# An 24 focal: cad is féiniúlacht chripteagrafach ann

Ní pasfhocal é féiniúlacht chripteagrafach: ní stórálann aon fhreastalaí é agus ní féidir é a fháil ar ais. Míniú oideachasúil ar mheicníocht BIP39, cén fáth go díreach fiche a ceathair focal, agus an meáchan iarbhír a thiteann ar an té a bhfuil siad aige.

**Chun go dtuigfimid a chéile:** Má dhéanann tú dearmad ar do phasfhocal Gmail, athshocraíonn Google duit é. Má chailleann tú an 24 focal atá mar chuid de fhéiniúlacht chripteagrafach, níl aon duine ann le hiad a iarraidh orthu. Ní hé go bhfuil an nós imeachta docht — is é nach bhfuil aon duine ar an taobh eile. Sin an difríocht ar fad.

## An difríocht idir pasfhocal agus féiniúlacht

Ní hé pasfhocal, i múnla clasaiceach an idirlín, féiniúlacht an úsáideora. Is cruthúnas é. Tá féiniúlacht ag an úsáideoir —ainm, ríomhphost, uimhir chustaiméara— agus, chun a chruthú do fhreastalaí gur eisean an té a deir sé, cuireann sé pasfhocal i láthair a chuireann an freastalaí i gcomparáid le lorg a bhí stóráilte aige. Má mheaitseálann na loirg, deonaíonn an freastalaí an seisiún. Má chailltear an pasfhocal, fanann an t-úsáideoir mar an t-úsáideoir céanna; is é an rud a chailleann sé ná an cruthúnas, agus tá nós imeachta téarnaimh ann — ríomhphost chuig an seoladh cláraithe, ceist slándála— chun é a fháil ar ais.

Oibríonn féiniúlacht chripteagrafach ar bhealach eile. Ní dintiúir é a chuireann duine éigin i gcomparáid le lorg stóráilte; *is* rún matamaiticiúil iomlán ann féin é. Is cuma cá bhfuil sé ina chónaí —ar pháipéar, i ngléas, fiú ar fhreastalaí strainséara—: tá an fhéiniúlacht ann mar gheall ar a matamaitic, ní mar gheall ar an té a bhailíochtaíonn é. Anseo feictear maoin cosúil leis an gceann a chonaic muid i «Cad is SHA-256 ann i ndáiríre»: ní cruthaítear seilbh tríd an rún a thaispeáint, ach trína úsáid chun síniú. Is féidir le duine ar bith an síniú a tháirgtear ar an mbealach seo a sheiceáil le luach poiblí a dhíorthaítear go matamaiticiúil ón rún féin, gan gá an rún féin a bheith ar eolas acu, agus gan tríú páirtí a bheith ag idirghabháil sa seiceáil. An té ag a bhfuil an rún, is é an fhéiniúlacht é; an té a chailleann é, scoirfidh sé de bheith mar sin. Tá an breithiúnas cinnte: **níl aon duine ann le hiarraidh orthu an fhéiniúlacht a thabhairt ar ais duit. Níl an duine sin ann, mar ní raibh sé acu sa chéad áit.**

## Cad a sheasann do fiche a ceathair focal

Léirítear féiniúlacht chripteagrafach de ghnáth le rún matamaiticiúil de thríocha a dó beart —dhá chéad caoga a sé giotán. Uimhir atá deacair a choinneáil i gcuimhne agus níos deacra fós a thrascríobh gan earráid. Réitigh an tionscal cripteagrafach an fhadhb seo in 2013 le caighdeán beag galánta ar a dtugtar BIP39: bealach chun na dhá chéad caoga a sé giotán sin a léiriú mar sheicheamh de fiche a ceathair focal tógtha ó liosta oifigiúil de dhá mhí daichead a hocht focal. Luíonn an uimhríocht taobh thiar de go galánta; an té ar mian leis é a fheiceáil go mion, faigheann sé é sa chorrlach.

