Oświadczenie dotyczące klucza podpisującego weryfikatora TLSNotary

Usługa: `pavoltravnik.witness.directcase.ai` · **Wersja dokumentu:** 1.0 · **Data:** 26 września 2026 r.

> **TRYB TESTOWY.** Usługa ma charakter eksperymentalny i jest świadczona bez jakiejkolwiek gwarancji. Poświadczenia są przeznaczone wyłącznie do testów i oceny i nie mogą stanowić podstawy dowodowej w sprawach prawnych, finansowych ani innych istotnych. Poniższy klucz może zostać w każdej chwili wycofany; jego historia jest publikowana pod `/keys.json`.

1. SKŁADAJĄCY OŚWIADCZENIE

Ing. Mgr. Pavol Trávnik, urodzony 22 lipca 1991 r., Zborovská 124/68, Malá Strana, 150 00 Praha 5, Republika Czeska, działający jako **osoba fizyczna** i wyłączny operator usługi.

2. DZIAŁANIE USŁUGI

Usługa jest *weryfikatorem* (notary, verifier) opartym na otwartoźródłowym protokole TLSNotary. Gdy użytkownik (*dowodzący*, prover) wczytuje stronę internetową przez HTTPS, weryfikator uczestniczy w sesji TLS — w drodze obliczeń wielostronnych (MPC-TLS) lub jako proxy — bez możliwości sfałszowania danych serwera. Dowodzący może ukryć części prywatne; weryfikator podpisuje następnie **poświadczenie**: zobowiązanie (commitment) do tożsamości serwera (sprawdzonej na podstawie jego certyfikatu TLS) i do ujawnionej treści, wraz z czasem weryfikacji. Każdy może później sprawdzić poświadczenie bez zaufania do dowodzącego.

Ważne poświadczenie dowodzi, że ujawniona treść została przekazana przez TLS przez wskazany serwer we wskazanym czasie i że ten weryfikator był tego świadkiem. **Nie dowodzi** prawdziwości treści ani niczego w zakresie części ukrytych. Weryfikator jest prowadzony niezależnie od obserwowanych stron internetowych.

3. DEKLAROWANY KLUCZ PODPISUJĄCY

Identyfikator klucza	`73a6bdba645a59e4` (pierwsze 8 bajtów SHA-256 klucza publicznego)
Algorytm	ECDSA, krzywa secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Klucz publiczny (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 klucza publicznego	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Aktywny od	2026-09-25T21:52:43Z

Oświadczam, że niniejszy klucz został wygenerowany przez usługę pod moją wyłączną kontrolą, że podpisane nim poświadczenia są wydawane przez opisaną powyżej usługę oraz że wycofanie tego klucza opublikuję pod `/keys.json`.

4. JAK ZWERYFIKOWAĆ POŚWIADCZENIE

1. Sprawdź, czy niniejszy dokument PDF opatrzony jest ważnym podpisem eIDAS składającego oświadczenie (np. walidatorem EU DSS).
2. Pobierz poświadczenie `{alg, key_id, payload, signature}` i potwierdź, że `key_id` i klucz publiczny są zgodne z sekcją 3.
3. Zweryfikuj podpis ECDSA (64 bajty `r‖s`, hex) nad SHA-256 dokładnych bajtów UTF-8 wartości `payload` lub wyślij poświadczenie na `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Sprawdź, czy `verified_at` w `payload` mieści się w okresie aktywności klucza.