Kunċett · 23 ta’ Mejju 2026

← Preċedenti·Li jmiss →

L-24 kelma: x'inhi identità kriptografika

Identità kriptografika mhijiex password: l-ebda server ma jżommha u ma tistax tiġi rkuprata. Spjegazzjoni didattika tal-mekkaniżmu BIP39, għaliex eżattament erbgħa u għoxrin kelma, u liema piż reali jaqa' fuq min jipposjedihom.

Biex niftehmu: Jekk tinsa l-password tal-Gmail tiegħek, Google tirrisetjahielek. Jekk titlef l-24 kelma li jiffurmaw identità kriptografika, m'hemm lil ħadd lil min titlobhom. Mhux għax il-proċedura hija stretta — imma għax m'hemm ħadd fin-naħa l-oħra. Dik id-differenza hija kollox.

Id-differenza bejn password u identità

Password, fil-mudell klassiku tal-internet, mhijiex l-identità tal-utent. Hija prova. L-utent għandu identità — isem, email, numru tal-klijent — u, biex jipprova lil server li huwa min jgħid li huwa, jippreżenta password li s-server iqabbel ma' marka li kellu maħżuna. Jekk il-marki jaqblu, is-server jippermetti s-sessjoni. Jekk il-password tintilef, l-utent jibqa' l-istess utent; dak li jitlef huwa l-prova, u teżisti proċedura ta' rkupru — email fl-indirizz irreġistrat, mistoqsija ta' sigurtà — biex tiġi rrestawrata.

Identità kriptografika taħdem b'mod differenti. Mhijiex kredenzjali li xi ħadd iqabbel ma' marka maħżuna; *hija* sigriet matematiku sħiħ fih innifsu. Ma jimpurtax fejn qiegħed — fuq karta, f'apparat, anke f'server ta' ħaddieħor —: l-identità teżisti minħabba l-matematika tagħha, mhux minħabba min jivvalidaha. Hawnhekk tidher proprjetà simili għal dik li rajna f'«X'inhu verament SHA-256»: il-pussess ma jiġix ippruvat billi turi s-sigriet, imma billi tużah biex tiffirma. Il-firma hekk prodotta kulħadd jista' jivverifikaha b'valur pubbliku li huwa derivat matematikament mis-sigriet innifsu, mingħajr il-ħtieġa li tkun taf is-sigriet, u mingħajr ma jintervjeni terz fil-verifika. Min għandu s-sigriet, huwa l-identità; min jitilfu, ma jibqax. Is-sentenza hija kategorika: **m'hemm ħadd lil min titlob biex jagħtik l-identità lura. Dak il-xi ħadd ma jeżistix, għax ma kellux f'idu fl-ewwel lok.**

Dak li jirrappreżentaw erbgħa u għoxrin kelma

L-identità kriptografika hija s-soltu rrappreżentata minn sigriet matematiku ta' tnejn u tletin byte — mitejn u sitta u ħamsin bit. Numru li diffiċli tiftakru u aktar u aktar diffiċli tiktbu mingħajr żbalji. L-industrija kriptografika solviet din il-problema fl-2013 bi standard żgħir u eleganti msejjaħ BIP39: mod kif tirrappreżenta dawk il-mitejn u sitta u ħamsin bit bħala sekwenza ta' erbgħa u għoxrin kelma meħuda minn lista uffiċjali ta' elfejn u tmienja u erbgħin. L-aritmetika ta' wara taqbel b'eleganza; min irid jaraha fid-dettall isibha fil-ġenb.

