Οι 24 λέξεις: τι είναι μια κρυπτογραφική ταυτότητα

Μια κρυπτογραφική ταυτότητα δεν είναι κωδικός πρόσβασης: δεν την αποθηκεύει κανένας διακομιστής και δεν ανακτάται. Μια διδακτική εξήγηση του μηχανισμού BIP39, γιατί ακριβώς είκοσι τέσσερις λέξεις και τι πραγματικό βάρος φέρει αυτός που τις κατέχει.

Για να συνεννοηθούμε: Αν ξεχάσετε τον κωδικό πρόσβασης του Gmail σας, η Google τον επαναφέρει. Αν χάσετε τις 24 λέξεις που αποτελούν μια κρυπτογραφική ταυτότητα, δεν υπάρχει κανένας να τις ζητήσετε. Δεν είναι ότι η διαδικασία είναι αυστηρή — είναι ότι δεν υπάρχει κανείς στην άλλη άκρη. Αυτή η διαφορά είναι όλη η ουσία.

Η διαφορά μεταξύ ενός κωδικού πρόσβασης και μιας ταυτότητας

Ένας κωδικός πρόσβασης, στο κλασικό μοντέλο του διαδικτύου, δεν είναι η ταυτότητα του χρήστη. Είναι ένα αποδεικτικό. Ο χρήστης έχει μια ταυτότητα —ένα όνομα, ένα email, έναν αριθμό πελάτη— και, για να αποδείξει σε έναν διακομιστή ότι είναι αυτός που λέει, παρουσιάζει έναν κωδικό πρόσβασης τον οποίο ο διακομιστής συγκρίνει με ένα αποθηκευμένο αποτύπωμα. Εάν τα αποτυπώματα συμπίπτουν, ο διακομιστής επιτρέπει τη συνεδρία. Εάν ο κωδικός πρόσβασης χαθεί, ο χρήστης παραμένει ο ίδιος χρήστης· αυτό που χάνει είναι το αποδεικτικό, και υπάρχει μια διαδικασία ανάκτησης —ένα email στην εγγεγραμμένη διεύθυνση, μια ερώτηση ασφαλείας— για την αποκατάστασή του.

Μια κρυπτογραφική ταυτότητα λειτουργεί διαφορετικά. Δεν είναι ένα διαπιστευτήριο που κάποιος συγκρίνει με ένα αποθηκευμένο αποτύπωμα· *είναι* ένα πλήρες μαθηματικό μυστικό από μόνο του. Δεν έχει σημασία πού βρίσκεται —σε ένα χαρτί, σε μια συσκευή, ακόμα και σε έναν ξένο διακομιστή—: η ταυτότητα υπάρχει λόγω των μαθηματικών της, όχι λόγω αυτού που την επικυρώνει. Εδώ εμφανίζεται μια ιδιότητα παρόμοια με αυτή που είδαμε στο «Τι είναι πραγματικά το SHA-256»: η κατοχή δεν αποδεικνύεται επιδεικνύοντας το μυστικό, αλλά χρησιμοποιώντας το για υπογραφή. Την υπογραφή που παράγεται με αυτόν τον τρόπο μπορεί ο καθένας να την ελέγξει με μια δημόσια τιμή που προκύπτει μαθηματικά από το ίδιο το μυστικό, χωρίς να χρειάζεται να γνωρίζει το μυστικό και χωρίς τη μεσολάβηση τρίτου μέρους στον έλεγχο. Όποιος έχει το μυστικό, είναι η ταυτότητα· όποιος το χάσει, παύει να είναι. Η απόφαση είναι κατηγορηματική: **δεν υπάρχει κανένας να του ζητήσετε να σας επιστρέψει την ταυτότητα. Αυτός ο κάποιος δεν υπάρχει, γιατί δεν την είχε εξαρχής.**

Τι αντιπροσωπεύουν είκοσι τέσσερις λέξεις

Η κρυπτογραφική ταυτότητα αντιπροσωπεύεται συνήθως από ένα μαθηματικό μυστικό τριάντα δύο byte — διακοσίων πενήντα έξι bit—. Ένας αριθμός δύσκολος στη συγκράτηση και ακόμα πιο δύσκολος στη μεταγραφή χωρίς σφάλμα. Η βιομηχανία της κρυπτογραφίας έλυσε αυτό το πρόβλημα το 2013 με ένα μικρό και κομψό πρότυπο που ονομάζεται BIP39: ένας τρόπος αναπαράστασης αυτών των διακοσίων πενήντα έξι bit ως μια ακολουθία είκοσι τεσσάρων λέξεων παρμένων από μια επίσημη λίστα δύο χιλιάδων σαράντα οκτώ λέξεων. Η αριθμητική από πίσω ταιριάζει με κομψότητα· όποιος θέλει να τη δει λεπτομερώς τη βρίσκει στο περιθώριο.

