Vyhlásenie o podpisovom kľúči overovateľa TLSNotary

Služba: `pavoltravnik.witness.directcase.ai` · **Verzia dokumentu:** 1.0 · **Dátum:** 26. septembra 2026

> **TESTOVACÍ REŽIM.** Služba je experimentálna a poskytuje sa bez akejkoľvek záruky. Potvrdenia sú určené výlučne na testovanie a hodnotenie a nemožno sa na ne spoliehať ako na dôkaz v právnych, finančných ani iných zásadných veciach. Nižšie uvedený kľúč môže byť kedykoľvek vyradený; jeho história je zverejnená na `/keys.json`.

1. VYHLASUJÚCI

Ing. Mgr. Pavol Trávnik, narodený 22. júla 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Česká republika, konajúci ako **fyzická osoba** a výhradný prevádzkovateľ služby.

2. ČO SLUŽBA ROBÍ

Služba je *overovateľom* (notary, verifier) postaveným na otvorenom protokole TLSNotary. Keď používateľ (*preukazujúci*, prover) načíta webovú stránku cez HTTPS, overovateľ sa zúčastní relácie TLS — viacstranným výpočtom (MPC-TLS) alebo ako proxy — bez toho, aby mohol údaje servera sfalšovať. Preukazujúci môže súkromné časti skryť; overovateľ potom podpíše **potvrdenie**: záväzok (commitment) k identite servera (overenej podľa jeho certifikátu TLS) a k sprístupnenému obsahu spolu s časom overenia. Ktokoľvek môže potvrdenie neskôr overiť bez toho, aby musel preukazujúcemu dôverovať.

Platné potvrdenie preukazuje, že sprístupnený obsah bol v uvedenom čase doručený cez TLS uvedeným serverom a že tento overovateľ bol toho svedkom. **Nepreukazuje** pravdivosť obsahu ani nič o skrytých častiach. Overovateľ je prevádzkovaný nezávisle od webových stránok, ktoré sleduje.

3. VYHLASOVANÝ PODPISOVÝ KĽÚČ

ID kľúča	`73a6bdba645a59e4` (prvých 8 bajtov SHA-256 verejného kľúča)
Algoritmus	ECDSA, krivka secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Verejný kľúč (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 verejného kľúča	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktívny od	2026-09-25T21:52:43Z

Vyhlasujem, že tento kľúč bol vygenerovaný službou pod mojou výhradnou kontrolou, že potvrdenia ním podpísané vydáva vyššie opísaná služba a že vyradenie tohto kľúča zverejním na `/keys.json`.

4. AKO OVERIŤ POTVRDENIE

1. Overte, že tento dokument PDF obsahuje platný podpis eIDAS vyhlasujúceho (napr. validátorom EU DSS).
2. Vezmite potvrdenie `{alg, key_id, payload, signature}` a overte, že `key_id` a verejný kľúč zodpovedajú oddielu 3.
3. Overte podpis ECDSA (64 bajtov `r‖s`, hex) nad SHA-256 presných bajtov UTF-8 hodnoty `payload`, alebo potvrdenie odošlite na `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Overte, že `verified_at` v `payload` spadá do obdobia platnosti kľúča.