Prohlášení o podpisovém klíči ověřovatele TLSNotary

Služba: `pavoltravnik.witness.directcase.ai` · **Verze dokumentu:** 1.0 · **Datum:** 26. září 2026

> **TESTOVACÍ REŽIM.** Služba je experimentální a poskytuje se bez jakékoli záruky. Potvrzení jsou určena výhradně k testování a hodnocení a nelze se na ně spoléhat jako na důkaz v právních, finančních ani jiných zásadních věcech. Níže uvedený klíč může být kdykoli vyřazen; jeho historie je zveřejněna na `/keys.json`.

1. PROHLAŠUJÍCÍ

Ing. Mgr. Pavol Trávnik, nar. 22. července 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Česká republika, jednající jako **fyzická osoba** a výhradní provozovatel služby.

2. CO SLUŽBA DĚLÁ

Služba je *ověřovatelem* (notary, verifier) postaveným na otevřeném protokolu TLSNotary. Když uživatel (*prokazující*, prover) načte webovou stránku přes HTTPS, ověřovatel se účastní relace TLS — vícestranným výpočtem (MPC-TLS) nebo jako proxy — aniž by mohl data serveru padělat. Prokazující může soukromé části skrýt; ověřovatel poté podepíše **potvrzení**: závazek (commitment) k identitě serveru (ověřené podle jeho certifikátu TLS) a ke zpřístupněnému obsahu, spolu s časem ověření. Kdokoli může potvrzení později ověřit, aniž by musel prokazujícímu důvěřovat.

Platné potvrzení prokazuje, že zpřístupněný obsah byl v uvedeném čase doručen přes TLS uvedeným serverem a že tomu byl tento ověřovatel svědkem. **Neprokazuje** pravdivost obsahu ani nic o skrytých částech. Ověřovatel je provozován nezávisle na webových stránkách, které sleduje.

3. PROHLAŠOVANÝ PODPISOVÝ KLÍČ

ID klíče	`73a6bdba645a59e4` (prvních 8 bajtů SHA-256 veřejného klíče)
Algoritmus	ECDSA, křivka secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Veřejný klíč (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 veřejného klíče	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktivní od	2026-09-25T21:52:43Z

Prohlašuji, že tento klíč byl vygenerován službou pod mou výhradní kontrolou, že potvrzení jím podepsaná vydává výše popsaná služba a že vyřazení tohoto klíče zveřejním na `/keys.json`.

4. JAK OVĚŘIT POTVRZENÍ

1. Ověřte, že tento dokument PDF nese platný podpis eIDAS prohlašujícího (např. validátorem EU DSS).
2. Vezměte potvrzení `{alg, key_id, payload, signature}` a ověřte, že `key_id` a veřejný klíč odpovídají oddílu 3.
3. Ověřte podpis ECDSA (64 bajtů `r‖s`, hex) nad SHA-256 přesných bajtů UTF-8 hodnoty `payload`, nebo potvrzení zašlete na `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Ověřte, že `verified_at` v `payload` spadá do období platnosti klíče.

Elektronicky podepsáno prohlašujícím elektronickým podpisem podle nařízení (EU) č. 910/2014 (eIDAS).