Η μέτρηση ξεκινά από το τέλος. Θέλουμε να αναπαραστήσουμε τα διακόσια πενήντα έξι bit του μυστικού προσθέτοντας οκτώ bit αθροίσματος ελέγχου (checksum): διακόσια εξήντα τέσσερα bit συνολικά. Εάν τα μοιράσουμε σε είκοσι τέσσερις λέξεις —ένας διαχειρίσιμος αριθμός για σημείωση και υπαγόρευση χωρίς

απώλεια— κάθε λέξη πρέπει να συνεισφέρει ακριβώς έντεκα bit πληροφορίας. Και έντεκα bit είναι δύο εις την ενδεκάτη πιθανότητες, δηλαδή δύο χιλιάδες σαράντα οκτώ. Εξ ου και το επίσημο λεξιλόγιο BIP39 έχει ακριβώς αυτό το μέγεθος: η λίστα υπάρχει στα μέτρα του προβλήματος, όχι το αντίστροφο.

Η μέτρηση δεν είναι διακοσμητική. Εάν κάποιος μεταγράψει σωστά είκοσι τρεις λέξεις και κάνει λάθος στην εικοστή τέταρτη, το άθροισμα ελέγχου θα το εντοπίσει: το λογισμικό θα του πει «αυτή η ακολουθία δεν είναι έγκυρη». Εάν κάποιος μεταγράψει και τις είκοσι τέσσερις σωστά, το λογισμικό θα αντλήσει την ίδια ταυτότητα χωρίς ασάφεια. Η επιλογή της λίστας λέξεων είναι επίσης σκόπιμη: οι λέξεις του λεξιλογίου BIP39 είναι σύντομες, διακριτές μεταξύ τους, χωρίς διακριτικά, επιλεγμένες για την ελαχιστοποίηση φωνητικών και ορθογραφικών συγχύσεων. Είναι ένα λεξιλόγιο σχεδιασμένο να απομνημονεύεται, να γράφεται και να υπαγορεύεται από ανθρώπους χωρίς απώλεια.

Από τη φράση στο κλειδί

Οι είκοσι τέσσερις λέξεις δεν είναι το κρυπτογραφικό κλειδί που υπογράφει μηνύματα. Είναι μια ανακτήσιμη αναπαράσταση της αρχικής εντροπίας που, μέσω μιας ντετερμινιστικής διαδικασίας που ονομάζεται PBKDF2, μετατρέπεται σε έναν «σπόρο» (seed) εξήντα τεσσάρων byte. Από αυτόν τον σπόρο παράγονται, επίσης ντετερμινιστικά, τα συγκεκριμένα κρυπτογραφικά κλειδιά που χρησιμοποιεί ο χρήστης: ένα ιδιωτικό κλειδί για υπογραφή και ένα αντίστοιχο δημόσιο κλειδί που δημοσιεύεται για την επαλήθευση των υπογραφών. Ο ίδιος μηχανισμός σε διαφορετικά συστήματα: τα κρυπτονομίσματα χρησιμοποιούν την καμπύλη secp256k1· το πρωτόκολλο Signal και πολλά σύγχρονα συστήματα χρησιμοποιούν το Ed25519 πάνω στην καμπύλη Curve25519. Για μια συγκεκριμένη καμπύλη όπως η Ed25519, τα πρότυπα BIP32 και SLIP-0010 λαμβάνουν αυτόν τον σπόρο των εξήντα τεσσάρων byte και παράγουν, ντετερμινιστικά, τα τριάντα δύο byte που αποτελούν το αποτελεσματικό κλειδί υπογραφής — τα ίδια τριάντα δύο byte με τα οποία ξεκινά το παράδειγμα κώδικα στην επόμενη ενότητα.