Il-kont jibda mill-aħħar. Irridu nirrappreżentaw il-mitejn u sitta u ħamsin bit tas-sigriet billi nżidu tmien bits ta' checksum: mitejn u erbgħa u sittin bit b'kollox. Jekk inqassmuhom f'erbgħa u għoxrin kelma — numru maniġġabbli biex tinnotahom u tiddettahom mingħajr telf — kull kelma trid tipprovdi eżattament ħdax-il bit ta' informazzjoni. U ħdax-il bit huma tnejn imtellgħin għall-ħdax-il qawwa ta' possibbiltajiet, jiġifieri, elfejn u tmienja u erbgħin. Għalhekk il-vokabularju uffiċjali BIP39 għandu preċiżament dak id-daqs: il-lista teżisti skont il-problema, mhux bil-maqlub.

Il-kont mhuwiex dekorattiv. Jekk xi ħadd jikteb tlieta u għoxrin kelma b'mod korrett u jiżbalja fl-erbgħa u għoxrin waħda, iċ-checksum jiskoprih: is-software jgħidlu "din is-sekwenza mhijiex valida". Jekk xi ħadd jikteb l-erbgħa u għoxrin kollha b'mod korrett, is-software jidderiva l-istess identità mingħajr ambigwità. L-għażla tal-lista tal-kliem hija wkoll intenzjonata: il-kliem fil-vokabularju BIP39 huma qosra, distinti minn xulxin, mingħajr dijakritiċi, magħżula biex jimminimizzaw konfużjonijiet foneticiċi u ortografiċi. Huwa vokabularju ddisinjat biex jiġi mfakkar, miktub u ddettat mill-bnedmin mingħajr telf.

Mill-fraži għaċ-ċavetta

L-erbgħa u għoxrin kelma mhumiex iċ-ċavetta kriptografika li tiffirma l-messaġġi. Huma rappreżentazzjoni li tista' tiġi rkuprata tal-entropija oriġinali li, permezz ta' proċess deterministiku msejjaħ PBKDF2, tinbidel f'żerriegħa (seed) ta' erbgħa u sittin byte. Minn dik iż-żerriegħa jidderivaw, ukoll b'mod deterministiku, iċ-ċwievet kriptografiċi konkreti li l-utent juża: ċavetta privata biex jiffirma u ċavetta pubblika korrispondenti li tiġi ppubblikata biex tivverifika l-firem. L-istess mekkaniżmu f'sistemi differenti: il-kriptovaluti jużaw il-kurva secp256k1; il-protokoll Signal u bosta sistemi moderni jużaw Ed25519 fuq il-kurva Curve25519. Għal kurva konkreta bħal Ed25519, l-istandards BIP32 u SLIP-0010 jieħdu dik iż-żerriegħa ta' erbgħa u sittin byte u jidderivaw, b'mod deterministiku, it-tnejn u tletin byte li jikkostitwixxu ċ-ċavetta tal-iffirmar effettiva — l-istess tnejn u tletin byte li bihom jibda l-eżempju tal-kodiċi fit-taqsima li jmiss.

Din hija l-forma standard li biha l-industrija kollha tippreżenta l-mekkaniżmu lill-utent —portafolli tal-kriptovaluti, maniġers tal-identità deċentralizzata, Signal fil-parti tal-identità persistenti tiegħu, Solo2 fosthom—: l-utent, fil-prattika, qatt ma jara ż-żerriegħa jew iċ-ċwievet derivati. Juri l-erbgħa u għoxrin kelma meta joħloq l-identità tiegħu u, b'mod fakultattiv, iniżżilhom fuq karta. Il-kliem imbagħad jivvjaġġa bejn it-tagħmir tiegħu meta jkun irid jemigra l-identità: idaħħalhom fl-applikazzjoni l-ġdida, l-applikazzjoni tidderiva l-istess żerriegħa, l-istess ċwievet, l-istess identità. Huwa mekkaniżmu portabbli, kriptografikament sod u, fil-limiti tar-raġonevoli, faċli biex tiftakru.

