Declaração da chave de assinatura do notário TLSNotary

Serviço: `pavoltravnik.witness.directcase.ai` · **Versão do documento:** 1.0 · **Data:** 26 de setembro de 2026

> **MODO DE TESTE.** O serviço é experimental e é prestado sem qualquer garantia. Os recibos destinam-se exclusivamente a fins de ensaio e avaliação e não devem ser invocados como prova em matérias jurídicas, financeiras ou outras matérias críticas. A chave abaixo indicada pode ser retirada a qualquer momento; o respetivo histórico é publicado em `/keys.json`.

1. DECLARANTE

Ing. Mgr. Pavol Trávnik, nascido a 22 de julho de 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, República Checa, que atua na qualidade de **pessoa singular** e único operador do serviço.

2. FUNCIONAMENTO DO SERVIÇO

O serviço é um *notário técnico* (notary; verificador) baseado no protocolo de código aberto TLSNotary. Quando um utilizador (o *provador*) carrega uma página web através de HTTPS, o notário participa na sessão TLS — por computação multipartidária (MPC-TLS) ou como proxy — sem conseguir falsificar os dados do servidor. O provador pode ocultar partes privadas; o notário assina então um **recibo**: um compromisso criptográfico sobre a identidade do servidor (verificada face ao respetivo certificado TLS) e sobre o conteúdo divulgado, com a hora da verificação. Qualquer pessoa pode depois verificar o recibo sem ter de confiar no provador.

Um recibo válido prova que o conteúdo divulgado foi servido através de TLS pelo servidor identificado na hora indicada, e que este notário o testemunhou. **Não prova** que o conteúdo seja verdadeiro, nem nada quanto às partes ocultadas. O notário é explorado de forma independente dos sítios web que observa.

3. CHAVE DE ASSINATURA DECLARADA

Identificador da chave	`73a6bdba645a59e4` (primeiros 8 bytes do SHA-256 da chave pública)
Algoritmo	ECDSA, curva secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Chave pública (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 da chave pública	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Ativa desde	2026-09-25T21:52:43Z

Declaro que esta chave foi gerada pelo serviço sob o meu controlo exclusivo, que os recibos assinados com a mesma são emitidos pelo serviço acima descrito e que publicarei a retirada desta chave em `/keys.json`.

4. COMO VERIFICAR UM RECIBO

1. Verificar que o presente PDF contém uma assinatura eIDAS válida do declarante (p. ex., com o validador EU DSS).
2. Obter o recibo `{alg, key_id, payload, signature}` e confirmar que `key_id` e a chave pública correspondem à secção 3.
3. Verificar a assinatura ECDSA (`r‖s` de 64 bytes, hex) sobre o SHA-256 dos bytes UTF-8 exatos de `payload`, ou enviar o recibo para `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Verificar se o valor `verified_at` de `payload` se situa dentro do período de atividade da chave.

Assinado eletronicamente pelo declarante com uma assinatura eletrónica nos termos do Regulamento (UE) n.º 910/2014 (eIDAS).