Αυτός είναι ο τυπικός τρόπος με τον οποίο ολόκληρη η βιομηχανία παρουσιάζει τον μηχανισμό στον χρήστη — πορτοφόλια κρυπτονομισμάτων, διαχειριστές αποκεντρωμένης ταυτότητας, το Signal στο τμήμα της μόνιμης ταυτότητάς του, το Solo2 μεταξύ αυτών—: ο χρήστης, στην πράξη, δεν βλέπει ποτέ τον σπόρο ούτε τα παραγόμενα κλειδιά. Βλέπει τις είκοσι τέσσερις λέξεις κατά τη δημιουργία της ταυτότητάς του και, προαιρετικά, τις σημειώνει σε ένα χαρτί. Οι λέξεις ταξιδεύουν στη συνέχεια μεταξύ των συσκευών του όταν θέλει να μεταφέρει την ταυτότητα: τις εισάγει στη νέα εφαρμογή, η εφαρμογή παράγει τον ίδιο σπόρο, τα ίδια κλειδιά, την ίδια ταυτότητα. Είναι ένας φορητός μηχανισμός, κρυπτογραφικά στιβαρός και, εντός των ορίων του λογικού, απομνημονεύσιμος.

Πώς υπογράφουμε με το κλειδί (μια πινελιά Zig)

Στη Zig, μόλις έχετε τον σπόρο των τριάντα δύο byte που προέρχεται από τις είκοσι τέσσερις λέξεις, η υπογραφή ενός μηνύματος με Ed25519 χωράει σε λίγες γραμμές:

```
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);
```

Η λειτουργία της υπογραφής παράγει εξήντα τέσσερα byte —που ονομάζονται υπογραφή— τα οποία θα μπορούσαν να έχουν δημιουργηθεί μόνο από το αντίστοιχο ιδιωτικό κλειδί. Η επαλήθευση είναι δημόσια: οποιοσδήποτε με το δημόσιο κλειδί μπορεί να ελέγξει ότι η υπογραφή αντιστοιχεί στο μήνυμα. Χωρίς το ιδιωτικό κλειδί, κανείς δεν μπορεί να παράγει μια έγκυρη υπογραφή για αυτό το μήνυμα· με το δημόσιο κλειδί, όλοι μπορούν να ανιχνεύσουν εάν μια υπογραφή είναι έγκυρη. Αυτή η ασυμμετρία είναι που επιτρέπει στον υπογράφοντα να αποδείξει την πατρότητα χωρίς να μοιραστεί το μυστικό.

Το προηγούμενο παράδειγμα είναι η ελάχιστη έκδοση του εγχειριδίου. Στον πραγματικό κώδικα του Solo2, η αλυσίδα διασχίζει δύο αρχεία, ένα σε JavaScript που ζει στον περιηγητή του χρήστη και ανακατασκευάζει την εντροπία από τις είκοσι τέσσερις λέξεις, και ένα άλλο σε Zig μέσα στη βιβλιοθήκη *zcatcrypto* που παίρνει αυτή την εντροπία και παράγει τα συγκεκριμένα κρυπτογραφικά κλειδιά. Ξεκινώντας από την πλευρά του περιηγητή:

```
// 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 };
}
```

Αυτά τα τριάντα δύο bytes εντροπίας, μαζί με άλλα τριάντα δύο που παράγονται στο ίδιο βήμα, ταξιδεύουν στη μονάδα WebAssembly της Zig που δημιουργεί τα ίδια τα κλειδιά Ed25519. Η πλήρης συνάρτηση, με τον τελικό καθαρισμό της μνήμης, χωράει σε μία οθόνη:

```
// 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;
}
```

Δύο λεπτομέρειες αξίζει να σημειωθούν. Η πρώτη: ένας ίδιος σπόρος (seed) παράγει πάντα το ίδιο ζεύγος κλειδιών — αυτό ακριβώς επιτρέπει την ανάκτηση της ταυτότητας εισάγοντας τις είκοσι τέσσερις λέξεις σε μια νέα συσκευή. Η δεύτερη: ο σπόρος διαγράφεται ρητά από τη μνήμη στην τελευταία γραμμή. Μετά από αυτό το σημείο, ούτε καν η ίδια η συνάρτηση δεν θα μπορούσε να ανακατασκευάσει τα κλειδιά· οι λέξεις του χρήστη θα ήταν η μόνη πηγή.

