2-von-3-Multisig mit Sparrow aufsetzen

Koordinator Sparrow Wallet · Cosigner BitBox02 (USB) + Trezor Safe 3 (USB) + SeedSigner (QR) · Native Segwit P2WSH · Selbstversuch 4 · gehört zu Kapitel 7/8

⚠ **Der Descriptor ist Teil des Backups.** Drei Seeds ohne die Bauanleitung `wsh(sortedmulti(2,…))` sind wertlos – niemand weiß, wie sie zusammengehören. Er wird in Teil C gesichert, **bevor** die erste Adresse Coins sieht, und liegt später bei jedem Cosigner-Backup.

⚠ **Erst Testbetrag, dann Test-Ausgaben, dann Recovery-Probe.** Echte Beträge erst danach. **Keine Passphrasen** auf den drei Cosignern. **Fingerprints, xpubs, Adressen nur auf dieses Blatt** – nicht in Chats, nicht auf Fotos.

VORBEREITUNG

- ☐ Sparrow läuft, Server-Symbol grün (eigene Node), Webcam angeschlossen. Trezor Suite und BitBoxApp sind **geschlossen** (nehmen das Gerät sonst exklusiv)
- ☐ BitBox02 und Trezor Safe 3 per USB, entsperrt. SeedSigner gebootet, **microSD gezogen**, Seed geladen (Seeds → Load a seed → Enter 24-word seed; Wortvorschläge: rechte Tasten oben/unten blättern, Mitte bestätigt), Fingerprint stimmt mit dem Würfelprotokoll überein
- ☐ Wallet-Name (neutral): _____ Uhr, Stift, dieses Blatt

A · WALLET ANLEGEN B · COSIGNER IMPORTIEREN

1. ☐ **File** → **New Wallet** → Name → Create Wallet → Settings: **Policy Type „Multi Signature HD"**, **Script Type „Native Segwit (P2WSH)"**, Cosigners **2 of 3** → drei Keystore-Reiter. Derivation `m/48'/0'/0'/2'` erscheint erst nach dem Geräteimport (Schritt 2–4) – dann stehen lassen.
2. ☐ **Keystore 1 – BitBox02:** „Connected Hardware Wallet" → „Scan…" → Gerät entsperren → „Import Keystore" → Label „BitBox02".
3. ☐ **Keystore 2 – Trezor:** dito, PIN am Gerät, Sparrow liest den xpub aus → Label „Trezor". Abfrage am Trezor: _____
4. ☐ **Keystore 3 – SeedSigner:** am Gerät **Seeds** → **Seed** → **Export Xpub** → **Multisig** → **Native Segwit** → **QR Format „Animated"** → Warnung → animierter QR. Sparrow: „Airgapped Hardware Wallet" → SeedSigner → „Scan" → Webcam aufs Display. Fingerprint am SeedSigner mit dem Sparrow-Feld vergleichen.
5. ☐ Kontrolle: drei verschiedene Fingerprints, drei xpubs, alle Derivations gleich → **Apply** → Wallet-Passwort (verschlüsselt nur die Datei, ist **keine** Passphrase und gehört **nicht** ins Backup). Settings → Descriptor beginnt mit `wsh(sortedmulti(2,`.

BitBox02 Master-Fingerprint:	**Trezor Safe 3** Master-Fingerprint:	**SeedSigner** Master-Fingerprint:
_____	_____	_____

