

ZNTRPHY

User Manual: air-gapped Bitcoin key generator

ZNTRPHY

User Manual — air-gapped Bitcoin key generator

Thank you for trusting ZNTRPHY to generate your Bitcoin keys. This manual will guide you step by step. Read it in full before generating keys that will hold real funds — some steps only give you one chance to get them right.

1. What ZNTRPHY is, and why "air-gapped" matters

ZNTRPHY generates Bitcoin seeds (12-to-24-word phrases), optional passphrases, and single-sig or multisig wallet setups — all **without ever connecting to the internet**.

"Air-gapped" means the machine where you generate your keys never touches a network. This matters because:

- A Bitcoin private key that never existed on an internet-connected machine can't be stolen by malware intercepting network traffic, nor leaked by a malicious app "phoning home".
- Most self-custody fund thefts don't happen by breaking Bitcoin's cryptography (that's practically impossible with the right parameters) — they happen because the private key passed, at some point, through an internet-connected machine, or was typed into a fake site.

Strong recommendation: generate your keys on a dedicated machine, booted from a "live" operating system (for example, Tails or Ubuntu running from a USB stick, without installing anything to disk) that never connects to the internet. If that's not possible, at minimum unplug the network cable and turn off wifi before opening the app.

2. Before you start: verify the file is genuine

Scammers sometimes distribute modified copies of Bitcoin wallets with backdoors. Before running ZNTRPHY for the first time:

- 1 **Verify the file's SHA-256 hash** against the one listed in `packaging/SHA256SUMS.txt` (or the one shared with you by whoever sold you the product, through a channel different from the file download itself). On macOS/Linux: `shasum -a 256 ZNTRPHY` (or `sha256sum` on Linux). On Windows (PowerShell): `Get-FileHash ZNTRPHY.exe -Algorithm SHA256`.
- 2 If the hash doesn't match exactly, **don't use it** — it may have been modified. Contact whoever sold it to you through a different channel to confirm.
- 3 Be wary of copies found through search engines, forums, or unofficial links — always use the original download channel.

The complete source code is included alongside this manual precisely so that you, or anyone you trust who can read code, can review exactly what the program does before trusting it with real funds.

See SECURITY.md for detailed instructions on how to verify, among other things, that the app never connects to the internet.

3. Generating a single-sig wallet (one key)

This is the simplest path: a single seed controls the funds.

- 1 Open the app and choose **"Single-sig wallet"**.
- 2 **Additional entropy (optional)**. The app already uses the operating system's secure random number generator — that alone is enough. If you'd also like to contribute dice rolls or mouse movement, you can do so here: it's combined so that it **can only add security, never remove it**. Also choose how many words you want (24 is the most secure; 12 is the BIP39 standard's minimum).
- 3 **Your seed phrase**. The app shows you the numbered words. **Write them down by hand, on paper (or metal), in the exact order**. Never type them into a computer, never photograph them, never upload them to any cloud service, never send them to anyone through any digital channel. Whoever has these words controls the funds, no exceptions — not even you can recover access if you lose them.
- 4 **Optional passphrase ("25th word")**. This is an extra layer of protection: even if someone finds your written-down words, they can't access the funds without this passphrase. It's completely optional, but if you enable it, write it down **in a different place** from where you wrote the words — and keep in mind that if you forget it, the funds are lost forever. There's no way to recover it: not the app, not us, not anyone.
- 5 **Summary**. You'll see your key's fingerprint, the account xpub, the receive and change descriptors, and a couple of example addresses. **Import the receive descriptor into your wallet** (Sparrow, Electrum, or whichever you use) and confirm that the addresses it generates match the ones ZNTRPHY shows you, before receiving real funds.

4. Generating a multisig wallet (multiple keys)

A multisig needs m of n signatures to spend funds (for example, "2 of 3"). There are two ways to build one:

Coordinator mode (recommended)

Each time you run the app in this mode, it generates **a single cosigner**. To build the final multisig, you gather the **public** information (never the seed) of each cosigner.

- 1 Choose **"Multisig wallet"** → **"Generate a cosigner now"**.
- 2 Follow the same steps as single-sig (entropy, seed, passphrase) — this seed belongs to **THIS** cosigner only.