Για όποιον θέλει να το ελέγξει με μικρούς αριθμούς. Το σχήμα υπογραφής μπορεί να διανυθεί ολόκληρο με ψηφία αρκετά μικρά ώστε να γίνουν οι πράξεις με το χέρι. Όποιος προτιμά να μην μπει στην αριθμητική μπορεί να παραλείψει αυτό το μπλοκ χωρίς να χάσει το νήμα του άρθρου· όποιος θέλει να δει τον μηχανισμό να λειτουργεί βήμα προς βήμα θα τον βρει εδώ. **Οι δημόσιοι κανόνες**, που οποιοσδήποτε μπορεί να διαβάσει: ένας πρώτος αριθμός $p = 23$ (στο πραγματικό Ed25519 είναι περίπου εβδομήντα επτά ψηφίων· χρησιμοποιούμε είκοσι τρία για να χωρέσουν οι πράξεις σε μια σελίδα), μια βάση $g = 2$ της οποίας η τάξη σε αυτή την ομάδα είναι $q = 11$, και η σύμβαση ότι όλη η αριθμητική με το g γίνεται *módulo p* και όλοι οι εκθέτες μειώνονται *módulo q*. **Η ιδιωτική επιλογή**, μία και μοναδική και ποτέ κοινοποιημένη: το μυστικό $x = 6$. Αυτή είναι η ταυτότητα.

Βήμα 1 — Το δημόσιο μέρος της ταυτότητας. Υπολογίζεται μία φορά και δημοσιεύεται ανοιχτά.

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

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

Το δημόσιο μέρος της ταυτότητας είναι το **18**. Οποιοσδήποτε μπορεί να το πάρει και να το χρησιμοποιήσει για να επαληθεύσει υπογραφές που έγιναν με αυτή την ταυτότητα. Κανείς, παρατηρώντας μόνο το 18, δεν μπορεί να ανακτήσει το μυστικό 6: αυτό είναι το πρόβλημα του διακριτού λογαρίθμου στο οποίο θα επιστρέψουμε στο τέλος.

Βήμα 2 — Υπογραφή μηνύματος. Ο κάτοχος της ταυτότητας θέλει να υπογράψει το μήνυμα $m = 7$. Ξεκινά επιλέγοντας μια νέα τυχαία τιμή $k = 4$, η οποία θα χρησιμοποιηθεί μόνο μία φορά και δεν θα κοινοποιηθεί ποτέ (στο πραγματικό Ed25519, το k παράγεται ντετερμινιστικά από το μήνυμα και το μυστικό για να αποφευχθεί ο κίνδυνος επαναχρησιμοποίησης, αλλά ο ρόλος που παίζει είναι ακριβώς αυτός). Στη συνέχεια υπολογίζει τρεις αριθμούς:

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

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

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

Η υπογραφή είναι το ζεύγος **(r, s) = (16, 10)**. Ταξιδεύει ανοιχτά μαζί με το μήνυμα. Οποιοσδήποτε μπορεί να την διαβάσει. Διδακτική σημείωση: στο πραγματικό Ed25519 η συνάρτηση H είναι η SHA-512, κρυπτογραφικά

ισχυρή· εδώ χρησιμοποιούμε την απλοποίηση $e = (r + m) \bmod q$ ώστε ο αναγνώστης να μπορεί να ακολουθήσει τα βήματα χωρίς να χρειάζεται να υπολογίσει ένα hash. Η δομή του αλγορίθμου είναι η ίδια.

Βήμα 3 — Επαλήθευση της υπογραφής. Ο επαληθευτής έχει το δημόσιο μέρος $y = 18$, το μήνυμα $m = 7$, και την υπογραφή $(r, s) = (16, 10)$. Ανακατασκευάζει το e με τον ίδιο τρόπο —$e = (16 + 7) \bmod 11 = 1$— και ελέγχει αν αυτή η ισότητα ισχύει:

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

Υπολογίζει τις δύο πλευρές χωριστά:

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

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

Οι δύο πλευρές δίνουν **12**. Η υπογραφή είναι έγκυρη. Οποιοσδήποτε με το δημόσιο μέρος 18 μπορεί να καταλήξει σε αυτό το συμπέρασμα χωρίς να έχει μάθει ποτέ ότι το μυστικό ήταν 6.