Tosaíonn an comhaireamh ón deireadh. Ba mhaith linn an dá chéad caoga a sé giotán den rún a léiriú trí ocht ngiotán de shuim seiceála (checksum) a chur leis: dhá chéad seasca a ceathair giotán san iomlán. Má roinnimid iad i bhfiche a ceathair focal —uimhir inláimhsithe le nótáil agus le deachtú gan chailliúint— caithfidh gach focal go díreach aon ghlúin déag giotán faisnéise a sholáthar. Agus is é aon ghlúin déag giotán ná dhá ardaithe go

dtí an t-aonú glúin déag de fhéidearthachtaí, is é sin, dhá mhí daichead a hocht. Sin an fáth go bhfuil an méid sin go díreach ag an stór focal oifigiúil BIP39: tá an liosta ann de réir na faidhbe, ní an bealach eile.

Níl an comhaireamh maisiúil. Má thrascríobhann duine éigin fiche a trí focal i gceart agus má dhéanann siad botún sa cheathrú focal is fiche, braithfidh an tsuim seiceála é: déarfaidh an bogearra leis "níl an seicheamh seo bailí". Má thrascríobhann duine éigin an fiche a ceathair i gceart, díorthóidh an bogearra an fhéiniúlacht chéanna gan débhrí. Tá rogha an liosta focal dándach freisin: tá focail an stór focal BIP39 gearr, difriúil óna chéile, gan diacritics, roghnaithe chun mearbhall foghraíochta agus litrithe a íoslaghdú. Is stór focal é atá deartha le bheith meabhraithe, scríofa agus deachtaithe ag daoine gan chailliúint.

# Ón bhfrása go dtí an eochair

Ní hé an ceithre fhocal is fiche an eochair chripteagrafach a shíníonn teachtaireachtaí. Is ionadaíocht in-aisghafa iad ar an eantrópacht bhunaidh a ndéantar síol (seed) ceithre bheart is seasca de trí phróiseas cinntitheach ar a dtugtar PBKDF2. Is ón síol sin a dhíorthaítear, ar bhealach cinntitheach chomh maith, na heochracha cripteagrafacha sonracha a úsáideann an t-úsáideoir: eochair phríobháideach le síniú agus eochair phoiblí chomhfhreagrach a fhoilsítear chun na sínithe a fhíorú. An mheicníocht chéanna i gcórais éagsúla: úsáideann cripteagearrthaí an cuar secp256k1; úsáideann prótacal Signal agus go leor córas nua-aimseartha Ed25519 ar an gcuar Curve25519. I gcás cuar sonrach cosúil le Ed25519, tógann na caighdeáin BIP32 agus SLIP-0010 an síol ceithre bheart is seasca sin agus díorthaíonn siad, ar bhealach cinntitheach, an dá bheart is tríocha arb iad an eochair sínithe éifeachtach iad — an dá bheart is tríocha céanna lena dtosaíonn an sampla cóid sa chéad alt eile.

Is é seo an bealach caighdeánach ina gcuireann an tionscal ar fad an mheicníocht i láthair an úsáideora —sparáin chripte airgeadra, bainisteoirí aitheantais díláraithe, Signal ina chuid aitheantais sheasmhaigh, Solo2 ina measc —: ní fheiceann an t-úsáideoir an síol ná na heochracha díorthaithe go praiticiúil riamh. Feiceann sé an ceithre fhocal is fiche agus é ag cruthú a aitheantais agus, de rogha air féin, scríobhann sé síos ar pháipéar iad. Taistealaíonn na focail ansin idir a ghléasanna nuair is mian leis an t-aitheantas a aistriú: cuireann sé isteach san fheidhmchlár nua iad, díorthaíonn an feidhmchlár an síol céanna, na heochracha céanna, an t-aitheantas céanna. Is meicníocht iompartha, cripteagrafach daingean é, agus is féidir é a mheabhrú laistigh de theorainneacha an réasúin.

