

Dikjarazzjoni ta' Ċavetta tal-Iffirmar ta' Nutar TLSNotary

Servizz: pavoltravnik.witness.directcase.ai · Verzjoni tad-dokument: 1.0 · Data: 26 ta' Settembru 2026

MODALITÀ TA' TESTJAR. Is-servizz huwa sperimentali u jiġi pprovdut mingħajr garanzija. L-irċevuti huma maħsuba biss għall-ittestjar u l-evalwazzjoni u m'għandux isir affidament fuqhom bħala evidenza f'kwistjonijiet legali, finanzjarji jew kritiċi oħra. Iċ-ċavetta hawn taht tista' tiġi rtirata fi kwalunkwe ħin; l-istorja tagħha hija ppubblikata f'/keys.json.

1. DIKJARANT

Ing. Mgr. Pavol Trávník, imwieled fit-22 ta' Lulju 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Repubblika Ċeka, li qed jaġixxi bħala **persuna fiżika** u operatur uniku tas-servizz.

2. X'JAGHMEL IS-SERVIZZ

Is-servizz huwa *nutar* (verifikatur) mibni fuq il-protokoll b'sors miftuħ TLSNotary. Meta utent (il-*pruvatur*, *prover*) jiftaħ paġna web permezz ta' HTTPS, in-nutar jiehu sehem fis-sessjoni TLS — permezz ta' komputazzjoni b'diversi partijiet (MPC-TLS) jew bħala proxy — mingħajr ma jkun jista' jiffalsifika d-data tas-server. Il-pruvatur jista' jaħbi partijiet privati; imbagħad in-nutar jiffirma **irċevuta**: impenn (commitment) għall-identità tas-server (ivverifikata skont iċ-ċertifikat TLS tiegħu) u għall-kontenut żvelat, flimkien mal-ħin tal-verifika. Kulhadd jista' aktar tard jivverifika l-irċevuta mingħajr ma jkollu jafta lill-pruvatur.

Irċevuta valida tipprova li l-kontenut żvelat ġie servut permezz ta' TLS mis-server imsemmi fil-ħin iddikjarat, u li dan in-nutar kien xhud tiegħu. **Ma tipprovax** li l-kontenut huwa veru, u lanqas xejn dwar il-partijiet moħbija. In-nutar jithaddem b'mod indipendenti mis-siti web li josserva.

3. ĊAVETTA TAL-IFFIRMAR IDDIKJARATA

ID taċ-ċavetta	73a6bdba645a59e4 (l-ewwel 8 bytes tas-SHA-256 taċ-ċavetta pubblika)
Algoritmu	ECDSA, kurva secp256k1, SHA-256 (secp256k1-ecdsa-sha256)
Ċavetta pubblika (SEC1, hex)	029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744
SHA-256 taċ-ċavetta pubblika	73a6bdba645a59e4ce5641cfa5f8e8e7bf0aad33e90004cc803ecf3ff47f181f
Attiva minn	2026-09-25T21:52:43Z

Niddikjara li din iċ-ċavetta ġiet iġġenerata mis-servizz taht il-kontroll esklużiv tiegħi, li l-irċevuti ffirmati biha jinħarġu mis-servizz deskritt hawn fuq, u li se nipubblika l-irtirar ta' din iċ-ċavetta f'/keys.json.

4. KIF TIVVERIFIKA IRĊEVUTA

- Ivverifika li dan il-PDF iġorr firma eIDAS valida tad-dikjarant (eż. bil-validatur EU DSS).
- Hu l-irċevuta {alg, key_id, payload, signature} u kkonferma li key_id u ċ-ċavetta pubblika jaqblu mat-taqsima 3.
- Ivverifika l-firma ECDSA (64 byte r||s, hex) fuq is-SHA-256 tal-bytes UTF-8 eżatti ta' payload, jew ibgħat l-irċevuta lil POST <https://pavoltravnik.witness.directcase.ai/verify>.
- Ivverifika li verified_at fil-payload jaqa' fil-perjodu attiv taċ-ċavetta.

Iffirmat elettronicament mid-dikjarant b'firma elettronika skont ir-Regolament (UE) Nru 910/2014 (eIDAS).