Και ένας τρίτος που θα προσπαθούσε να πλαστογραφήσει; Η Εύα έχει δει να περνά από το κανάλι ό,τι είναι δημόσιο: $p = 23$, $g = 2$, $q = 11$, $y = 18$, $m = 7$, $r = 16$, $s = 10$. Για να υπογράψει ένα *διαφορετικό* μήνυμα στο όνομα αυτής της ταυτότητας, θα έπρεπε να γνωρίζει το x. Ο μόνος τρόπος της είναι να αναρωτηθεί: «για ποιον εκθέτη x ισχύει $2^x \bmod 23 = 18$;». Με $p = 23$ μπορεί να δοκιμάσει 0, 1, 2, 3, … και να το βρει σε δευτερόλεπτα. Αλλά αντικαθιστώντας το 23 με έναν πρώτο των πραγματικών διαστάσεων του Ed25519, ο χώρος των πιθανών εκθετών υπερβαίνει τον αριθμό των ατόμων στο παρατηρήσιμο σύμπαν. **Δεν υπάρχει σήμερα κανένας αλγόριθμος γνωστός στην ανθρωπότητα που να μπορεί να διανύσει αυτόν τον χώρο σε λιγότερο από δισεκατομμύρια χρόνια.** Είναι το ίδιο πρόβλημα του διακριτού λογαρίθμου που στηρίζει το Diffie-Hellman του προηγούμενου άρθρου, εφαρμοσμένο εδώ στο σχήμα υπογραφής.

Αυτό που μόλις διανύσαμε είναι *ακριβώς* το Schnorr, το σχήμα υπογραφής του οποίου το Ed25519 είναι μια παραλλαγή προσαρμοσμένη σε μια ελλειπτική καμπύλη. Στο πραγματικό Ed25519, όλες οι πράξεις γίνονται πάνω στα σημεία μιας συγκεκριμένης καμπύλης (Curve25519) αντί για ακέραιους αριθμούς modulo ενός πρώτου, και η συνάρτηση H είναι η SHA-512 αντί για το άθροισμα-παιχνίδι που χρησιμοποιήσαμε παραπάνω. Οι δύο αντικαταστάσεις είναι προσαρμογές υλοποίησης — κέρδος κρυπτογραφικής αντοχής στην ωμή βία, κέρδος πρόσθετων ιδιοτήτων ασφαλείας για το k. Η αλγοριθμική δομή, οι τρεις πράξεις, το γιατί της ασυμμετρίας, είναι τα ίδια.

Εδώ ενδείκνυται μια σύντομη στάση, γιατί ολόκληρη η αλυσίδα μπορεί να συγχέεται με μια γρήγορη ματιά με μια άλλη πρωταρχική της τριάδας: το hash. Δεν είναι. Ένα hash είναι μια μοναδική συνάρτηση που συμπιέζει — εισέρχονται πολλά bytes, εξέρχεται ένα σύντομο αποτύπωμα, εκεί τελειώνει η διαδρομή. Μια κρυπτογραφική ταυτότητα είναι ένα συμπληρωματικό μαθηματικό ζεύγος: το μυστικό μένει και υπογράφει· το δημόσιο αντίστοιχό του δημοσιεύεται και επαληθεύει. Εκεί που το hash καταρρέει τις πληροφορίες προς μία κατεύθυνση, η ταυτότητα εγκαθιστά μια ασυμμετρία μεταξύ δύο μισών. Το hash πιστοποιεί τι ειπώθηκε· η ταυτότητα πιστοποιεί ποιος το είπε.

Τι δεν είναι η φράση

Τρεις συχνές παρανοήσεις πρέπει να αποσαφηνιστούν. Η φράση δεν είναι κωδικός πρόσβασης με την κυριολεκτική έννοια: δεν συγκρίνεται με ένα αποτύπωμα αποθηκευμένο σε έναν διακομιστή· εισάγεται στη συσκευή του χρήστη για να ανακατασκευάσει μαθηματικά την ταυτότητα. Η φράση δεν ανακτάται: εάν χαθεί, δεν υπάρχει κανείς να τη ζητήσετε· εάν αναπαραχθεί, αναπαράγεται και η ταυτότητα. Η φράση δεν είναι ένα διαπιστευτήριο διαχωρίσιμο από την ταυτότητα: η φράση *είναι* η ταυτότητα. Όποιος την έχει μπορεί να ενεργεί ως αυτή, χωρίς πρόσθετη άδεια, χωρίς διαδικασία εξουσιοδότησης, χωρίς δυνατότητα ανάκτησης.