Kif tiffirma biċ-ċavetta (pinzellata Zig)

F'Zig, ladarba jkollok iż-żerriegħa tat-tnejn u tletin byte derivata mill-erbgħa u għoxrin kelma, l-iffirmar ta' messaġġ b'Ed25519 jidħol fi ftit linji:

```
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);
```

L-operazzjoni tal-iffirmar tipproduċi erbgħa u sittin byte —imsejħa firma— li setgħu jiġu ġġenerati biss miċ-ċavetta privata korrispondenti. Il-verifika hija pubblika: kull min għandu ċ-ċavetta pubblika jista' jiċċekkja li l-firma tikkorrispondi mal-messaġġ. Mingħajr iċ-ċavetta privata, ħadd ma jista' jipproduċi firma valida għal dak il-messaġġ; biċ-ċavetta pubblika, kulħadd jista' jiskopri jekk firma hijiex valida. Dik l-asimmetrija hija dik li tippermetti lill-firmatarju juri l-awtur tiegħu mingħajr ma jaqsam is-sigriet.

L-eżempju preċedenti huwa l-verżjoni minima tal-manwal. Fil-kodiċi reali ta' Solo2, il-katina tgħaddi minn żewġ fajls, wieħed f'JavaScript li jgħix fil-browser tal-utent u jibni mill-ġdid l-entropija mill-erbgħa u għoxrin kelma, u

ieħor f'Zig fil-librerija *zcatcrypto* li jieħu dik l-entropija u joħroġ il-muftieħ kriptografiċi speċifiċi. Nibdew minnaħa tal-browser:

```
// 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 };
}
```

Dawk it-tnejn u tletin byte ta' entropija, flimkien ma' tnejn u tletin oħra derivati fl-istess pass, jivvjaġġaw lejn il-modulu WebAssembly ta' Zig li jiġġenera l-muftieħ Ed25519 proprji. Il-funzjoni sħiħa, bit-tindif finali tal-memorja tagħha, toqgħod fuq skrin wieħed:

```
// 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;
}
```

Żewġ dettalji ta' min jinnotahom. L-ewwel wieħed: l-istess seed dejjem jipproduċi l-istess par ta' muftieħ — huwa eżattament dan li jippermetti l-irkupru tal-identità billi ddaħħal l-erbgħa u għoxrin kelma f'apparat ġdid. It-tieni wieħed: is-seed titħassar b'mod espliċitu mill-memorja fl-aħħar linja. Wara dak il-punt, lanqas il-funzjoni nnifisha ma tkun tista' tibni mill-ġdid il-muftieħ; il-kliem tal-utent ikun l-uniku sors.

Għal dawk li jridu jivverifikaw b'numri żgħar. L-iskema tal-firma tista' tiġi rintraċċata kollha b'ċifri żgħar biżżejjed biex isiru l-kontijiet bl-idejn. Min jippreferi ma jidħolx fl-aritmetika jista' jaqbeż dan il-blokk mingħajr ma jitlef il-fil tal-artiklu; min irid jara l-mekkaniżmu jaħdem pass pass isibu hawnhekk. **Ir-regoli pubbliċi**, li kulħadd jista' jaqra: prim $p = 23$ (f'Ed25519 reali huwa ta' madwar sebgħa u sebgħin ċifra; nużaw tlieta u għoxrin biex il-kontijiet joqogħdu fuq paġna waħda), bażi $g = 2$ li l-ordni tagħha f'dan il-grupp hija $q = 11$, u l-konvenzjoni li l-aritmetika kollha b' g issir *módulo p* u l-esponenti kollha jitnaqqsu *módulo q*. **L-għażla privata**, waħda biss u qatt ma tinqasam: is-sigriet $x = 6$. Dik hija l-identità.

Pass 1 — Il-parti pubblika tal-identità. Tiġi kkalkulata darba u tiġi ppubblikata fil-miftuħ.

$y = g^x \bmod p$

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

Il-parti pubblika tal-identità hija **18**. Kulħadd jista' jeħodha u jużaha biex jivverifika firem magħmula b'din l-identità. Ħadd, billi josserva biss it-18, ma jista' jirkupra s-sigriet 6: dik hija l-problema tal-logaritmu diskret li se nerġgħu lura għaliha fl-aħħar.

