Das Erben-Paket mit dem Nachlassplaner erstellen

Vordruckgenerator (eine HTML-Datei, offline) · Klasse A Existenzhinweis · Klasse B Zugangsanleitung · Klasse P Protokoll · Selbstversuch 7 · gehört zu Kapitel 9/12

⚠ **Kein Seed in irgendeinem Dokument.** Nie, auch nicht teilweise, auch nicht „nur die ersten vier Wörter". Der Nachlassplaner fragt nicht danach – wer ihn irgendwo dazuschreibt, hebelt das ganze Konzept aus. **Standorte, Beutel-Nummern, Zugangswege nur von Hand**, nach dem Drucken, mit dokumentenechtem Stift. Der Generator kennt diese Angaben nie.

⚠ **Der Descriptor stiehlt nichts, aber er verrät alles.** Er enthält alle xpubs: Wer ihn hat, kann nicht ausgeben, sieht aber jede Adresse, den ganzen Bestand und jeden künftigen Eingang. Deshalb steht er **nicht** auf dem Bogen: Der Ausdruck deines Koordinators (Sparrow: „Save PDF" mit QR + Text) liegt bei **jedem** Cosigner-Backup. Blatt B beschreibt nur die Struktur.

VORBEREITUNG

- ☐ **Tool offline öffnen:** Netz getrennt, Browser ohne Erweiterungen (Vault-Benutzer oder Tails). Vorher Hash prüfen: `sha256sum nachlassplaner.html` gegen den Wert auf der Download-Seite. Das Tool sendet und speichert nichts – Neuladen löscht alles.
- ☐ Bereitlegen: Gerätemodelle, **Master-Fingerprints** aller Cosigner (vom Multisig-Blatt), **Koordinator**-Name (das Programm, das die Wallet verwaltet und selbst keinen Schlüssel hat, z. B. Sparrow), **Derivation** (der Ableitungspfad, den der Koordinator beim Cosigner anzeigt, z. B. `m/48'/0'/0'/2'`) und Adresstyp. **Nicht** bereitlegen: Descriptor, Seeds, Passphrase, Standorte.
- ☐ Drucker A4. Browser-Druckdialog: **Hintergrundgrafiken AN, Kopf- und Fußzeilen AUS**. Bleistift für den Probelauf, **dokumentenechter Stift** (ISO 12757-2 / ISO 14145-2, Aufdruck „dokumentenecht") für die gültige Fassung. Fassung Nr. _____ Datum _____

A · BÖGEN AUSFÜLLEN – NUR ÖFFENTLICHE ANGABEN TIPPEN

1. ☐ **Blatt A – Existenzhinweis (darf offen liegen):** nur, **dass** es Bitcoin gibt und **wo** Blatt B liegt (Verweis von Hand). Keine Beträge, keine Geräte, keine Orte. Das ist das Blatt für Testament, Anwalt oder die Schublade, die jeder findet.
2. ☐ **Blatt B – „Bevor du handelst":** einmal lesen, als wärst du der Erbe. Die Regeln (erste Wochen nichts tun, Recovery-Dienste sind Betrug, Seed nie in eine Webseite tippen, keinem „Helfer" die Wörter zeigen) stehen **vor** allen Zugangsangaben – so bleibt es.
3. ☐ **Blatt B – Wallet-Inventar (je Wallet ein Bogen):** Bezeichnung neutral, Typ (z. B. 2-of-3 Multisig), Hardware-Modelle, Fingerprints, Derivation `m/48'/0'/0'/2'`, Adresstyp Native SegWit, Passphrase ja/nein. **Descriptor-Feld leer lassen** (siehe Warnung), stattdessen von Hand: „Descriptor-Ausdruck liegt bei jedem Cosigner-Backup". Handzeilen „Welcher Cosigner liegt wo" erst nach dem Druck.
4. ☐ **Blatt B – Physische Standorte (je Standort ein Block):** komplett handschriftlich. Ort, Zugangsweg (Schlüssel, Tresorcode-Verwahrung, Schließfachvollmacht), Behälter und **Siegel-/Beutel-Nummer**. Bei 2-von-3: drei Blöcke, ein Ort darf nie zwei Schlüssel beherbergen.
5. ☐ **Blatt B – Software und Reihenfolge:** Koordinator (z. B. Sparrow Wallet), Weg zum reinen Kontostand (Descriptor-Ausdruck scannen → Watch-only, nichts kann passieren), dann die Schrittfolge **jargonfrei**: Der Leser kennt Bitcoin nicht. Wer helfen darf und wer nicht. Übrige Bögen (Zeitkritisches, Depots, Edelmetalle, Steuer) nur, soweit sie dich betreffen.
6. ☐ **Blatt P – Protokoll:** Fassungsnummer, „Ersetzt Fassung vom", Datum. Trockenübung und Vernichtungsvermerk kommen in Teil C.