Αυτή η τρίτη ιδιότητα είναι που αλλάζει το βάρος του ζητήματος. Ένας χαμένος κωδικός πρόσβασης είναι μια διοικητική ενόχληση. Μια χαμένη κρυπτογραφική ταυτότητα είναι η ίδια η ταυτότητα. Ένα χαρτί με τη φράση που βρέθηκε από τρίτους δεν είναι κίνδυνος κλοπής λογαριασμού: είναι η παράδοση ολόκληρης της ταυτότητας. Η υπόσχεση του συστήματος —ότι κανείς δεν μπορεί να σας ανακαλέσει την ταυτότητά σας ή να σας μπλοκάρει αυθαίρετα— συνοδεύεται αναπόσπαστα από την ευθύνη —ότι εσείς είστε ο μόνος θεματοφύλακας κάτι που κανείς δεν μπορεί να αποκαταστήσει για εσάς.

Η υπόσχεση και το βάρος

Το μοντέλο της κρυπτογραφικής ταυτότητας δέχεται συχνά τον χαρακτηρισμό *αυτοκυρίαρχη* —self-sovereign στην αγγλοσαξονική βιβλιογραφία—. Η επιλογή της λέξης είναι σκόπιμη και περιγράφει με μεγάλη ακρίβεια την κατάσταση. Ο χρήστης είναι κυρίαρχος της ταυτότητάς του με μια σχεδόν μεσαιωνική έννοια: δεν την παραχωρεί κανένας βασιλιάς, κανένας εκδότης, καμία κεντρική αρχή· ούτε μπορεί να την αφαιρέσει κανένας από τους παραπάνω. Αλλά επίσης, όπως ο μεσαιωνικός μονάρχης, ο χρήστης φέρει ολόκληρη τη συνέπεια των λαθών του: δεν υπάρχει αντιβασιλέας που να λαμβάνει αποφάσεις στη θέση του εάν χάσει τη σφραγίδα.

Η επιλογή μεταξύ ταυτότητας που διαχειρίζεται τρίτος και αυτοκυρίαρχης ταυτότητας δεν έχει μία παγκόσμια σωστή απάντηση. Για τον λογαριασμό ενός ασήμαντου φόρουμ, η διαχειριζόμενη ταυτότητα είναι πιθανώς ανάλογη του κινδύνου. Για μια επαγγελματική ταυτότητα που υπογράφει νομικά δεσμευτικά έγγραφα, για μια οικονομική ταυτότητα που φυλάσσει προσωπικές αποταμιεύσεις, για μια ταυτότητα επαγγελματικής επικοινωνίας με πελάτες που έχουν εμπιστευθεί ευαίσθητες πληροφορίες, το ζήτημα αλλάζει. Εκεί η ερώτηση παύει να είναι «είναι βολικό;» και γίνεται «ποιος, εκτός από εμένα, έχει τη δύναμη να ενεργεί ως εγώ, και υπό ποιες συνθήκες;».

Πού εμφανίζεται αυτός ο μηχανισμός σε πραγματικά συστήματα

Το BIP39 γεννήθηκε στον κόσμο του Bitcoin το 2013 και εξαπλώθηκε γρήγορα σε ολόκληρο το οικοσύστημα των κρυπτονομισμάτων: οποιοδήποτε σοβαρό πορτοφόλι σήμερα δέχεται μια φράση BIP39 δώδεκα ή είκοσι τεσσάρων λέξεων ως εφεδρικό αντίγραφο της οικονομικής ταυτότητας του κατόχου του. Εκτός των κρυπτονομισμάτων, η ίδια υποκείμενη έννοια — ένα κρυπτογραφικό ζεύγος που αποδεικνύει την πατρότητα χωρίς μεσάζοντα — εμφανίζεται σε άλλα συστήματα με διαφορετική σύνταξη. Τα κλειδιά SSH που χρησιμοποιεί ένας διαχειριστής συστημάτων για την πρόσβαση στους διακομιστές του είναι μια κλασική περίπτωση: ένα ιδιωτικό κλειδί που ο διαχειριστής φυλάσσει στο μηχάνημά του και ένα δημόσιο που αντιγράφεται σε κάθε διακομιστή· δεν παρεμβαίνει καμία οντότητα συγκρίσιμη με μια κεντρική υπηρεσία. Το πρωτόκολλο Signal χρησιμοποιεί Ed25519 με μόνιμο υλικό κλειδιού στη συσκευή· το ευρωπαϊκό eIDAS, στο μέρος της ειδικής υπογραφής, βασίζεται στην ίδια κρυπτογραφική αρχή, με τη διαφορά ότι το κλειδί φυλάσσεται από έναν ειδικό πάροχο υπηρεσιών εμπιστοσύνης αντί για τον χρήστη.

