These are the words used in this guide, and what they mean.

entropy

Entropy is the randomness that is made with the dice, and it is the material the 24 words are built from.

airgap / Tails, networking off

It is critical that each key is made on a computer that is offline. Tails OS is installed on one of the two USB drives. It can be booted on any computer, and it is designed to forget the session when the machine shuts down. When Tails is booted, networking is set to Disabled.

2-of-3 native SegWit (P2WSH)

This is a wallet that needs any two of three keys before it can spend. One key by itself cannot move the long-term fund.

m/48'/0'/0'/2'

This is the path Sparrow fills in for this kind of wallet. It is confirmed on the screen, and it is not typed from memory.

PSBT

A PSBT is an unsigned payment file that is carried on the USB drive. The seed stays on the offline computer.

descriptor / xpub

The descriptor is the wallet map, and an xpub is a public watch key. Either one can watch the money, and neither one can spend it.

BIP39

BIP39 is the standard list of 2,048 words that a seed is written in. This process uses 24 of those words.

hash

These files are downloaded from their original sources. The fingerprint on that source has to match the fingerprint the computer prints for the saved file. If the lines do not match, the file is deleted.

signature

A signature is the project confirming the file. If the signature fails, the file is deleted and downloaded again.

zero-trust

Zero-trust means a company’s word is not accepted for a download or for a key. Two tools have to agree.