B · PRÜFEN, SICHERN, DRUCKEN

7. ☐ **Drucken auslösen → Vollständigkeits-Check.** Fehlende Fingerprints oder Fassung: nachtragen. Meldung „Multisig ohne Output-Descriptor": **gewollt**, wenn der Ausdruck bei den Backups liegt (Schritt 3) – trotzdem prüfen, dass er wirklich dort liegt, bevor du weitermachst.
8. ☐ **Verschlüsselt exportieren** (Passwort aus dem Passwortmanager, Datei auf den verschlüsselten Stick, nie in eine Cloud). Dann **Laden testen**: Tool neu laden, Datei importieren, getippte Felder wieder da. Handschriftfelder bleiben leer – so gewollt, sie existieren im Tool nie.
9. ☐ **Drucken.** Kontrolle auf Papier: Klassenband auf jedem Blatt, Fassungsnummer, Handschriftlinien vorhanden, nichts abgeschnitten. Seiten: _____ Probelauf mit Bleistift ☐ gültige Fassung mit dokumentenechtem Stift ☐

C · TROCKENÜBUNG – UNGETESTETE PLÄNE FUNKTIONIEREN NICHT

Gemeint ist nicht die Wiederherstellung, sondern der Erben-Weg: Trägt dein Papier jemanden bis zur sichtbaren Wallet – ohne Seed, ohne Gerät, ohne dass ein Satoshi bewegt wird? Wenn möglich mit der Person üben, die es einmal brauchen wird.

10. ☐ **Watch-only aus dem Papier:** Koordinator (offline reicht) → neue Wallet → Import „Output Descriptor" → Descriptor-Ausdruck per **Webcam** scannen → Fingerprints und erste Empfangsadresse mit der echten Wallet vergleichen. **Nie mit dem Handy scannen** (Kamera-Apps mit Bilderkennung, QR-Verlauf, Cloud-Foto-Backup tragen den Descriptor aus dem Haus), nie fotografieren.
11. ☐ **Erben-Perspektive:** Blatt B „Software und Reihenfolge" der Person zeigen, die es einmal brauchen wird – ersatzweise einer unbeteiligten (ohne die Standort-Blätter): Versteht sie, was Schritt 1 wäre und wen sie fragen darf? Jeden Fachbegriff, an dem sie hängt, umschreiben. Alternativ laut vorlesen.
12. ☐ **Zwei Informationsstufen prüfen:** Wissen die Erben zu Lebzeiten, **dass** es Bitcoin gibt und **wo** Blatt A liegt – und nicht, wie viel und wo die Schlüssel sind? Wenn Blatt A allein mehr verrät, kürzen.
13. ☐ **Abschluss:** Trockenübung auf Blatt P eintragen (Datum, wer, Ergebnis). Probe-Wallet im Koordinator schließen und löschen (kein Gerät zurücksetzen). Probelauf-Ausdrucke und alte Fassungen **schreddern**, Vernichtungsvermerk auf Blatt P. Gültige Fassung verteilen: Blatt A zum Testament-Ort, Blatt B zu den Backups.

ZEIT & TERMINE

Ausfüllen (A): _____
Druck + Export (B): _____
Trockenübung (C): _____
Nächste Fassung fällig: _____

WAS FEHLTE, WAS UNKLAR WAR, WAS DER ERBE NICHT VERSTAND

_____
_____
_____

ERGEBNIS

- ☐ **Bestanden:** Der Descriptor-Ausdruck allein stellt die Sicht auf die Wallet her, ein Unbeteiligter versteht Blatt B, Blatt A verrät nichts, Blatt P trägt Fassung und Trockenübung. Wiederholen bei jeder Änderung am Setup und mindestens **einmal im Jahr** (Auffrisch-Routine, Kap. 12).
- ☐ **Abweichung:** Scan liefert andere Fingerprints oder Adressen → falscher oder alter Ausdruck bei den Backups, sofort ersetzen. Erbe versteht Blatt B nicht → Schrittfolge umschreiben, neue Fassung, alte vernichten. **Ein PDF ist kein Testament** (§ 2247 BGB, eigenhändig) – das Paket ergänzt es, ersetzt es nicht.