Το Solo2, η πλατφόρμα έκδοσης αυτού του εντύπου, χρησιμοποιεί μια φράση BIP39 είκοσι τεσσάρων λέξεων ως ταυτότητα για κάθε χρήστη. Ο χρήστης, κατά τη δημιουργία του λογαριασμού του, βλέπει τις λέξεις μία φορά. Δεν αποθηκεύονται σε κανέναν διακομιστή του Solo2 ούτε κανενός άλλου: εάν ο χρήστης τις σημειώσει και τις φυλάξει, διατηρεί την ταυτότητά του για πάντα. Εάν τις χάσει, τις έχασε. Είναι η συνεπής συνέπεια μιας αρχιτεκτονικής χωρίς μεσάζοντα χειριστή: εάν το Solo2 μπορούσε να επιστρέψει την ταυτότητα στον χρήστη που την έχασε, θα μπορούσε επίσης να τη δώσει σε οποιονδήποτε πιέσει το Solo2 για να του τη δώσει.

Για τον επαγγελματία αναγνώστη

Τέσσερις σκέψεις για όσους αξιολογούν την υιοθέτηση κρυπτογραφικής αυτοκυρίαρχης (autosoberana) ταυτότητας σε επαγγελματικό πλαίσιο:

1. Η φράση είναι η ταυτότητα. Η φυσική φύλαξη — χαρτί, πολλά αντίγραφα σε διαφορετικά μέρη, τελικά χαραγμένο μέταλλο για μακροχρόνια χρήση — προσφέρει περισσότερες εγγυήσεις από την ψηφιακή

φύλαξη, η οποία προσθέτει επιφάνεια επίθεσης χωρίς να μειώνει τον κίνδυνο απώλειας.
2. Δεν υπάρχει ανάκτηση. Ο σχεδιασμός της διαδικασίας με την υπόθεση ότι μια μέρα θα χαθεί το κύριο αντίγραφο είναι πολύ προτιμότερος από το να το ανακαλύψετε την ημέρα που θα χαθεί. Ένα δεύτερο γεωγραφικά διαχωρισμένο αντίγραφο επιλύει σχεδόν όλα τα σενάρια.
3. Δεν είναι το ίδιο με ένα ειδικό πιστοποιητικό eIDAS. Για ειδική υπογραφή στην Ένωση — συμβολαιογραφικές πράξεις, ορισμένες διαδικασίες με τη Διοίκηση — η νομοθεσία απαιτεί έναν ειδικό πάροχο που φυλάσσει το κλειδί. Η κρυπτογραφική αυτοκυρίαρχη ταυτότητα χρησιμεύει για την επαγγελματική επικοινωνία και την υπογραφή εγγράφων με αποδεικτική αξία, αλλά δεν αντικαθιστά αυτόματα το ειδικό πιστοποιητικό στις περιπτώσεις όπου ο κανόνας το απαιτεί.
4. Εάν η ταυτότητα πρόκειται να μεταβιβαστεί — κληρονομιά, επαγγελματική διαδοχή, παύση δραστηριότητας — είναι σκόπιμο να προετοιμαστεί η διαδικασία πριν, όχι μετά. Οι επίσημες διαδικασίες με φακέλους σφραγισμένους με βουλοκέρι (lacre), οι οδηγίες σε έναν εκτελεστή διαθήκης, η κατάθεση σε συμβολαιογραφείο, είναι κλασικές ρυθμίσεις απόλυτα συμβατές με την κρυπτογραφική φύση του περιουσιακού στοιχείου.