Pass 2 — L-iffirmar ta' messaġġ. Is-sid tal-identità jrid jiffirma l-messaġġ $m = 7$. Jibda billi jagħżel valur każwali ġdid $k = 4$, li se jintuża darba waħda biss u qatt ma jinqasam (f'Ed25519 reali, k jiġi derivat b'mod deterministiku mill-messaġġ u mis-sigriet biex jiġi evitat il-periklu ta' użu mill-ġdid, iżda r-rwol li għandu huwa eżattament dan). Imbagħad jikkalkula tliet numri:

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

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

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

Il-firma hija l-par **(r, s) = (16, 10)**. Tivvjaġġa fil-miftuħ flimkien mal-messaġġ. Kulħadd jista' jaqraha. Nota didattika: f'Ed25519 reali l-funzjoni H hija SHA-512, kriptografikament robusta; hawnhekk nużaw is-simplifikazzjoni $e = (r + m) \bmod q$ biex il-qarrej ikun jista' jsegwi l-passi mingħajr bżonn li jikkalkula hash. L-istruttura tal-algoritmu hija l-istess.

Pass 3 — Il-verifika tal-firma. Il-verifikatur għandu l-parti pubblika $y = 18$, il-messaġġ $m = 7$, u l-firma $(r, s) = (16, 10)$. Jibni mill-ġdid e bl-istess mod — $e = (16 + 7) \bmod 11 = 1$ — u jiċċekkja jekk din l-ugwaljanza hijiex sodisfatta:

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

Ikkalkula ż-żewġ naħat separatament:

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

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

Iż-żewġ naħat jagħtu **12**. Il-firma hija valida. Kulħadd bil-parti pubblika 18 jista' jasal għal din il-konklużjoni mingħajr ma qatt ikun jaf li s-sigriet kien 6.

U parti terza li tipprova tiffalsifika? Eva rat dak kollu li huwa pubbliku jgħaddi mill-kanal: $p = 23$, $g = 2$, $q = 11$, $y = 18$, $m = 7$, $r = 16$, $s = 10$. Biex tiffirma messaġġ *differenti* f'isem din l-identità, hija jkollha bżonn tkun taf x. L-uniku mod tagħha huwa li tistaqsi lilha nnifisha: "għal liema esponent x huwa sodisfatt $2^x \bmod 23 = 18$?". Bi $p = 23$ hija tista' tipprova 0, 1, 2, 3, … u ssibu f'sekondi. Iżda meta tissostitwixxi 23 b'prim tad-dimensjonijiet reali ta' Ed25519, l-ispazju ta' esponenti possibbli jaqbeż in-numru ta' atomi fl-univers osservabbli. **Sal-lum m'hemm l-ebda algoritmu magħruf mill-umanità li jista' jgħaddi minn dak l-ispazju f'inqas minn biljuni ta' snin.** Hija l-istess problema tal-logaritmu diskret li tappoġġja d-Diffie-Hellman mill-artiklu preċedenti, applikata hawnhekk għall-iskema tal-firma.

Dak li għadna kif għaddejna minnu huwa *eżattament* Schnorr, l-iskema tal-firma li tagħha Ed25519 hija varjant adattat għal kurva ellittika. F'Ed25519 reali, l-operazzjonijiet kollha jsiru fuq il-punti ta' kurva speċifika (Curve25519) minflok fuq numri sħaħ modulo prim, u l-funzjoni H hija SHA-512 minflok is-somma tal-logħob li użajna hawn fuq. Iż-żewġ sostituzzjonijiet huma aġġustamenti tal-implimentazzjoni — ksib ta' reżistenza kriptografika għal brute force, ksib ta' proprjetajiet ta' sigurtà addizzjonali għal k —. L-istruttura algoritmika, it-tliet operazzjonijiet, ir-raġuni għall-asimmetrija, huma l-istess.