# Conas síniú leis an eochair (stroc beag Zig)

I Zig, nuair atá an síol dá bheart is tríocha agat atá díorthaithe ón gceithre fhocal is fiche, is féidir teachtaireacht a shíniú le Ed25519 i gcúpla líne:

```
const std = @import("std");
const Ed25519 = std.crypto.sign.Ed25519;

// 'semilla' son los 32 bytes derivados de las 24 palabras.
const par = Ed25519.KeyPair.create(semilla);

// Firmar un mensaje con la clave privada:
const mensaje = "Este mensaje lo escribí yo.";
const firma = try par.sign(mensaje, null);

// Cualquiera con la clave pública del par puede verificar:
try Ed25519.Signature.verify(firma, mensaje, par.public_key);
```

Gineann an oibríocht sínithe ceithre bheart is seasca —ar a dtugtar síniú— nár fhéadadh a ghiniúint ach ón eochair phríobháideach chomhfhreagrach. Is poiblí an fíorú: is féidir le duine ar bith a bhfuil an eochair phoiblí aige a sheiceáil go gcomhfhreagraíonn an síniú don teachtaireacht. Gan an eochair phríobháideach, ní féidir le duine ar bith síniú bailí a tháirgeadh don teachtaireacht sin; leis an eochair phoiblí, is féidir le gach duine a

bhrath an bhfuil síniú bailí. Is é an neamhshiméadracht seo a ligeann don sínitheoir údaracht a léiriú gan an rún a roinnt.

Is é an sampla roimhe seo an leagan íosta den lámhleabhar. I gcód fíor Solo2 téann an slabhra trí dhá chomhad, ceann amháin i JavaScript a chónaíonn i mbrabhsálaí an úsáideora agus a atógann an t-eantrópacht ó na ceithre fhocal fhichead, ceann eile i Zig laistigh den leabharlann *zcatcrypto* a thógann an t-eantrópacht sin agus a dhíorthaíonn na heochracha cripteagrafacha sonracha. Ag tosú ar thaobh an bhrabhsálaí:

```
// solo2/web-app/js/lib/bip39.js
async function mnemonicToEntropy(mnemonic, lang) {
    const validation = await validateMnemonic(mnemonic, lang);
    if (!validation.valid) {
        return { entropy: null, valid: false, error: validation.error };
    }
    const wordlist = WORDLISTS[lang || 'en'];
    const words = mnemonic.trim().split(/\s+/);

    // Cada palabra aporta 11 bits (su índice en la lista de 2048).
    let bits = '';
    for (let i = 0; i < words.length; i++) {
        bits += wordlist.indexOf(words[i]).toString(2).padStart(11, '0');
    }

    // 24 palabras = 264 bits. Los primeros 256 son la entropía.
    const entropyBytes = new Uint8Array(32);
    for (let j = 0; j < 32; j++) {
        entropyBytes[j] = parseInt(bits.slice(j * 8, (j + 1) * 8), 2);
    }
    return { entropy: entropyBytes, valid: true };
}
```

Taistealaíonn na tríocha a dó beart eantrópachta sin, mar aon le tríocha a dó eile a dhíorthaítear sa chéim chéanna, go dtí modúl WebAssembly Zig a ghineann na heochracha Ed25519 féin. Luíonn an fheidhm iomlán, lena glanadh cuimhne deiridh, ar scáileán amháin:

```
// zcatcrypto/wasm/bindings/identity.zig
const Ed25519 = std.crypto.sign.Ed25519;
const X25519  = std.crypto.dh.X25519;

export fn identity_generate() ?*IdentityHandle {
    var seed: [64]u8 = undefined;
    if (!common.getRandomBytes(&seed)) return null;

    const handle = common.wasm_allocator.create(IdentityHandle) catch return null;

    // Bytes 0..31: semilla determinista del par Ed25519 (firma).
    const sign_kp = Ed25519.KeyPair.generateDeterministic(seed[0..32].*) catch {
        common.wasm_allocator.destroy(handle);
        return null;
    };
    handle.sign_secret = sign_kp.secret_key.toBytes();
    handle.sign_public = sign_kp.public_key.toBytes();

    // Bytes 32..63: secreto X25519 (para acordar claves de cifrado con el otro).
    handle.exchange_secret = seed[32..64].*;
```

```
    handle.exchange_public = X25519.recoverPublicKey(handle.exchange_secret) catch {
        common.wasm_allocator.destroy(handle);
        return null;
    };

    @memset(&seed, 0);  // Borra la semilla de la memoria.
    return handle;
}
```

