Nyilatkozat a TLSNotary tanúsító aláírókulcsáról

Szolgáltatás: `pavoltravnik.witness.directcase.ai` · **Dokumentum verziója:** 1.0 · **Kelt:** 2026. szeptember 26.

> **TESZTÜZEMMÓD.** A szolgáltatás kísérleti jellegű, és mindennemű szavatosság nélkül érhető el. Az igazolások kizárólag tesztelési és értékelési célra szolgálnak, és jogi, pénzügyi vagy más kritikus ügyekben nem használhatók bizonyítékként. Az alábbi kulcs bármikor visszavonható; előzményei a `/keys.json` címen kerülnek közzétételre.

1. NYILATKOZATTEVŐ

Ing. Mgr. Pavol Trávnik, született: 1991. július 22., Zborovská 124/68, Malá Strana, 150 00 Praha 5, Cseh Köztársaság, aki **természetes személyként** és a szolgáltatás kizárólagos üzemeltetőjeként jár el.

2. A SZOLGÁLTATÁS MŰKÖDÉSE

A szolgáltatás a nyílt forráskódú TLSNotary protokollra épülő *tanúsító* (notary, ellenőrző). Amikor a felhasználó (a *bizonyító fél*, prover) HTTPS-en keresztül betölt egy weboldalt, a tanúsító részt vesz a TLS-munkamenetben – többfelű számítással (MPC-TLS) vagy proxyként –, anélkül hogy a szerver adatait meghamisíthatná. A bizonyító fél a magánjellegű részeket kitakarhatja; a tanúsító ezt követően aláír egy **igazolást** (receipt): a szerver (TLS-tanúsítványa alapján ellenőrzött) azonosságára és a feltárt tartalomra vonatkozó kötelezettségvállalást (commitment), az ellenőrzés időpontjával. Az igazolást később bárki ellenőrizheti anélkül, hogy a bizonyító félben meg kellene bíznia.

Az érvényes igazolás bizonyítja, hogy a feltárt tartalmat a megnevezett szerver a megjelölt időpontban TLS-en keresztül szolgáltatta, és hogy e tanúsító ennek tanúja volt. **Nem bizonyítja** a tartalom valóságát, sem a kitakart részekkel kapcsolatos bármely tényt. A tanúsítót az általa megfigyelt weboldalaktól függetlenül üzemeltetik.

3. A BEJELENTETT ALÁÍRÓKULCS

Kulcsazonosító	`73a6bdba645a59e4` (a nyilvános kulcs SHA-256 értékének első 8 bájtja)
Algoritmus	ECDSA, secp256k1 görbe, SHA-256 (`secp256k1-ecdsa-sha256`)
Nyilvános kulcs (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
Nyilvános kulcs SHA-256	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktív ettől	2026-09-25T21:52:43Z

Kijelentem, hogy e kulcsot a szolgáltatás kizárólagos ellenőrzésem alatt hozta létre, hogy az ezzel aláírt igazolásokat a fent leírt szolgáltatás bocsátja ki, és hogy e kulcs visszavonását a `/keys.json` címen közzéteszem.

4. AZ IGAZOLÁS ELLENŐRZÉSE

1. Ellenőrizze, hogy e PDF a nyilatkozattevő érvényes eIDAS-aláírását viseli (pl. az EU DSS validátorral).
2. Vegye az `{alg, key_id, payload, signature}` igazolást, és győződjön meg arról, hogy a `key_id` és a nyilvános kulcs megegyezik a 3. pontban foglaltakkal.
3. Ellenőrizze az ECDSA-aláírást (64 bájtos `r‖s`, hex) a `payload` pontos UTF-8 bájtjainak SHA-256 értékén, vagy küldje el az igazolást a `POST https://pavoltravnik.witness.directcase.ai/verify` címre.
4. Ellenőrizze, hogy a payloadban szereplő `verified_at` a kulcs aktív időszakán belül esik.