Declarație privind cheia de semnare a notarului TLSNotary

Serviciu: `pavoltravnik.witness.directcase.ai` · **Versiunea documentului:** 1.0 · **Data:** 26 septembrie 2026

> **MOD DE TEST.** Serviciul este experimental și este furnizat fără nicio garanție. Atestările sunt destinate exclusiv testării și evaluării și nu pot fi invocate ca probă în chestiuni juridice, financiare sau în alte chestiuni critice. Cheia de mai jos poate fi retrasă oricând; istoricul acesteia este publicat la `/keys.json`.

1. DECLARANT

Ing. Mgr. Pavol Trávnik, născut la 22 iulie 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Republica Cehă, acționând în calitate de **persoană fizică** și de operator unic al serviciului.

2. CE FACE SERVICIUL

Serviciul este un *notar* (notary, verificator) construit pe protocolul open-source TLSNotary. Când un utilizator (*probatorul*, prover) încarcă o pagină web prin HTTPS, notarul participă la sesiunea TLS – prin calcul multipartit (MPC-TLS) sau ca proxy – fără a putea falsifica datele serverului. Probatorul poate masca părțile private; notarul semnează apoi o **atestare** (receipt): un angajament (commitment) privind identitatea serverului (verificată pe baza certificatului său TLS) și conținutul divulgat, împreună cu momentul verificării. Oricine poate verifica ulterior atestarea fără a fi nevoit să aibă încredere în probator.

O atestare validă dovedește că conținutul divulgat a fost furnizat prin TLS de serverul indicat la momentul menționat, și că acest notar a fost martor la aceasta. **Nu dovedește** că acel conținut este adevărat și nici nimic privind părțile mascate. Notarul este operat independent de site-urile web pe care le observă.

3. CHEIA DE SEMNARE DECLARATĂ

Identificatorul cheii	`73a6bdba645a59e4` (primii 8 octeți ai SHA-256 al cheii publice)
Algoritm	ECDSA, curba secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Cheia publică (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 al cheii publice	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Activă de la	2026-09-25T21:52:43Z

Declar că această cheie a fost generată de serviciu sub controlul meu exclusiv, că atestările semnate cu aceasta sunt emise de serviciul descris mai sus și că voi publica retragerea acestei chei la `/keys.json`.

4. CUM SE VERIFICĂ O ATESTARE

1. Verificați că prezentul PDF poartă o semnătură eIDAS validă a declarantului (de ex. cu validatorul EU DSS).
2. Luați atestarea `{alg, key_id, payload, signature}` și confirmați că `key_id` și cheia publică corespund secțiunii 3.
3. Verificați semnătura ECDSA (`r‖s` de 64 de octeți, hex) asupra SHA-256 al octeților UTF-8 exacți ai `payload`, sau trimiteți atestarea la `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Verificați că `verified_at` din payload se încadrează în perioada de activitate a cheii.

Semnat electronic de declarant cu o semnătură electronică în temeiul Regulamentului (UE) nr. 910/2014 (eIDAS).