Is fiú dhá mhionsonra a thabhairt faoi deara. An chéad cheann: gineann síol céanna an péire eochracha céanna i gcónaí — is é sin go díreach a ligeann an t-aitheantas a aisghabháil trí na ceithre fhocal fhichead a chur isteach i ngléas nua. An dara ceann: scriostar an síol go sainráite ón gcuimhne sa líne dheireanach. Tar éis an phointe sin, ní fhéadfadh fiú an fheidhm féin na heochracha a atógáil; bheadh focail an úsáideora mar an t-aon bhunús amháin.

**Dóibh siúd ar mian leo é a sheiceáil le huimhreacha beaga.** Is féidir an scéim sínithe a chur i gcrích go hiomlán le huimhreacha atá beag go leor chun na ríomhaireachtaí a dhéanamh de láimh. Is féidir leo siúd ar fearr leo gan dul isteach san uimhríocht an bloc seo a scipeáil gan snáth an ailt a chailleadh; gheobhaidh siad siúd ar mian leo an mheicníocht a fheiceáil ag obair céim ar chéim anseo é. **Na rialacha poiblí**, ar féidir le duine ar bith iad a léamh: príomhuimhir $p = 23$ (i bhfíor-Ed25519 tá sé thart ar seachtó a seacht ndigit ar fad; úsáidimid fiche a trí ionas go n-oireann na ríomhaireachtaí ar leathanach amháin), bunáit $g = 2$ a bhfuil a ord sa ghrúpa seo $q = 11$, agus an gnás go ndéantar an uimhríocht go léir le *g módulo p* agus go laghdaítear gach easpónant *módulo q*. **An rogha phríobháideach**, ceann amháin agus nach roinntear go deo: an rún $x = 6$. Sin é an t-aitheantas.

**Céim 1 — Cuid phoiblí an aitheantais.** Ríomhtar é uair amháin agus foilsítear é go hoscailte.

$$y = g^x \bmod p$$

$$y = 2^6 \bmod 23 = 64 \bmod 23 = 18$$

Is é **18** cuid phoiblí an aitheantais. Is féidir le duine ar bith é a thógáil agus é a úsáid chun sínithe a rinneadh leis an aitheantas seo a fhíorú. Ní féidir le duine ar bith, ag breathnú ar an 18 amháin, an rún 6 a aisghabháil: sin fadhb an logartaim scoite a bhfillfimid air ag an deireadh.

**Céim 2 — Teachtaireacht a shíniú.** Is mian le sealbhóir an aitheantais an teachtaireacht $m = 7$ a shíniú. Tosaíonn sé trí luach randamach nua $k = 4$ a roghnú, a úsáidfear uair amháin amháin agus nach roinnfear go deo (i bhfíor-Ed25519, díorthaítear $k$ go cinntitheach ón teachtaireacht agus ón rún chun an baol a bhaineann le hathúsáid a sheachaint, ach is é seo go díreach an ról a imríonn sé). Ansin ríomhann sé trí uimhir:

$$r = g^k \bmod p = 2^4 \bmod 23 = 16$$

$$e = H(r, m) \bmod q = (16 + 7) \bmod 11 = 1$$

$$s = (k + x \cdot e) \bmod q = (4 + 6 \cdot 1) \bmod 11 = 10$$

Is é an péire **(r, s) = (16, 10)** an síniú. Taistealaíonn sé go hoscailte in éineacht leis an teachtaireacht. Is féidir le duine ar bith é a léamh. Nóta didactic: i bhfíor-Ed25519 is é an fheidhm *H* ná SHA-512, atá láidir ó thaobh cripteagrafaíochta de; anseo úsáidimid an simpliú *e = (r + m) mod q* ionas gur féidir leis an léitheoir na céimeanna a leanúint gan gá le hais a ríomh. Tá struchtúr an algartaim mar an gcéanna.

