Déclaration relative à la clé de signature du notaire TLSNotary

Service : `pavoltravnik.witness.directcase.ai` · **Version du document :** 1.0 · **Date :** 26 septembre 2026

> **MODE TEST.** Le service est expérimental et fourni sans aucune garantie. Les reçus sont destinés exclusivement à des fins d'essai et d'évaluation et ne doivent pas être invoqués comme preuve dans des affaires juridiques, financières ou autres matières critiques. La clé ci-dessous peut être retirée à tout moment ; son historique est publié à `/keys.json`.

1. DÉCLARANT

Ing. Mgr. Pavol Trávnik, né le 22 juillet 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, République tchèque, agissant en qualité de **personne physique** et d'exploitant unique du service.

2. OBJET DU SERVICE

Le service est un *notaire technique* (notary ; vérificateur) fondé sur le protocole open source TLSNotary. Lorsqu'un utilisateur (le *prouveur*) charge une page web via HTTPS, le notaire participe à la session TLS — par calcul multipartite (MPC-TLS) ou en tant que proxy — sans pouvoir falsifier les données du serveur. Le prouveur peut masquer les parties privées ; le notaire signe alors un **reçu** : un engagement cryptographique sur l'identité du serveur (vérifiée au regard de son certificat TLS) et sur le contenu divulgué, ainsi que l'heure de la vérification. Quiconque peut ensuite vérifier le reçu sans devoir se fier au prouveur.

Un reçu valide prouve que le contenu divulgué a été servi via TLS par le serveur désigné à l'heure indiquée, et que le présent notaire en a été témoin. **Il ne prouve pas** que ce contenu est véridique, ni quoi que ce soit concernant les parties masquées. Le notaire est exploité indépendamment des sites web qu'il observe.

3. CLÉ DE SIGNATURE DÉCLARÉE

Identifiant de clé	`73a6bdba645a59e4` (8 premiers octets du SHA-256 de la clé publique)
Algorithme	ECDSA, courbe secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Clé publique (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 de la clé publique	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Active depuis	2026-09-25T21:52:43Z

Je déclare que cette clé a été générée par le service sous mon contrôle exclusif, que les reçus signés au moyen de celle-ci sont émis par le service décrit ci-dessus et que je publierai le retrait de cette clé à `/keys.json`.

4. VÉRIFICATION D'UN REÇU

1. Vérifier que le présent PDF porte une signature eIDAS valide du déclarant (p. ex. au moyen du validateur EU DSS).
2. Prendre le reçu `{alg, key_id, payload, signature}` et confirmer que `key_id` et la clé publique correspondent à la section 3.
3. Vérifier la signature ECDSA (`r‖s` de 64 octets, hex) sur le SHA-256 des octets UTF-8 exacts de `payload`, ou envoyer le reçu à `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Vérifier que la valeur `verified_at` de `payload` se situe dans la période d'activité de la clé.

Signé électroniquement par le déclarant au moyen d'une signature électronique au sens du règlement (UE) n° 910/2014 (eIDAS).