Hawnhekk jaqbel nieqfu ftit, għax il-katina kollha tista' tiġi konfuża mal-ewwel daqqa t'għajn ma' primittiva oħra tat-trio: il-hash. Mhijiex. Hash hija funzjoni unika li tikkompressa — jidħlu ħafna bytes, toħroġ marka qasira, hemmhekk jispiċċa t-triq. Identità kriptografika hija par matematiku komplementari: is-sigriet jibqa' u jiffirma; il-kontroparti pubblika tiegħu tiġi ppubblikata u tivverifika. Fejn il-hash iwaqqa' l-informazzjoni f'direzzjoni waħda, l'identità tistabbilixxi asimmetrija bejn żewġ nofsijiet. Il-hash jixhed x'intqal; l'identità tixhed min qalha.

Dak li l-frażi mhijiex

Tliet żbalji frekwenti għandhom jiġu kklerjati. Il-frażi mhijiex password f'sens proprju: mhijiex imqabbla ma' marka tas-swaba' maħżuna fuq server; tiddaħħal fl-apparat tal-utent biex tibni mill-ġdid l-identità b'mod matematiku. Il-frażi ma tistax tiġi rkuprata: jekk tintilef, m'hemm ħadd mingħand min titlobha; jekk tiġi dduplikata, l-identità tiġi dduplikata wkoll. Il-frażi mhijiex kredenzjali separabbli mill-identità: il-frażi *hija* l-identità. Min għanduha jista' jaġixxi bħala dik l-identità, mingħajr permess addizzjonali, mingħajr proċess ta' awtorizzazzjoni, mingħajr irkupru possibbli.

Din it-tielet proprjetà hija dik li tbiddel il-piż tal-kwistjoni. Password mitlufa hija inkonvenjent amministrattiv. Identità kriptografika mitlufa hija l-identità nnifisha. Karta bil-frażi misjuba minn terzi mhijiex riskju ta' serq ta' kont: hija l-konsenja tal-identità kollha. Il-wegħda tas-sistema —li ħadd ma jista' jirrevoka l-identità tiegħek jew jimblukkak b'mod arbitrarju— tiġi akkumpanjata b'mod inseparabbli mir-responsabbiltà —li inti l-uniku kustodju ta' xi ħaġa li ħadd ma jista' jreġġa' lura għalik.

Il-wegħda u l-piż

Il-mudell ta' identità kriptografika spiss jirċievi l-kwalifika ta' *sovran-awtonoma* —self-sovereign fil-letteratura anglo-sassona—. L-għażla tal-kelma hija deliberata u tiddeskrivi l-kundizzjoni b'mod pjuttost preċiż. L-utent huwa sovran fuq l-identità tiegħu f'sens kważi medjevali: ma jagħtiha ebda re, ebda emittent, ebda awtorità ċentrali; u lanqas ma jista' jirtiraha ħadd minn dawk imsemmija qabel. Iżda wkoll, bħall-monarka medjevali, l-utent iġorr il-konsegwenza sħiħa tal-iżbalji tiegħu: m'hemm l-ebda reġent li jieħu deċiżjonijiet f'ismu jekk jitlef is-siġill.

L-għażla bejn identità ġestita minn parti terza u identità sovran-awtonoma m'għandhiex tweġiba universali korretta waħda. Għall-kont ta' forum irrilevanti, l-identità ġestita hija probabbilment proporzjonata għar-riskju. Għal identità professjonali li tiffirma dokumenti li huma legalment vinkolanti, għal identità ekonomika li tgħasses it-tfaddil personali tagħha, għal identità ta' komunikazzjoni professjonali ma' klijenti li fdaw

informazzjoni sensittiva, il-kwistjoni tinbidel. Hemmhekk il-mistoqsija tieqaf milli tkun «huwa konvenjenti?» u ssir «min, minbarra jien, għandu s-setgħa li jaġixxi bħali, u taħt liema ċirkostanzi?».