**Céim 3 — An síniú a fhíorú.** Tá an chuid phoiblí $y = 18$ ag an bhfíoraitheoir, an teachtaireacht $m = 7$, agus an síniú $(r, s) = (16, 10)$. Atógann sé $e$ ar an mbealach céanna — $e = (16 + 7) \bmod 11 = 1$ — agus seiceálann sé an gcomhlíontar an chothromóid seo:

$$g^s \bmod p \overset{?}{=} r \cdot y^e \bmod p$$

Ríomhann sé an dá thaobh ar leithligh:

Izquierda: $2^{10} \bmod 23 = 1024 \bmod 23 = 12$

Derecha: $16 \cdot 18^{1} \bmod 23 = 288 \bmod 23 = 12$

Tugann an dá thaobh **12**. Tá an síniú bailí. Is féidir le duine ar bith a bhfuil an chuid phoiblí 18 acu an tátal seo a bhaint amach gan a fhios a bheith acu riamh gurbh é an rún ná 6.

**Agus tríú páirtí ag iarraidh brionnú a dhéanamh?** Tá gach rud poiblí feicthe ag Eva ag dul tríd an gcainéal: $p = 23$, $g = 2$, $q = 11$, $y = 18$, $m = 7$, $r = 16$, $s = 10$. Chun teachtaireacht *dhifriúil* a shíniú thar ceann an aitheantais seo, bheadh uirthi $x$ a bheith ar eolas aici. Is é an t-aon bhealach atá aici ná í féin a cheistiú: «cén easpónant $x$ a gcomhlíontar $2^x \bmod 23 = 18$ dó?». Le $p = 23$ is féidir léi triail a bhaint as 0, 1, 2, 3, … agus é a fháil i soicindí. Ach nuair a chuirtear príomhuimhir de thoisí fíor Ed25519 in ionad 23, sáraíonn spás na n-easpónant féideartha líon na n-adamh sa chruinne inbhreathnaithe. **Níl aon algartam ar eolas ag an gcine daonna inniu atá in ann an spás sin a thrasnú i níos lú ná na billiúin bliain.** Is í an fhadhb chéanna logartaim scoite í atá mar bhonn faoi Diffie-Hellman san alt roimhe seo, curtha i bhfeidhm anseo ar an scéim sínithe.

Is é an rud atá díreach tar éis dul tríd ná Schnorr *go díreach*, an scéim sínithe ar leagan é Ed25519 de atá oiriúnaithe do chuar éilipseach. I bhfíor-Ed25519, déantar gach oibríocht ar phointí cuair shonraigh (Curve25519) in ionad slánuimhreacha modulo príomhuimhir, agus is é an fheidhm $H$ ná SHA-512 in ionad na suime bréagán a d'úsáideamar thuas. Is coigeartuithe cur chun feidhme iad an dá ionadú — friotaíocht cripteagrafach a fháil in aghaidh fórsa brúidiúil, airíonna slándála breise a fháil do $k$ —. Tá an struchtúr algartamach, na trí oibríocht, an fáth leis an neamhshiméadracht, mar an gcéanna.

Is cuí sos gairid anseo, mar is féidir an slabhra iomlán a mheascadh ar amharc tapa le horgánach eile den triúr: an hais. Ní hea. Is feidhm uathúil é hais a chomhbhrúíonn — téann go leor beart isteach, tagann lorg gearr amach, ansin a chríochnaíonn an bealach. Is péire matamaiticiúil comhlántach é aitheantas cripteagrafach: fanann an rún agus síníonn sé; foilsítear a mhacasamhail phoiblí agus fíoraítear é. Nuair a chliseann an hais faisnéis i dtreo amháin, bunaíonn an t-aitheantas neamhshiméadracht idir dhá leath. Deimhníonn an hais cad a dúradh; deimhníonn an t-aitheantas cé a dúirt é.

