Декларация за ключа за подписване на удостоверител TLSNotary

Услуга: `pavoltravnik.witness.directcase.ai` · **Версия на документа:** 1.0 · **Дата:** 26 септември 2026 г.

> **ТЕСТОВ РЕЖИМ.** Услугата е експериментална и се предоставя без каквато и да е гаранция. Разписките са предназначени единствено за изпитване и оценка и не могат да се използват като доказателство по правни, финансови или други критични въпроси. Посоченият по-долу ключ може да бъде оттеглен по всяко време; историята му се публикува на `/keys.json`.

1. ДЕКЛАРАТОР

Ing. Mgr. Pavol Trávnik, роден на 22 юли 1991 г., Zborovská 124/68, Malá Strana, 150 00 Praha 5, Чешка република, действащ като **физическо лице** и единствен оператор на услугата.

2. КАКВО ИЗВЪРШВА УСЛУГАТА

Услугата е *удостоверител* (notary, проверяващ), изграден върху протокола с отворен код TLSNotary. Когато потребител (*доказващият*, prover) зарежда уеб страница чрез HTTPS, удостоверителят участва в TLS сесията – чрез многостранно изчисление (MPC-TLS) или като прокси – без да може да подправи данните на сървъра. Доказващият може да скрие частни части; след това удостоверителят подписва **разписка** (receipt): обвързване (commitment) с идентичността на сървъра (проверена спрямо неговия TLS сертификат) и с разкритото съдържание, заедно с момента на проверката. Всеки може по-късно да провери разписката, без да е необходимо да се доверява на доказващия.

Валидната разписка доказва, че разкритото съдържание е предоставено чрез TLS от посочения сървър в посочения момент и че този удостоверител е бил свидетел на това. **Тя не доказва**, че съдържанието е вярно, нито каквото и да е относно скритите части. Удостоверителят се управлява независимо от уебсайтовете, които наблюдава.

3. ДЕКЛАРИРАН КЛЮЧ ЗА ПОДПИСВАНЕ

Идентификатор на ключа	`73a6bdba645a59e4` (първите 8 байта от SHA-256 на публичния ключ)
Алгоритъм	ECDSA, крива secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Публичен ключ (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 на публичния ключ	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Активен от	2026-09-25T21:52:43Z

Декларирам, че този ключ е генериран от услугата под мой изключителен контрол, че подписаните с него разписки се издават от описаната по-горе услуга и че ще публикувам оттеглянето на този ключ на `/keys.json`.

4. КАК СЕ ПРОВЕРЯВА РАЗПИСКА

1. Проверете дали този PDF носи валиден eIDAS подпис на декларатора (напр. чрез валидатора EU DSS).
2. Вземете разписката `{alg, key_id, payload, signature}` и потвърдете, че `key_id` и публичният ключ съответстват на раздел 3.
3. Проверете ECDSA подписа (64-байтов `r‖s`, hex) върху SHA-256 на точните UTF-8 байтове на `payload` или изпратете разписката на `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Проверете дали `verified_at` в payload попада в периода на активност на ключа.

Подписано електронно от декларатора с електронен подпис съгласно Регламент (ЕС) № 910/2014 (eIDAS).