

Dearbhú maidir le hEochair Sínithe Nótaire TLSNotary

Seirbhís: pavoltravnik.witness.directcase.ai · Leagan an doiciméid: 1.0 · Dáta: 26 Meán Fómhair 2026

MÓD TÁSTÁLA. Is seirbhís thurgnamhach í seo agus cuirtear ar fáil í gan bharántas. Níl na hadmhálacha ceaptha ach le haghaidh tástála agus meastóireachta agus ní ceart brath orthu mar fhianaise in ábhair dhlíthiúla, airgeadais ná in ábhair chriticiúla eile. Féadfar an eochair thíos a scor tráth ar bith; foilsítear a stair ag /keys.json.

1. AN DEARBHÓIR

Ing. Mgr. Pavol Trávník, a rugadh an 22 Iúil 1991, Zborovská 124/68, Malá Strana, 150 00 Praha 5, Poblacht na Seice, ag gníomhú mar **dhuine nádúrtha** agus mar aon oibreoir na seirbhíse.

2. CAD A DHÉANANN AN TSEIRBHÍS

Is **nótaire** (fíoraitheoir) í an tseirbhís atá tógtha ar phrótacal foinse oscailte TLSNotary. Nuair a lódálann úsáideoir (an **cruthaitheoir**, *prover*) leathanach gréasáin thar HTTPS, glacann an nótaire páirt sa seisiún TLS — trí ríomh ilpháirtí (MPC-TLS) nó mar sheachfhreastalaí — gan é a bheith in ann sonraí an fhreastalaí a bhrionnú. Féadfaidh an cruthaitheoir codanna príobháideacha a cheilt; síníonn an nótaire **admháil** ansin: gealltanais (commitment) i leith chéannacht an fhreastalaí (arna seiceáil i gcoinne a dheimhnithe TLS) agus i leith an ábhair nochta, mar aon le ham an fhíoraithe. Is féidir le duine ar bith an admháil a sheiceáil níos déanaí gan muinín a bheith aige as an gcruthaitheoir.

Cruthaíonn admháil bhailí gur sheirbheáil an freastalaí ainmnithe an t-ábhar nochta thar TLS ag an am luaite, agus go raibh an nótaire seo ina fhinné air. **Ní chruthaíonn sí** go bhfuil an t-ábhar fíor, ná aon ní faoi na codanna ceilte. Oibrítear an nótaire go neamhspleách ar na suíomhanna gréasáin a bhreathnaíonn sé.

3. AN EOCHAIR SÍNITHE DEARBHAITHE

Aitheantas eochrach	73a6bdba645a59e4 (an chéad 8 mbeart de SHA-256 na heochrach poiblí)
Algartam	ECDSA, cuar secp256k1, SHA-256 (secp256k1-ecdsa-sha256)
Eochair phoiblí (SEC1, hex)	029ba59091fb1d63de1b7db1e92bc2bd0ffadc82a8d6522c102cd3db5635b9b744
SHA-256 na heochrach poiblí	73a6bdba645a59e4ce5641cfa5f8e8e7bf0aad33e90004cc803ecf3ff47f181f
Gníomhach ó	2026-09-25T21:52:43Z

Dearbhaím gur ghin an tseirbhís an eochair seo faoi mo rialú aonair, gurb í an tseirbhís a thuiriscítear thuas a eisiúnn admhálacha a shínítear léi, agus go bhfoilseoidh mé scor na heochrach seo ag /keys.json.

4. CONAS ADMHÁIL A FHÍORÚ

- Seiceáil go bhfuil síniú bailí eIDAS ón dearbhóir ar an PDF seo (m.sh. leis an mbailíochtóir EU DSS).
- Glac an admháil {alg, key_id, payload, signature} agus deimhnigh go bhfreagraíonn key_id agus an eochair phoiblí do roinn 3.
- Fíoraigh an síniú ECDSA (64 beart rlls, hex) thar SHA-256 de bheartanna beachta UTF-8 payload, nó seol an admháil chuig POST <https://pavoltravnik.witness.directcase.ai/verify>.
- Seiceáil go bhfuil verified_at sa lasta laistigh de thréimhse ghníomhach na heochrach.

Arna shíniú go leictreonach ag an dearbhóir le síniú leictreonach faoi Rialachán (AE) Uimh. 910/2014 (eIDAS).