# An rud nach bhfuil sa bhfrása

Is fiú trí mhíthuiscint choitianta a ghlanadh suas. Ní pasfhocal é an frása sa chiall cheart: ní dhéantar é a chur i gcomparáid le lorg méire atá stóráilte ar fhast freastalaí; cuirtear isteach i ngléas an úsáideora é chun an t-aitheantas a atógáil go matamaiticiúil. Ní aisghabhtar an frása: má chailltear é, níl aon duine ann le hiontaoibh a chur as chun é a fháil; má dhéantar macasamhail de, déantar macasamhail den aitheantas freisin. Ní dintiúr in-scartha ón aitheantas é an frása: *is é* an frása an t-aitheantas. An té a bhfuil sé aige, is féidir leis gníomhú mar an t-aitheantas sin, gan cead breise, gan phróiseas údaraithe, gan aisghabháil fhéideartha.

Is é an tríú maoin seo a athraíonn meáchan an ábhair. Is crá riaracháin é pasfhocal caillte. Is é an t-aitheantas é aitheantas cripteagrafach caillte. Ní riosca goid cuntais é páipéar leis an bhfrása a aimsíonn tríú páirtithe: is é sin seachadadh an aitheantais iomláin. Tá gealltanas an chórais —nach féidir le duine ar bith d’aitheantas a chúlghairm ná tú a bhlocáil go treallach— ag gabháil go do-scartha leis an bhfreagracht —gur tusa an t-aon choimeádaí ar rud nach féidir le duine ar bith a chur ar ais duit.

# An gealltanas agus an meáchan

Is minic a thugtar *féiniúlacht fhéin-sobhrainneach* ar an tsamhail aitheantais chripteagrafach —self-sovereign sa litríocht Bhéarla—. Tá an rogha focal d’aon ghnó agus déanann sé cur síos cruinn ar an riocht. Tá an t-úsáideoir ina fhlaitheas ar a aitheantas i gciall atá beagnach meánaoiseach: ní thugann aon rí, aon eisitheoir, aon údarás lárnach é; ná ní féidir le haon cheann acu é a tharraingt siar ach an oiread. Ach chomh maith leis sin, cosúil leis

an monarc meánaoiseach, iompraíonn an t-úsáideoir iarmhairt iomlán a bhotúin: níl aon t-ionadaí ann chun cinntí a dhéanamh ina áit má chailleann sé an séala.

Níl freagra uilíoch amháin i gceart ar an rogha idir aitheantas arna bhainistiú ag tríú páirtí agus aitheantas féin-sobhrainneach. I gcás cuntas fóraim nach bhfuil tábhacht leis, is dócha go bhfuil an t-aitheantas bainistithe i gcomhréir leis an riosca. I gcás aitheantas gairmiúil a shíníonn cáipéisí atá ceangailteach ó thaobh an dlí de, i gcás aitheantas eacnamaíoch a choimeádann coigilteas pearsanta, i gcás aitheantas cumarsáide gairmiúla le cliaint a chuir faisnéis íogair de chúram orthu, athraíonn an cheist. Ansin stopann an cheist de bheith «an bhfuil sé áisiúil?» agus éiríonn sí «cé, seachas mé féin, a bhfuil an chumhacht aige gníomhú mar mé, agus faoi cad iad na cúinsí?».