C · DESCRIPTOR SICHERN D · ADRESSE AUF ALLEN DREI GERÄTEN PRÜFEN

6. ☐ **File** → **Export Wallet**: Format „Sparrow" (Wallet-Datei) **und** „Output Descriptor" (Text) → USB-Stick, später Kopie zu jedem Cosigner-Backup. Keine privaten Schlüssel, aber alle Adressen: privat, nicht geheim.
7. ☐ Settings → **Script Policy** → **QR-Symbol** rechts neben dem Descriptor → QR bereithalten (auch „Save PDF…").
8. ☐ **BitBox02:** Receive → **„Display Address"** → beim ersten Mal **registriert** das Gerät die Wallet (Name, xpubs – nicht wegklicken, mit der Settings-Seite abgleichen) → danach „2-of-3 Bitcoin Multisig" → Wallet-Name → Adresse: Zeichen für Zeichen mit Sparrow vergleichen.
9. ☐ **Trezor:** Receive → „Display Address" mit Trezor-Keystore → vergleichen. Trezor bestätigt nur, dass SEIN Schlüssel drinsteckt, er registriert die Cosigner nicht (Issue #7118) – deshalb sind Schritt 8 und 10 der eigentliche Schutz.
10. ☐ **SeedSigner: Tools** → **Address Explorer** → **Scan wallet descriptor** → QR aus Schritt 7 → Adressliste → Adresse #0 mit Sparrow vergleichen. 0.8.7: „Descriptor Loaded" (Policy 2 of 3, Signing Keys) → „Receive Address".
11. ☐ Vergleich = **Sparrow-Receive-Tab gegen die drei Geräte-Displays** (nicht BitBoxApp/Trezor Suite). Erst wenn **alle drei** gleich: als „Test #0" labeln.

E · TESTBETRAG + TEST-AUSGABEN F · RECOVERY-PROBE

12. ☐ Kleinbetrag an Adresse #0, Bestätigung über die eigene Node abwarten.
13. ☐ **Ausgabe 1 – BitBox + SeedSigner:** Send → „Pay to" (Ziel), Label, Amount → Create Transaction → Finalize Transaction for Signing → Sign → Scan: BitBox per USB (BitBox: Wallet, Betrag/Adresse, „Locktime on block" = Blockhöhe, normal, RBF, Total, Fee) → „Show QR" → SeedSigner **Scan** → Select Signer → Review Transaction → **„Your Change": „Verify multisig change"** wählen, Descriptor-QR aus Schritt 7 scannen, nicht „Skip" → Sign → Rück-QR → Sparrow „Scan QR" → 2/2 → **Broadcast Transaction**.
14. ☐ **Ausgabe 2 – Trezor + BitBox** (Trezor: Empfänger, Betrag, „Sperrzeit festgelegt auf Blockhöhe" = normal, Gesamtbetrag, Konto). Jedes Paar einmal, sonst ist der dritte Schlüssel unbewiesen. Drittes Paar in Schritt 15.
15. ☐ **Recovery-Probe:** File → **Close Tab** (**nichts löschen**) → Import Wallet → „Output Descriptor" → QR vom Papierausdruck scannen (oder Datei aus Schritt 6) → **neuen Namen** (z. B. „Probe") → Bestand, Adresse #0 + Fingerprints identisch. Dann „BitBox verloren" spielen: Ausgabe nur mit Trezor (wird per USB erkannt) + SeedSigner. **Zwei beliebige Seeds + Descriptor sind die Wallet, drei Seeds ohne Descriptor sind ein Rätsel.**
16. ☐ **Fingerprint-Probe vom Stahl** (sobald die Backups geschlagen sind, dann jährlich): SeedSigner, microSD gezogen, **Seeds** → **Load a seed** → **Enter 24-word seed**, Wörter **vom Stahl** abgelesen → Fingerprint mit den drei Feldern oben vergleichen. Gilt für alle drei Seeds, kein Gerät muss gelöscht werden. Danach Strom weg. Stahl 1 ☐ Stahl 2 ☐ Stahl 3 ☐

ZEIT

Start: _____
Wallet steht (B): _____
Adressen geprüft (D): _____
Erste Ausgabe / Datum: _____

STOLPERSTEINE / BESCHRIFTUNGEN, DIE ABWICHEN (FÜRS LOGBUCH)

_____

_____

ERGEBNIS

- ☐ **Bestanden:** Alle drei Geräte zeigen dieselbe Adresse, alle drei Paare haben ausgegeben, der Descriptor allein stellt die Sicht auf die Wallet wieder her, drei Stahl-Fingerprints stimmen. Erst jetzt darf die Wallet echte Beträge tragen – Descriptor-Kopien liegen bei allen drei Backups.
- ☐ **Abweichung:** Zeigt ein Gerät eine andere Adresse oder verweigert die Registrierung: **nichts einzahlen**, Fingerprints und xpubs gegen die Settings-Seite prüfen (meist falscher Keystore-Reiter oder falsche Derivation), Wallet neu anlegen.