržaj, uz vrijeme provjere. Svatko može naknadno provjeriti potvrdu bez potrebe za povjerenjem u dokazivatelja.

Valjana potvrda dokazuje da je otkriveni sadržaj putem TLS-a poslužio navedeni poslužitelj u navedeno vrijeme te da je tomu svjedočio ovaj ovjeritelj. **Ona ne dokazuje** da je sadržaj istinit niti išta o prikrivenim dijelovima. Ovjeritelj djeluje neovisno o web-stranicama koje promatra.

3. PRIJAVLJENI KLJUČ ZA POTPISIVANJE

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

Izjavljujem da je ovaj ključ generirala usluga pod mojom isključivom kontrolom, da potvrde potpisane njime izdaje prethodno opisana usluga te da ću povlačenje ovog ključa objaviti na `/keys.json`.

4. KAKO PROVJERITI POTVRDU

1. Provjerite nosi li ovaj PDF valjani eIDAS potpis davatelja izjave (npr. validatorom EU DSS).
2. Uzmite potvrdu `{alg, key_id, payload, signature}` i provjerite odgovaraju li `key_id` i javni ključ odjeljku 3.
3. Provjerite ECDSA potpis (64 bajta `r||s`, hex) nad SHA-256 točnih UTF-8 bajtova polja `payload` ili pošaljite potvrdu na `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Provjerite je li `verified_at` u sadržaju unutar razdoblja aktivnosti ključa.