Verklaring betreffende een ondertekeningssleutel van een TLSNotary-notaris

Dienst: `pavoltravnik.witness.directcase.ai` · **Documentversie:** 1.0 · **Datum:** 26 september 2026

> **TESTMODUS.** De dienst is experimenteel en wordt zonder enige garantie aangeboden. Ontvangstbewijzen zijn uitsluitend bedoeld voor test- en evaluatiedoeleinden en mogen niet als bewijs worden gebruikt in juridische, financiële of andere kritieke aangelegenheden. De onderstaande sleutel kan te allen tijde buiten gebruik worden gesteld; de geschiedenis ervan wordt gepubliceerd op `/keys.json`.

1. VERKLAARDER

Ing. Mgr. Pavol Trávnik, geboren op 22 juli 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Tsjechische Republiek, handelend als **natuurlijke persoon** en enige exploitant van de dienst.

2. WAT DE DIENST DOET

De dienst is een *notaris* (notary, verifier) gebaseerd op het opensourceprotocol TLSNotary. Wanneer een gebruiker (de *bewijsvoerder*, prover) een webpagina via HTTPS laadt, neemt de notaris deel aan de TLS-sessie – via meerpartijenberekening (MPC-TLS) of als proxy – zonder de gegevens van de server te kunnen vervalsen. De bewijsvoerder kan privégedeelten afschermen; de notaris ondertekent vervolgens een **ontvangstbewijs**: een verbintenis (commitment) op de identiteit van de server (gecontroleerd aan de hand van zijn TLS-certificaat) en op de vrijgegeven inhoud, met het tijdstip van verificatie. Eenieder kan het ontvangstbewijs later controleren zonder de bewijsvoerder te hoeven vertrouwen.

Een geldig ontvangstbewijs bewijst dat de vrijgegeven inhoud op het vermelde tijdstip door de genoemde server via TLS is geleverd en dat deze notaris dit heeft waargenomen. **Het bewijst niet** dat de inhoud juist is, noch iets over afgeschermde gedeelten. De notaris wordt onafhankelijk geëxploiteerd van de websites die hij waarneemt.

3. VERKLAARDE ONDERTEKENINGSSLEUTEL

Sleutel-id	`73a6bdba645a59e4` (eerste 8 bytes van SHA-256 van de openbare sleutel)
Algoritme	ECDSA, curve secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Openbare sleutel (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 van openbare sleutel	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Actief sinds	2026-09-25T21:52:43Z

Ik verklaar dat deze sleutel door de dienst onder mijn uitsluitende controle is gegenereerd, dat daarmee ondertekende ontvangstbewijzen worden afgegeven door de hierboven beschreven dienst, en dat ik de buitengebruikstelling van deze sleutel zal publiceren op `/keys.json`.

4. EEN ONTVANGSTBEWIJS VERIFIËREN

1. Controleer dat deze PDF een geldige eIDAS-handtekening van de verklaarder draagt (bijv. met de EU DSS-validator).
2. Neem het ontvangstbewijs `{alg, key_id, payload, signature}` en bevestig dat `key_id` en de openbare sleutel overeenkomen met afdeling 3.
3. Verifieer de ECDSA-handtekening (64 bytes `r‖s`, hex) over SHA-256 van de exacte UTF-8-bytes van `payload`, of stuur het ontvangstbewijs naar `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Controleer dat `verified_at` in de payload binnen de actieve periode van de sleutel valt.

Elektronisch ondertekend door de verklaarder met een elektronische handtekening overeenkomstig Verordening (EU) nr. 910/2014 (eIDAS).