Declaración de la clave de firma del notario TLSNotary

Servicio: `pavoltravnik.witness.directcase.ai` · **Versión del documento:** 1.0 · **Fecha:** 26 de septiembre de 2026

> **MODO DE PRUEBA.** El servicio es experimental y se presta sin garantía alguna. Los recibos están destinados únicamente a fines de ensayo y evaluación y no deben invocarse como medio de prueba en asuntos jurídicos, financieros u otros asuntos críticos. La clave que figura a continuación puede retirarse en cualquier momento; su historial se publica en `/keys.json`.

1. DECLARANTE

Ing. Mgr. Pavol Trávnik, nacido el 22 de julio de 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, República Checa, que actúa en calidad de **persona física** y único operador del servicio.

2. OBJETO DEL SERVICIO

El servicio es un *notario técnico* (notary; verificador) basado en el protocolo de código abierto TLSNotary. Cuando un usuario (el *probador*) carga una página web mediante HTTPS, el notario participa en la sesión TLS —mediante computación multipartita (MPC-TLS) o como proxy— sin poder falsificar los datos del servidor. El probador puede ocultar las partes privadas; a continuación, el notario firma un **recibo**: un compromiso criptográfico sobre la identidad del servidor (comprobada frente a su certificado TLS) y sobre el contenido revelado, junto con la hora de la verificación. Cualquiera puede comprobar después el recibo sin tener que confiar en el probador.

Un recibo válido prueba que el contenido revelado fue servido mediante TLS por el servidor indicado en el momento señalado, y que este notario fue testigo de ello. **No prueba** que el contenido sea veraz, ni nada respecto de las partes ocultas. El notario se opera de forma independiente de los sitios web que observa.

3. CLAVE DE FIRMA DECLARADA

Identificador de clave	`73a6bdba645a59e4` (primeros 8 bytes del SHA-256 de la clave pública)
Algoritmo	ECDSA, curva secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Clave pública (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 de la clave pública	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Activa desde	2026-09-25T21:52:43Z

Declaro que esta clave fue generada por el servicio bajo mi control exclusivo, que los recibos firmados con ella son emitidos por el servicio descrito anteriormente y que publicaré la retirada de esta clave en `/keys.json`.

4. CÓMO VERIFICAR UN RECIBO

1. Comprobar que este PDF lleva una firma eIDAS válida del declarante (p. ej., con el validador EU DSS).
2. Tomar el recibo `{alg, key_id, payload, signature}` y confirmar que `key_id` y la clave pública coinciden con la sección 3.
3. Verificar la firma ECDSA (`r‖s` de 64 bytes, hex) sobre el SHA-256 de los bytes UTF-8 exactos de `payload`, o enviar el recibo a `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Comprobar que el valor `verified_at` de `payload` se encuentra dentro del período de actividad de la clave.

Firmado electrónicamente por el declarante mediante firma electrónica con arreglo al Reglamento (UE) n.º 910/2014 (eIDAS).