## Cá bhfeictear an mheicníocht seo i gcórais fíor

Rugadh BIP39 i saol Bitcoin in 2013 agus leath sé go tapa chuig an éiceachóras cryptocurrency iomlán: glacann aon sparán tromchúiseach inniu le frása BIP39 de dhá fhocal déag nó fiche a ceathair mar thacaíocht d’aitheantas eacnamaíoch a shealbhóra. Lasmuigh de cryptocurrencies, feictear an coincheap bunúsach céanna — péire cripteagrafach a chruthaíonn údar gan idirghabhálaí — i gcórais eile le comhréir dhifriúil. Is cás clasaiceach iad na heochracha SSH a úsáideann riarthóir córais chun rochtain a fháil ar a fhreastalaithe: eochair phríobháideach a choinníonn an riarthóir ar a mheaisín agus eochair phoiblí a dhéantar a chóipeáil chuig gach freastalaí; ní dhéanann aon eintiteas atá inchomparáide le seirbhís lárnaithe idirghabháil. Úsáideann prótacal Signal Ed25519 le hábhar eochrach leanúnach ar an bhfeiste; tá eIDAS na hEorpa, ina chuid de shíniú cáilithe, bunaithe ar an bprionsabal cripteagrafach céanna, leis an difríocht go gcoimeádann soláthraí seirbhíse iontaobhais cáilithe an eochair in ionad an úsáideora.

Úsáideann Solo2, ardán foilsitheoireachta an fhoilseacháin seo, frása BIP39 de fiche a ceathair focal mar aitheantas do gach úsáideoir. Feiceann an t-úsáideoir, nuair a chruthaíonn sé a chuntas, na focail uair amháin. Ní stóráiltear iad ar aon fhreastalaí Solo2 ná ar aon duine eile: má dhéanann an t-úsáideoir iad a nótáil agus a chosaint, coimeádann sé a aitheantas go deo. Má chailleann sé iad, chailleann sé iad. Is é an toradh comherent ar ailtireacht gan oibreoir sa lár: dá bhféadfadh Solo2 an t-aitheantas a thabhairt ar ais don úsáideoir a chaill é, d’fhéadfadh sé é a thabhairt freisin do dhuine ar bith a chuireann brú ar Solo2 é a thabhairt.

## Don léitheoir gairmiúil

Ceithre bhreithniú dóibh siúd atá ag déanamh meastóireachta ar ghlacadh le haitheantas cripteagrafach féinfhlaitheasach (autosoberana) i gcomhthéacs gairmiúil:

1. Is é an frása an t-aitheantas. Tugann cosaint fhisiceach — páipéar, roinnt cóipeanna in áiteanna difriúla, miotal greanta sa deireadh le haghaidh úsáide fadtéarmaí — níos mó ráthaíochtaí ná cosaint dhigiteach, a chuireann dromchla ionsaithe leis gan an riosca caillteanais a laghdú.
2. Níl aon téarnamh ann. Tá sé i bhfad níos críonna an próiseas a dhearadh ag glacadh leis go gcaillfear an phríomhchóip lá éigin ná é a fháil amach an lá a chaillfear í. Réitíonn an dara cóip atá scartha go geografach beagnach gach cás.
3. Ní hionann é agus deimhniú cáilithe eIDAS. Maidir le síniú cáilithe san Aontas — gníomhais nótaireachta, nósanna imeachta áirithe leis an Riarachán — éilíonn an reachtaíocht soláthraí cáilithe a choimeádann an eochair. Freastalaíonn aitheantas cripteagrafach féinfhlaitheasach ar chumarsáid ghairmiúil agus ar shíniú doiciméadach le luach probháideach, ach ní thagann sé in ionad an deimhnithe cháilithe go huathoibríoch i gcásanna ina n-éilíonn an riail é.
4. Má tá an t-aitheantas le haistriú — oidhreacht, comharbas gairmiúil, deireadh le gníomhaíocht — is fiú an nós imeachta a ullmhú roimh ré, ní tar éis. Is socruithe clasaiceacha iad nósanna imeachta foirmiúla le clúdaigh séalaithe le céir (lacre), treoracha d’fhorghníomhaí uachta, taisce in oifig nótaire, atá ag luí go hiomlán le cineál cripteagrafach an tsócmhainne.

