Building the heir package with the Estate Planner

Form generator (one HTML file, offline) · class A proof of existence · class B access instructions · class P record · Self-Experiment 7 · belongs to chapter 9/12

⚠ **No seed in any document.** Never, not even partly, not even "just the first four words". The Estate Planner does not ask for it, and anyone who writes it in somewhere defeats the whole idea. **Locations, bag numbers and access routes by hand only**, after printing, with a document-proof pen. The generator never learns these entries.

⚠ **The descriptor steals nothing, but it reveals everything.** It contains every xpub: whoever holds it cannot spend, but sees every address, the entire balance and every future incoming payment. That is why it is **not** on the sheet. The printout from your coordinator (Sparrow: "Save PDF" with QR code and text) lies with **every** cosigner backup. Sheet B describes the structure only.

PREPARATION

- ☐ **Open the tool offline:** network disconnected, browser without extensions (separate user account or Tails). Check the hash first: `sha256sum nachlassplaner.html` against the value on the download page. The tool sends and stores nothing, and reloading clears everything.
- ☐ Have ready: device models, **master fingerprints** of every cosigner (from the multisig sheet), **coordinator** name (the program that manages the wallet and holds no key of its own, for example Sparrow), **derivation path** (the path the coordinator shows at the cosigner, for example `m/48'/0'/0'/2'`) and address type. **Do not** have ready: descriptor, seeds, passphrase, locations.
- ☐ A4 printer. Browser print dialog: **background graphics ON, headers and footers OFF**. Pencil for the trial run, **document-proof pen** (ISO 12757-2 / ISO 14145-2, marked "document proof", in Germany "dokumentenecht") for the valid version. Version no. _____ Date _____

A · FILL IN THE SHEETS — TYPE PUBLIC ENTRIES ONLY

1. ☐ **Sheet A — proof of existence (may lie in the open):** only **that** there is Bitcoin and **where** sheet B is kept (pointer by hand). No amounts, no devices, no locations. This is the sheet for the will, the lawyer or the drawer that everyone finds.
2. ☐ **Sheet B — "Before you act":** read it once as if you were the heir. The rules (do nothing in the first weeks, recovery services are fraud, never type a seed into a website, show the words to no "helper") stand **before** all access entries, and that is where they stay.
3. ☐ **Sheet B — wallet inventory (one sheet per wallet):** neutral name, type (2-of-3 multisig, for example), hardware models, fingerprints, derivation path `m/48'/0'/0'/2'`, address type Native SegWit, passphrase yes/no. **Leave the descriptor field empty** (see warning), instead by hand: "the descriptor printout lies with every cosigner backup". The handwritten lines "which key lies where" only after printing.
4. ☐ **Sheet B — physical locations (one block per location):** handwritten throughout. Location, how to get in (keys, where the safe code is kept, power of attorney for a safe deposit box), container and **seal or bag number**. With 2-of-3: three blocks, and one location must never hold two keys.
5. ☐ **Sheet B — software and order of work:** coordinator (Sparrow Wallet, for example), the way to the plain balance (scan the descriptor printout → watch-only, nothing can happen), then the steps **free of jargon**: the reader does not know Bitcoin. Who may help and who may not. The remaining sheets (time-critical matters, brokerage accounts, precious metals, tax) only as far as they concern you.
6. ☐ **Sheet P — record:** version number, "replaces the version of", date. Dry run and record of destruction come in part C.

B · CHECK, SAVE, PRINT

7. ☐ **Start printing → completeness check.** Missing fingerprints or version: add them. The message "multisig without output descriptor" is **intended** when the printout lies with the backups (step 3). Check that it really does lie there before you carry on.
8. ☐ **Export encrypted** (password from the password manager, file onto the encrypted stick, never into a cloud). Then **test the loading**: reload the tool, import the file, and the typed fields are back. Handwritten fields stay empty, as intended, because they never exist in the tool.
9. ☐ **Print.** Check on paper: class band on every sheet, version number, handwriting lines present, nothing cut off. Pages: _____ trial run with pencil ☐ valid version with document-proof pen ☐

C · DRY RUN — UNTESTED PLANS DO NOT WORK

This is not about the restore, it is about the path of the heir: does your paper carry someone as far as the visible wallet, without a seed, without a device, without a single satoshi moving? Practise with the person who will one day need it, if you can.

10. ☐ **Watch-only from the paper:** coordinator (offline is enough) → new wallet → import "Output Descriptor" → scan the descriptor printout with a **webcam** → compare fingerprints and the first receiving address with the real wallet. **Never scan with a phone** (camera apps with image recognition, QR history and cloud photo backup carry the descriptor out of the house), never photograph it.
11. ☐ **The view of the heir:** show sheet B "software and order of work" to the person who will one day need it, or failing that to an uninvolved person (without the location sheets). Do they understand what step 1 would be and whom they may ask? Rewrite every technical term they stumble over. Reading it out loud works too.
12. ☐ **Check the two levels of information:** do the heirs know during your lifetime **that** there is Bitcoin and **where** sheet A is kept, and not how much and where the keys are? If sheet A alone reveals more, cut it down.
13. ☐ **Closing:** enter the dry run on sheet P (date, who, result). Close the test wallet in the coordinator and delete it (do not reset any device). **Shred** the trial printouts and older versions, and note the destruction on sheet P. Distribute the valid version: sheet A to the place of the will, sheet B to the backups.

TIME & DATES

Filling in (A): _____
Print + export (B): _____
Dry run (C): _____
Next version due: _____

WHAT WAS MISSING, WHAT WAS UNCLEAR, WHAT THE HEIR DID NOT UNDERSTAND

_____
_____
_____

RESULT

- ☐ **Passed:** the descriptor printout alone establishes the view of the wallet, an uninvolved person understands sheet B, sheet A reveals nothing, sheet P carries version and dry run. Repeat after every change to the setup and at least **once a year** (refresh routine, chapter 12).
- ☐ **Deviation:** the scan yields different fingerprints or addresses → the wrong or an outdated printout lies with the backups, replace it at once. The heir does not understand sheet B → rewrite the steps, new version, destroy the old one. **A PDF is not a will**: German inheritance law requires it in your own handwriting (§ 2247 of the German Civil Code, Bürgerliches Gesetzbuch, BGB), so check the law of your own jurisdiction. The package supplements a will, it does not replace it.