Fejn jidher dan il-mekkaniżmu f'sistemi reali

Il-BIP39 twieled fid-dinja tal-Bitcoin fl-2013 u nfirex malajr fl-ekosistema kollha tal-kriptovaluti: kull kartiera serja llum taċċetta frażi BIP39 ta' tnax jew erbgħa u għoxrin kelma bħala backup tal-identità ekonomika tad-detentur tagħha. Barra mill-kriptovaluti, l-istess kunċett sottostanti — par kriptografiku li jagħti prova tal-awtur mingħajr intermedjarju — jidher f'sistemi oħra b'sintassi differenti. Iċ-ċwievet SSH li amministratur tas-sistemi juża biex jaċċessa s-servers tiegħu huma każ klassiku: ċavetta privata li l-amministratur iżomm fuq il-magna tiegħu u waħda pubblika li tiġi kkupjata fuq kull server; l-ebda entità komparabbli ma' servizz ċentralizzat ma tintervjeni. Il-protokoll Signal juża Ed25519 b'materjal taċ-ċavetta persistenti fuq it-tagħmir; l-eIDAS Ewropej, fil-parti tagħhom ta' firma kkwalifikata, jistrieħu fuq l-istess prinċipju kriptografiku, bid-differenza li ċ-ċavetta hija kkurata minn fornitur ta' servizzi ta' fiduċja kkwalifikat minflok mill-utent.

Solo2, il-pjattaforma tal-pubblikazzjoni ta' din il-pubblikazzjoni, tuża frażi BIP39 ta' erbgħa u għoxrin kelma bħala identità ta' kull utent. L-utent, meta joħloq il-kont tiegħu, jara l-kliem darba. Dawn mhumiex maħżuna fuq l-ebda server ta' Solo2 jew ta' ħaddieħor: jekk l-utent jannotahom u jikkurahom, huwa jżomm l-identità tiegħu għal dejjem. Jekk jitlefhom, jitlefhom. Hija l-konsegwenza koerenti ma' arkitettura mingħajr operatur fin-nofs: li kieku Solo2 seta' jagħti l-identità lura lill-utent li tilifha, seta' wkoll jagħtiha lil kull min jagħmel pressjoni fuq Solo2 biex jagħtihielu.

Għall-qarrej professjonali

Erba' kunsiderazzjonijiet għal min qed jevalwa l-adozzjoni ta' identità kriptografika sovrana (autosoberana) f'kuntest professjonali:

1. Il-frażi hija l-identità. Il-kura fiżika — karta, diversi kopji f'postijiet differenti, eventwalment metall imnaqqax għal użu fit-tul — toffri aktar garanziji mill-kura diġitali, li żżid is-superfiċje tal-attakk mingħajr ma tnaqqas ir-riskju ta' telf.
2. M'hemm l-ebda rkupru. It-tfassil tal-proċess billi wieħed jassumi li xi darba l-kopja primarja tintilef huwa ħafna aktar għaqli milli tiskoprih dakinhar li tintilef. It-tieni kopja separata ġeografikament issolvi kważi kull xenarju.
3. Mhuwiex l-istess ħaġa bħal ċertifikat ikkwalifikat eIDAS. Għal firma kkwalifikata fl-Unjoni — atti notarili, ċerti proċeduri mal-Amministrazzjoni — il-leġiżlazzjoni teħtieġ fornitur ikkwalifikat li jikkura ċ-ċavetta. L-identità kriptografika sovrana sservi għall-komunikazzjoni professjonali u l-iffirmar dokumentarju b'valur probatorju, iżda ma tissostitwixxix awtomatikament iċ-ċertifikat ikkwalifikat f'każijiet fejn in-norma teħtieġu.
4. Jekk l-identità se tiġi trasferita — wirt, suċċessjoni professjonali, għeluq tal-attività — huwa rakkomandabbli li tħejji l-proċedura qabel, mhux wara. Proċeduri formali b'envelops issiġillati bil-laker (lacre), struzzjonijiet lil eżekutur testamentarju, depożitu f'uffiċċju notarili, huma arranġamenti klassiċi perfettament kompatibbli man-natura kriptografika tal-attiv.

