



Würfelprotokoll – Seed selbst würfeln

SeedSigner Dice-Modus · 24 Wörter aus 99 Würfeln (SHA-256) · Selbstversuch 1b

⚠ **Diese Ziffernfolge IST der Seed.** Wer die 99 Zahlen kennt, kann die 24 Wörter nachrechnen. Nie fotografieren, nie scannen, nie digital abtippen (einzige Ausnahme: die Offline-Verifikation unten). Nach der Verifikation dieses Blatt vernichten – oder es wie das Backup selbst lagern.

⚠ **Für Selbstversuche:** Ein dokumentierter Seed gilt als kompromittiert und wird nie für echte Coins verwendet.

METHODE (KURZFASSUNG – GLEICHE WURFTECHNIK WIE BLATT 1A)

Du brauchst: 5 Casino-Würfel · Würfelbecher mit Deckel · Stift · SeedSigner (Dice-Modus, 24 Wörter = 99 Würfe). Keine Münze, keine Wörkertabelle.

1. Alle 5 Würfel zusammen werfen. **Jede Zahl von 1 bis 6 zählt** – hier gibt es keine Neuwürfe bei 5/6.
2. Ablese-Konvention vorher festlegen und durchziehen: von links nach rechts, wie die Würfel liegen (im Zweifel oben nach unten). Nicht sortieren, nicht umlegen.
3. SeedSigner booten, **dann die microSD ziehen** (läuft aus dem RAM, das Gerät meldet es selbst). Die 5 Ziffern in die Zeile eintragen und direkt am Gerät eingeben.
4. 19 Runden mit 5 Würfeln, Runde 20 mit 4 Würfeln = **99 Ziffern**. Danach zeigt der SeedSigner die 24 Wörter an.

1 **2** **3** **4** **5** = 5 Ziffern je Runde · Runde 20 nur 4 Würfel

Runde	W1	W2	W3	W4	W5	Ziffern	Runde	W1	W2	W3	W4	W5	Ziffern
1						5	11						55
2						10	12						60
3						15	13						65
4						20	14						70
5						25	15						75
6						30	16						80
7						35	17						85
8						40	18						90
9						45	19						95
10						50	20					×	99

Die 24 Wörter: Der SeedSigner zeigt sie nach der 99. Ziffer am Display an. **Sie kommen NICHT auf dieses Blatt** – direkt handschriftlich auf die Backup-Karte übertragen. Dieses Blatt trägt nur die Ziffern, und die reichen zum Nachrechnen.

ZEIT

Start: _____

Ende: _____

Tippfehler
korrigiert: _____

NOTIZEN / FEHLVERSUCHE (FÜRS LOGBUCH)

VERIFIKATION – OHNE DIESE SCHRITTE IST DER SEED NICHTS WERT

- ☐ **Unabhängig nachrechnen (Offline-Rechner, nie online):** Ziffernfolge in tools/mnemonic.py aus dem SeedSigner-Repo eingeben – oder im lokal gespeicherten Ian-Coleman-Tool, dort „Base 10“ wählen und „Mnemonic Length“ auf 24 Words stellen. ⚠ NIE dessen „Dice“-Modus – der macht aus jeder 6 eine 0 und liefert stillschweigend einen anderen Seed.
- ☐ Alle 24 Wörter stimmen exakt mit der SeedSigner-Anzeige überein. Gleiche Würfe = gleicher Seed – weicht ein Wort ab, liegt ein Tippfehler vor: abbrechen und neu würfeln.
- ☐ Wörter handschriftlich auf die Backup-Karte übertragen (kein Foto, kein Textdokument).
- ☐ Dieses Blatt vernichtet – oder es wird ab jetzt wie das Backup selbst gelagert.