- 3 The app shows you a text block with this cosigner's fingerprint, xpub, and derivation path — **this is the only thing you need to share** with whoever is going to assemble the multisig. Copy it or save it to a text file.
- 4 Repeat this process once per cosigner you need (in separate runs, and if possible, on separate machines for each person/device).
- 5 On the **"Assemble multisig"** screen, paste in the public information for each cosigner, choose how many signatures are required (m), and the app builds the final `wsh(sortedmulti(...))` descriptor.

With this mode, **no single run of the app ever sees more than one seed** — this is the safest way if the cosigners are different people or devices.

Convenience mode

Generates **all** the seeds at once, in the same run. Only useful if a single person controls every device/cosigner (for example, your own three computers or hardware wallets). **Don't use this** if the cosigners are different people who shouldn't share the same machine — in that case, a compromised machine would see every seed it generated, even if only transiently.

5. Completing a seed you generated by hand

If you already generated your own words on your own (for example, by rolling physical dice and using your own conversion table) and you're missing the last word, the **"Complete seed"** screen (available from the home screen) calculates it for you.

How it works: in a BIP39 seed, the last word isn't fully free — part of its bits are a mathematical checksum that depends on every earlier word. Given the first N-1 words (for example, 23 of 24), only a handful of final words produce a valid checksum (8 in the 24-word case). The app computes those options and lets you pick one (or pick one at random, using the same secure generator the rest of the app uses).

Important: this does not recover a lost or someone else's seed. It only works if you already have your own N-1 words, real and in the correct order. It doesn't generate any new entropy on its own, and it's not useful for guessing a seed that isn't yours.

Once you've chosen the final word, you can continue the same flow as if you'd generated it normally: as a single-sig wallet, or as one cosigner of a multisig.

6. Verifying your backup

Before trusting any wallet generated here with real funds:

- 1 Write down the words exactly as shown, in the order shown.
- 2 Read them back aloud, comparing against what you wrote, word by word.
- 3 Import the descriptor (single-sig or multisig) into a reputable wallet (Sparrow Wallet, Electrum) and confirm that the generated addresses match the ones ZNTRPHY shows.

- 4 Consider testing first with a small amount before moving large funds, especially the first time you use a multisig.

ZNTRPHY Verify (the companion web/mobile app) can do this same check from your phone: paste the public descriptor (never the seed) and confirm the addresses match, without installing a full wallet. Just like the desktop app, it never asks for or handles seeds.

7. Exporting, encrypted with a PIN

From the summary screen you can export the information to a file, protected with a PIN you choose (encrypted with Argon2id + AES-256-GCM).

- The PIN **doesn't replace** writing down the seed by hand — it's an additional layer for anyone who also wants an encrypted digital backup.
- Store the PIN somewhere **different** from where you store the exported file.
- If you lose the PIN, the file is useless — not even the app can help you recover it.
- Nothing is written to disk until you reach this screen and explicitly confirm the export.

8. Phishing and fake-copy warnings

- Always verify the file's hash (section 2) before using it.
- ZNTRPHY will **never** ask for your seed, your passphrase, or your PIN through any channel (email, chat, social media, web form). If someone asks for it while claiming to be the seller or support, it's a scam attempt.
- This app has no "cloud recovery" or "sync" feature of any kind — any offer of that sort related to the product is fake.
- Always download from the official channel indicated by whoever sold you the product, never from a search-engine link or a third party.

9. Frequently asked questions

Can I use ZNTRPHY on a machine with internet access? Technically yes, the app works the same — but for maximum security, the recommendation is to always generate keys on a machine disconnected from the network.

What happens if I lose my seed words? You lose access to the funds forever. There's no way to recover them — not ZNTRPHY, not us, not anyone.

Can I add more cosigners to a multisig after creating it? No — the number of cosigners (n) and the threshold (m) of a multisig are fixed when it's created. Changing them requires creating a new multisig and moving the funds.

Does this app store anything on the internet or in the cloud? No, never. See SECURITY.md for how to verify this yourself.

This manual and the accompanying software are provided with no warranties beyond what the law requires. Safeguarding your seed words, your passphrase, and your PIN is exclusively your responsibility.

ZNTRPHY is an original idea by the fnalysis.com team. © fnalysis.com. All rights reserved.