Dan l-artiklu jagħlaq it-trio kunċettwali li fetaħ iċ-ċiklu — hash, kriptaġġ, identità —. It-tliet ideat jinbnew fuq xulxin: il-hash jagħti l-marka li ma tinbidilx, il-kriptaġġ jagħti l-kunfidenzjalità mingħajr it-tielet parti fdata, l-identità tagħti l-awtur mingħajr it-tielet parti tal-konċessjoni. It-tlieta jaqsmu proprjetà li lanqas mhi ideoloġika: jittrasferixxu, minn min imexxi servizz għal min jużah, kapaċitajiet tekniċi li tradizzjonalment kienu jinsabu għand l-operatur. Jittrasferixxu wkoll responsabbiltajiet magħhom. Li titkellem b'onestà dwar kwalunkwe mit-tlieta teħtieġ li titkellem ukoll dwar it-tnejn l-oħra.

Sorsi u aktar qari

- Palatinus, M.; Rusnak, P.; Voisine, A.; Bowe, S. — *BIP-0039: Mnemonic code for generating deterministic keys*, proposta ta’ titjib tal-Bitcoin tal-2013. Standard de facto għal frażijiet ta’ rkupru fl-industrija tal-kripto.
- RFC 8032 — Edwards-Curve Digital Signature Algorithm (EdDSA), inkluż Ed25519. IETF, Jannar 2017. Speċifikazzjoni normattiva tal-iskema tal-firma użata f’parti kbira mill-industrija kontemporanja.
- RFC 2898 — PKCS #5: Password-Based Cryptography Specification, verżjoni 2.0. IETF, Settembru 2000. Jiddefinixxi l-algoritmu PBKDF2 użat fid-derivazzjoni tal-BIP39 minn frażi għal żerriegħa (seed).
- Regolament (UE) 910/2014 (eIDAS) u l-evoluzzjoni tiegħu mir-Regolament (UE) 2024/1183 (eIDAS 2) — qafas Ewropew għall-identità elettronika u l-firma kkwalifikata. Reġim differenti minn dak sovran, iżda appoġġjat kunċettwalment mill-istess primittivi kriptografiċi.
- Allen, C. — *The Path to Self-Sovereign Identity* (2016). Test kanoniku dwar il-prinċipji u l-impenji tal-mudell sovran, preċedenti iżda rilevanti għall-fehim tal-familja ta’ soluzzjonijiet kontemporanji.

← PreċedentiIl-mudell tan-negozju bħala sinjal ta' fiduċjaLi jmiss →Self-hosting bħala prattika professjonali

Letturi riċenti

- Riflessjoni · 29 ta’ Ġunju 2026 M'intix anonimu
- Riflessjoni · 27 ta’ Mejju 2026 Dak li firma ma tistax tirranġa
- Analiżi · 26 ta’ Mejju 2026 Privatezza reali vs apparenti: il-mistoqsijiet li jaqbel li tistaqsi lilek innifsek

Ħu dan l-artiklu miegħek kull fejn għandek bżonnu.

↓ Markdown ↓ Test sempliċi ↓ PDF

Il-fajl se jitniżżel fuq it-tagħmir tiegħek. Minn hemm tista' ssalvah, timportah f'Solo2 jew taqsmu kull fejn tixtieq. Cuadernos ma jiddeċidix id-destinazzjoni għalik.

Siġill tax-xama' · SHA-256 27f949fe5bba477480e5d5322ef1a5e72374ab2184688b415b4e1f4446dbf313

Cuadernos Lacre · Pubblikazzjoni ta' Menzuri Gestión S.L. ·
miktuba minn R.Eugenio · editjata mit-tim ta' Solo2.