Αυτό το άρθρο κλείνει την εννοιολογική τριάδα που άνοιξε τον κύκλο — hash, κρυπτογράφηση, ταυτότητα —. Οι τρεις ιδέες χτίζονται η μία πάνω στην άλλη: το hash δίνει το αναλλοίωτο αποτύπωμα, η κρυπτογράφηση δίνει την εμπιστευτικότητα χωρίς αξιόπιστο τρίτο μέρος, η ταυτότητα δίνει την πατρότητα χωρίς τρίτο μέρος παραχώρησης. Και οι τρεις μοιράζονται μια ιδιότητα που επίσης δεν είναι ιδεολογική: μεταφέρουν, από αυτόν που διαχειρίζεται μια υπηρεσία σε αυτόν που τη χρησιμοποιεί, τεχνικές δυνατότητες που παραδοσιακά ανήκαν στον χειριστή. Μεταφέρουν μαζί τους και ευθύνες. Το να μιλάς με ειλικρίνεια για οποιαδήποτε από τις τρεις απαιτεί να μιλάς και για τις άλλες δύο.

Πηγές και περαιτέρω μελέτη

- Palatinus, M.; Rusnak, P.; Voisine, A.; Bowe, S. — *BIP-0039: Mnemonic code for generating deterministic keys*, πρόταση βελτίωσης του Bitcoin του 2013. De facto πρότυπο για φράσεις ανάκτησης στη βιομηχανία κρυπτογράφησης.
- RFC 8032 — Edwards-Curve Digital Signature Algorithm (EdDSA), συμπεριλαμβανομένου του Ed25519. IETF, Ιανουάριος 2017. Κανονιστική προδιαγραφή του σχήματος υπογραφής που χρησιμοποιείται σε μεγάλο μέρος της σύγχρονης βιομηχανίας.
- RFC 2898 — PKCS #5: Password-Based Cryptography Specification, έκδοση 2.0. IETF, Σεπτέμβριος 2000. Ορίζει τον αλγόριθμο PBKDF2 που χρησιμοποιείται στην παραγωγή BIP39 από φράση σε σπόρο (seed).
- Κανονισμός (ΕΕ) 910/2014 (eIDAS) και η εξέλιξή του από τον Κανονισμό (ΕΕ) 2024/1183 (eIDAS 2) — ευρωπαϊκό πλαίσιο για την ηλεκτρονική ταυτότητα και την ειδική υπογραφή. Καθεστώς διαφορετικό από το αυτοκυρίαρχο, αλλά εννοιολογικά υποστηριζόμενο από τα ίδια κρυπτογραφικά πρωτόγονα.
- Allen, C. — *The Path to Self-Sovereign Identity* (2016). Κανονικό κείμενο για τις αρχές και τις δεσμεύσεις του αυτοκυρίαρχου μοντέλου, προγενέστερο αλλά σχετικό για την κατανόηση της οικογένειας των σύγχρονων λύσεων.

← ΠροηγούμενοΤο επιχειρηματικό μοντέλο ως σήμα εμπιστοσύνηςΕπόμενο →Self-hosting ως επαγγελματική πρακτική

Πρόσφατα αναγνώσματα

- Στοχασμός · 29 Ιουνίου 2026 Δεν είσαι ανώνυμος
- Στοχασμός · 27 Μαΐου 2026 Αυτό που μια υπογραφή δεν μπορεί να διορθώσει
- Ανάλυση · 26 Μαΐου 2026 Πραγματική vs φαινομενική ιδιωτικότητα: οι ερωτήσεις που πρέπει να θέσετε

Πάρτε αυτό το άρθρο μαζί σας όπου το χρειάζεστε.

↓ Markdown ↓ Απλό κείμενο ↓ PDF

Το αρχείο θα ληφθεί στη συσκευή σας. Από εκεί μπορείτε να το αποθηκεύσετε, να το εισαγάγετε στο Solo2 ή να το μοιραστείτε όπου θέλετε. Το Cuadernos δεν αποφασίζει τον προορισμό για εσάς.

Σφραγίδα από βουλοκέρι · SHA-256 987bd18ab47c3f0b4d0da9466a3ff7f20e82ed4294dde7168e2eaf9f5ea18ba7

Cuadernos Lacre · Μια έκδοση της Menzuri Gestión S.L. ·
γραμμένη από τον R.Eugenio · επιμελημένη από την ομάδα του Solo2.