SeedSigner – Seed würfeln im Dice-Modus

99 Würfe → 24 Wörter · Menüpfad SeedSigner OS 0.8.7 · unabhängige Verifikation · Selbstversuch 1b · gehört zum Würfelprotokoll-Blatt 1b

⚠ **Die Ziffernfolge IST der Seed.** Aus den 99 Ziffern entstehen per SHA-256 die 24 Wörter – wer die Ziffern kennt, kennt die Wallet. Das ausgefüllte Würfelprotokoll-Blatt ist so geheim wie die Wörter.

⚠ **Erster Durchlauf immer als Übung** mit einem Wegwerf-Seed, der danach nie echte Coins trägt. Erst wenn Menü, Ablauf und Verifikation sitzen, wird der produktive Seed gewürfelt. ⚠ **Keine Kamera im Raum:** Handy weg, Webcam abgezogen, Fenster und Spiegel bedenken.

VORBEREITUNG

- ☐ Würfelprotokoll-Blatt 1b liegt bereit (20 Runden à 5 Ziffern = 99, letzte Runde 4)
- ☐ Würfel-Setup: Becher mit Deckel (Eisverpackung tut es), Wurffläche mit Rand (Schachteldeckel), fünf Würfel gleicher Sorte, Casino-Qualität
- ☐ SeedSigner an Powerbank oder Netzteil, rund 45 Sekunden booten. **Dann die microSD ziehen** – das Gerät läuft komplett aus dem RAM und meldet selbst „You can remove the SD card now". Ohne Karte kann nichts auf sie geschrieben werden. Dauerhaft: Settings → Persistent settings → Enabled, dann Advanced → MicroSD notification duration → Until SD removed.
- ☐ Zettel für Fingerprint (8 Zeichen) und abweichende Gerätebeschriftungen, Uhr

MENÜPFAD AM GERÄT (SEEDSIGNER OS 0.8.7)

1. ☐ Hauptmenü → **Tools**
2. ☐ Es gibt **zwei** Einträge „New seed": der erste mit **Kamera-Symbol** (Bild-Entropie), der zweite mit **Würfel-Symbol**. **Den zweiten wählen.** Verwechslungsgefahr – die Kamera-Variante ist ebenfalls legitim, aber nicht nachrechenbar.
3. ☐ Bildschirm „Mnemonic Length": **„24 words (99 rolls)"** wählen, nicht „12 words (50 rolls)". Beschriftung am Gerät: _____
4. ☐ Bildschirm **„Dice Roll 1/99"**: 3×3-Feld mit Würfelaugen 1 bis 6. Pro Wurf die Augenzahl anwählen und drücken, der Titel zählt hoch (2/99, 3/99 …). Vertippt? Die Löschtaste (⌫, rechts unten im Feld) nimmt die letzte Ziffer zurück – danach Zähler und Blatt neu abgleichen.
5. ☐ Nach der 99. Ziffer springt das Gerät von selbst weiter – kein Bestätigen nötig.
6. ☐ Warnbildschirm **„Caution – Classified Info!"** (Seed-Wörter privat halten, weg von Online-Geräten) → **„I understand"**
7. ☐ **„Seed Words 1/6" bis „6/6"**, vier Wörter pro Seite, „Next" bis „Done". Beim Übungs-Seed die Wörter zum Vergleichen notieren – beim echten Seed nur aufs Backup.
8. ☐ Abfrage **„Verify" / „Skip"** → **Verify**: das Gerät fragt alle 24 Wörter einzeln ab, je vier Optionen. Mitmachen, das ist der erste Backup-Test.
9. ☐ Abschluss zeigt den **Fingerprint** (8 Zeichen): _____ notieren → „Done". Erscheint „BIP-39 Passphrase": für Multisig-Cosigner nicht nutzen.
10. ☐ Der Seed liegt jetzt nur im Arbeitsspeicher (Menü „Seeds"). Strom weg = Seed weg. Für die Übung ist das gewollt.

Ablauf beim Würfeln: Pro Runde fünf Würfel schütteln, werfen, Ziffern in **fester Leserichtung** (links nach rechts) aufs Blatt, dann dieselben fünf am Gerät antippen, **Zähler am Gerät mit dem Blatt abgleichen.** Dieser Abgleich alle fünf Würfe ist die Fehlerbremse. Kein Wurf wird wiederholt, weil einem die Zahl nicht gefällt. Verkantete oder gestapelte Würfel: ganze Runde neu, Notiz aufs Blatt.

Warum 99 Würfe: Jeder Wurf bringt $\log_2 6 \approx 2{,}58$ Bit, 99 Würfe rund 256 Bit – so viel, wie 24 Wörter tragen (50 Würfe = 12 Wörter). Der SeedSigner nimmt die 99 Ziffern als Text, bildet SHA-256 daraus und leitet nach BIP39 die Wörter ab. Genau deshalb kann man ihn nachrechnen.

VERIFIKATION – DEM GERÄT NICHT GLAUBEN MÜSSEN

A ☐ **Eigenes Prüfskript** (im Werkstatt-Paket: `verify_dice_seed.py`, nur Python-Standardbibliothek plus offizielle BIP39-Wortliste, kein SeedSigner-Code): `python3 verify_dice_seed.py` starten, die 99 Ziffern auf Nachfrage eintippen (so landen sie nicht in der Befehls-History) → 24 Wörter Wort für Wort mit dem Display vergleichen. Vorher `--selftest` laufen lassen (prüft gegen die Beispiele der SeedSigner-Doku). Das Skript sendet und speichert nichts.

B ☐ **Zweite Codebasis** (optional): Ian Colemans `bip39-standalone.html` offline → „Show entropy details" → **„Base 10"** aktiv anklicken (**nie „Dice [1-6]"**: macht aus 6 eine 0) → **„Mnemonic Length" auf „24 Words"** (sonst bleibt „Use Raw Entropy" aktiv, nichts wird gehasht) → Ziffern eingeben → vergleichen.

! ☐ **Geprüft wird die Methode, nicht der echte Seed:** Rechnet das Gerät bei Übungs-Ziffern richtig, rechnet es immer richtig – der echte Seed verlässt das Gerät nie. Wer ihn dennoch gegenrechnet: **nur offline** (Tails ohne Netz), danach herunterfahren. Terminal, History und Zwischenablage sehen alles.

ZEIT

Start: _____
Würfeln fertig: _____
Verifikation fertig: _____
Datum: _____

STOLPERSTEINE / BESCHRIFTUNGEN, DIE ABWICHEN (FÜRS LOGBUCH)

_____
_____
_____

ERGEBNIS

- ☐ **Bestanden:** Die 24 Wörter aus der eigenen Rechnung sind identisch mit dem Display – der SeedSigner hat korrekt gerechnet, und der Seed hängt an keinem Hersteller-Zufall.
- ☐ **Abweichung:** Übungs-Seed verwerfen, Ziffern am Blatt gegen die Eingabe prüfen (häufigster Grund: ein Tippfehler zwischen Blatt und Gerät), Durchlauf wiederholen. Ein echter Seed wird erst gewürfelt, wenn die Übung glatt läuft.