Δήλωση κλειδιού υπογραφής πιστοποιητή TLSNotary

Υπηρεσία: `pavoltravnik.witness.directcase.ai` · **Έκδοση εγγράφου:** 1.0 · **Ημερομηνία:** 26 Σεπτεμβρίου 2026

> **ΛΕΙΤΟΥΡΓΙΑ ΔΟΚΙΜΗΣ.** Η υπηρεσία είναι πειραματική και παρέχεται χωρίς καμία εγγύηση. Οι βεβαιώσεις προορίζονται αποκλειστικά για δοκιμές και αξιολόγηση και δεν επιτρέπεται να χρησιμοποιούνται ως αποδεικτικό μέσο σε νομικά, οικονομικά ή άλλα κρίσιμα ζητήματα. Το κατωτέρω κλειδί μπορεί να αποσυρθεί ανά πάσα στιγμή· το ιστορικό του δημοσιεύεται στο `/keys.json`.

1. ΔΗΛΩΝ

Ing. Mgr. Pavol Trávnik, γεννηθείς στις 22 Ιουλίου 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Τσεχική Δημοκρατία, ενεργών ως **φυσικό πρόσωπο** και αποκλειστικός φορέας λειτουργίας της υπηρεσίας.

2. ΤΙ ΚΑΝΕΙ Η ΥΠΗΡΕΣΙΑ

Η υπηρεσία είναι *πιστοποιητής* (notary, επαληθευτής) βασισμένος στο πρωτόκολλο ανοικτού κώδικα TLSNotary. Όταν ένας χρήστης (ο *αποδεικνύων*, prover) φορτώνει μια ιστοσελίδα μέσω HTTPS, ο πιστοποιητής συμμετέχει στη συνεδρία TLS – μέσω πολυμερούς υπολογισμού (MPC-TLS) ή ως διακομιστής μεσολάβησης (proxy) – χωρίς να μπορεί να πλαστογραφήσει τα δεδομένα του διακομιστή. Ο αποδεικνύων μπορεί να αποκρύψει ιδιωτικά τμήματα· ο πιστοποιητής υπογράφει στη συνέχεια **βεβαίωση** (receipt): δέσμευση (commitment) ως προς την ταυτότητα του διακομιστή (ελεγμένη βάσει του πιστοποιητικού TLS του) και ως προς το αποκαλυφθέν περιεχόμενο, με τον χρόνο της επαλήθευσης. Οποιοσδήποτε μπορεί αργότερα να ελέγξει τη βεβαίωση χωρίς να εμπιστεύεται τον αποδεικνύοντα.

Μια έγκυρη βεβαίωση αποδεικνύει ότι το αποκαλυφθέν περιεχόμενο παρασχέθηκε μέσω TLS από τον κατονομαζόμενο διακομιστή κατά τον αναφερόμενο χρόνο και ότι ο παρών πιστοποιητής υπήρξε μάρτυρας αυτού. **Δεν αποδεικνύει** ότι το περιεχόμενο είναι αληθές, ούτε οτιδήποτε σχετικά με τα αποκρυφθέντα τμήματα. Ο πιστοποιητής λειτουργεί ανεξάρτητα από τους ιστοτόπους που παρατηρεί.

3. ΔΗΛΟΥΜΕΝΟ ΚΛΕΙΔΙ ΥΠΟΓΡΑΦΗΣ

Αναγνωριστικό κλειδιού	`73a6bdba645a59e4` (τα πρώτα 8 byte του SHA-256 του δημόσιου κλειδιού)
Αλγόριθμος	ECDSA, καμπύλη secp256k1, SHA-256 (`secp256k1-ecdsa-sha256`)
Δημόσιο κλειδί (SEC1, hex)	`029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744`
SHA-256 δημόσιου κλειδιού	`73a6bdba645a59e4ce5641cfa5fbe8e7bf0aad33e90004cc803ecf3ff47f181f`
Ενεργό από	2026-09-25T21:52:43Z

Δηλώνω ότι το κλειδί αυτό δημιουργήθηκε από την υπηρεσία υπό τον αποκλειστικό μου έλεγχο, ότι οι βεβαιώσεις που υπογράφονται με αυτό εκδίδονται από την ανωτέρω περιγραφόμενη υπηρεσία και ότι θα δημοσιεύσω την απόσυρση του κλειδιού αυτού στο `/keys.json`.

4. ΠΩΣ ΕΠΑΛΗΘΕΥΕΤΑΙ ΜΙΑ ΒΕΒΑΙΩΣΗ

1. Ελέγξτε ότι το παρόν PDF φέρει έγκυρη υπογραφή eIDAS του δηλούντος (π.χ. με τον επικυρωτή EU DSS).
2. Λάβετε τη βεβαίωση `{alg, key_id, payload, signature}` και επιβεβαιώστε ότι το `key_id` και το δημόσιο κλειδί συμφωνούν με την ενότητα 3.
3. Επαληθεύστε την υπογραφή ECDSA (`r‖s` 64 byte, hex) επί του SHA-256 των ακριβών byte UTF-8 του `payload` ή αποστείλετε τη βεβαίωση στο `POST https://pavoltravnik.witness.directcase.ai/verify`.
4. Ελέγξτε ότι το `verified_at` στο payload εμπίπτει στο διάστημα ενεργότητας του κλειδιού.