*Dúnann an t-alt seo an triúr coincheapúil a d’oscail an timthriall — hash, criptiú, aitheantas —. Tógann na trí smaoineamh ar a chéile: tugann an hash an rian do-athraithe, tugann an criptiú an rúnmhaireacht gan tríú páirtí iontaofa, tugann an t-aitheantas an t-údar gan tríú páirtí deonaithe. Tá maoin ag an triúr acu nach bhfuil idé-eolaíoch ach an oiread: aistríonn siad, ón té a bhainistíonn seirbhís chuig an té a úsáideann í, cumais theicniúla a bhíodh de ghnáth ag an oibreoir. Aistríonn siad freisin freagrachtaí leo. Chun labhairt go hionraic faoi aon cheann de na trí cinn, caithfear labhairt freisin faoin dá cheann eile.*

## Foinsí agus léitheoireacht bhreise

- Palatinus, M.; Rusnak, P.; Voisine, A.; Bowe, S. — *BIP-0039: Mnemonic code for generating deterministic keys*, moladh feabhsúcháin Bitcoin de 2013. Caighdeán de facto do fhrásaí aisghabhála sa tionscal cripte.
- RFC 8032 — Edwards-Curve Digital Signature Algorithm (EdDSA), lena n-áirítear Ed25519. IETF, Eanáir 2017. Sonraíocht normatach an scéim sínithe a úsáidtear i gcuid mhaith den tionscal comhaimseartha.
- RFC 2898 — PKCS #5: Password-Based Cryptography Specification, leagan 2.0. IETF, Meán Fómhair 2000. Sainmhíníonn sé an t-algartam PBKDF2 a úsáidtear i ndíorthú BIP39 ó fhrása go síol (seed).
- Rialachán (AE) 910/2014 (eIDAS) agus a éabhlóid trí Rialachán (AE) 2024/1183 (eIDAS 2) — creat Eorpach d’aitheantas leictreonach agus síniú cáilithe. Réimeas atá difriúil ón gceann féinfhlaitheasach, ach atá tacaithe go coincheapúil ag na bunmhéideanna cripteagrafacha céanna.
- Allen, C. — *The Path to Self-Sovereign Identity* (2016). Téacs canónta ar phrionsabail agus tiomantais an mhúnla féinfhlaitheasaigh, níos luaithe ach ábhartha chun tuiscint a fháil ar theaghlach na réiteach comhaimseartha.

← Roimhe seoAn tsamhail ghnó mar chomhartha muiníneAr aghaidh →Féin-óstáil mar chleachtas gairmiúil

## Léitheoireacht le déanaí


- Machnamh · 29 Meitheamh 2026 Níl tú gan ainm
- Machnamh · 27 Bealtaine 2026 An rud nach féidir le síniú a dheisiú
- Anailís · 26 Bealtaine 2026 Príobháideacht iarbhír vs príobháideacht dhealraitheach: na ceisteanna ba chóir duit a chur ort féin


Beir an t-alt seo leat áit ar bith a dteastaíonn sé uait.

↓ Markdown ↓ Téacs simplí ↓ PDF

Íoslódálfar an comhad chuig do ghléas. Ón áit sin is féidir leat é a shábháil, é a iompórtáil go Solo2 nó é a roinnt cibé áit is mian leat. Ní chinneann Cuadernos an ceann scríbe duitse.

Séala céir · SHA-256 f317190ee3f3309e7d34df10309b02d5fe150acb4b465c3234e1f1b5dc16db21



Cuadernos Lacre · Foilseachán de chuid Menzuri Gestión S.L. ·
scríofa ag R.Eugenio · curtha in eagar ag foireann Solo2.

Ní úsáideann an suíomh seo fianáin. Tá gach a luchtaíonn do bhrabhsálaí scríofa nó maoirsithe againn agus óstáilte ar ár bhfreastalaithe Eorpacha: an córas tomhais anaithnid (Umami, féin-óstáilte) agus an t-íosmhéid JavaScript is gá don roghnóir teanga agus do do rogha téama solais nó dorcha, a shábháiltear ar do ghléas féin. Gan acmhainní ó chuideachtaí seachtracha, gan rianairí, gan próifíliú, gan comhroinnt sonraí. Más mian leat sinn a leanúint: RSS.