

Do these sheets in order

This packet is the work, from the closed door to the three houses. Read a sheet, do it, then go to the next. If a check fails, stop. Do not pick the result you like better.

- 03 Gather what the list names. Tick it.
- 04 One computer. Two boots. Label the USBs.
- 05 Check the files before anything is copied.
- 06 Roll the dice. Three lists of 24 words.
- 07 Build the 2-of-3 in Sparrow. One seed per boot.
- 08 Practice spend. Dust in. Two signatures. Dust out.
- 09 Stamp the plates. Read them back. Split them.
- 11 Hide the wallet map. It is not a seed.
- 12 Leave the letter. Two plates, not one.

Sparrow for Tails is version 2.5.5, file sparrowwallet-2.5.5-x86_64.tar.gz. The Windows or Mac installer does not go on the USB. A newer download that does not match is a stop, not an upgrade.

Before the first roll

- A room you can close. Phones and cameras out while words or plates are visible.
- Five casino dice you can read. A pen. Extra copies of the recording grid.
- One computer. Two USB sticks. Label one TAILS and one DATA.
- Tails 7.13, Sparrow 2.5.5 Linux file, Electrum 4.8.2, the Ian Coleman page. Each one checked.
- Three 24-word titanium plates. One method per plate. Do not mix stamp letters and number punches.

Then, in this order

- Boot 1 watches. It never holds a seed. Boot 2 is Tails, networking off.
- Seed 1 from dice. Two tools print the same 24 words. Shutdown.
- Seed 2, new rolls, same checks. Shutdown. Seed 3, new rolls, same checks. Shutdown.
- Build the 2-of-3 from the three public keys. No seed is typed in that boot.
- Import the map on the watching computer. Receive dust. Spend dust with two keys.
- Stamp, read back, restore from the plate, then destroy the paper.
- Three plates, three places. Two keys in one house is one point of failure.

Hardware signers are optional later, and only from more than one maker. A signer does not create the key.

You are here after the files pass

One computer. Boot 1 is the system you already use. It may be on the network. It watches. It never holds a seed. Shut it down fully before Boot 2.

Boot 2 is the Tails USB in that same computer. On the welcome screen, set Networking to Disabled before the desktop appears. Do not create Persistent Storage. Do not unlock it if the stick already has it.

What crosses on the DATA stick

- Checked files, the three public keys, the wallet map, and payment files.
- Never a photo of the words. Never two seeds in one boot.
- Copy the result back to the stick. Shut down. Wait until the screen is dark before you unplug.

Every offline session

1. Insert Tails. Boot. Networking Disabled. Start Tails.
2. Plug in DATA. Copy only the files this session needs.
3. Do one job: convert one list, load one seed, or sign one payment file.
4. Copy the result back. Shut down fully.

You are here before anything is copied

A hash is the file's fingerprint. A signature is the project saying that fingerprint is theirs. If either fails, delete the file. A bad file means the funds are bad.

The files

- Tails 7.13. tails-amd64-7.13.img or tails-amd64-7.13.iso. From tails.net. Wait until that page says the check passed.
- Sparrow 2.5.5. sparrowwallet-2.5.5-x86_64.tar.gz. That is the Linux file. Not the Windows installer. Not the Mac installer.
- Electrum 4.8.2. electrum-4.8.2-x86_64.AppImage. From electrum.org.
- Ian Coleman. bip39-standalone.html from the official GitHub. Open it only while offline.
- The dice converter is in this kit. Its fingerprint is in VERIFY.md.

Compare the fingerprint

Windows: Start menu, PowerShell. Type cd, a space, drag the folder in, press Enter. Then:

```
Get-FileHash .filename -Algorithm SHA256
```

Mac: Spotlight, Terminal. Same cd step. Then:

```
shasum -a 256 filename
```

The long line must match the site, every character. Then run verify_kit.sh in that folder. It checks fingerprints. It does not check signatures. One failure means stop.

You are here on Tails, networking off

Five casino dice. Read left to right every time.

- 1 is 00. 2 is 01. 3 is 10. 4 is 11.
- 5 and 6 are not bits. Roll those dice again.
- Example: 4, 6, 1, 3, 2 becomes 11, skip, 00, 10, 01.
- Write only 0 and 1. At least 256 bits. Extra bits are folded down.

Three keys, three boots

1. Run the checked converter. Paste the bits. It prints 24 words. Word 24 is the check. Do not invent it.
2. Open the Ian Coleman page offline. Entropy type Binary. 24 words. Same bits. The words must match. If they differ, stop.
3. Write the words. Read them back once. Shut down. Wait for a dark screen.
4. Seed 2 is a new set of rolls. Seed 3 is a new set of rolls. Never continue a list from the previous boot.

On the Desktop: `python3 bip39_dice_converter.py`

Dice recording sheet

Read left to right. Write only 00 / 01 / 10 / 11. Leave a cell blank if that die was 5 or 6. Print extra copies — each seed needs ~50–60 shakes.

Seed # 1 2 3			Date _____		Reader _____		Checker _____	
#	Die 1	Die 2	Die 3	Die 4	Die 5	Bits this shake		
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								

Running bit count (filled pairs × 2): _____ Target ≥ 256, better 320–400. Do not photograph this sheet. Destroy it after the 24 words are stamped and verified.

Launch, one seed per boot

The file is sparrowwallet-2.5.5-x86_64.tar.gz. Copy it to the Desktop. Applications menu, Terminal. Type these lines, Enter after each:

```
cd ~/Desktop
```

```
tar -xvf sparrowwallet-2.5.5-x86_64.tar.gz
```

```
cd Sparrow
```

```
./bin/Sparrow
```

Load Seed 1 only. The path must read m/48'/0'/0'/2'. Confirm it. Do not type a different path. Copy that key's public key to the DATA stick. Shut down. Repeat for Seed 2. Then Seed 3.

Build the 2-of-3 with no seed loaded

1. Fresh boot. Networking off. Do not type a seed.
2. File, New Wallet. Multi-signature. Native Segwit. 2 of 3.
3. Import the three public keys. Confirm the path still reads m/48'/0'/0'/2'.
4. Export the output descriptor. That is the map. It watches. It cannot spend. Shut down.
5. On the everyday computer, import the map as watch-only. That computer never holds a seed.
6. On a later offline boot, open the same map in Electrum with one seed. The first addresses must match. If they differ, stop.

Dust only, until this has worked once**1. Online, watch-only**

- Open the watching Sparrow. Confirm the receive history is this wallet.
- Write the destination, amount, and fee on paper. Read the screen against the paper.
- Export tx-unsigned.psbt to the DATA stick.

2. First signature

- Tails, networking off. Seed 1 only. Open the payment file. Confirm the fields. Sign.
- Export tx-partial-s1.psbt. Shut down. Wait for a dark screen.

3. Second signature

- Fresh boot. Seed 2 only. Open the partial file. Confirm the first signature and the unchanged spend. Sign.
- Export tx-signed.psbt. Shut down.

4. Broadcast

- Watching Sparrow. Open the signed file. Confirm it is fully signed and the fields did not change. Broadcast.
- Write the transaction id in the recovery log. Not on this site. Not in a photo.

If Sparrow and Electrum disagree about the payment, stop. Do not sign. Savings move only after dust has gone in and dust has come out.

Stamp only after the practice spend

1. Closed room. No phones. Stamp words 1 through 24. A quiet label such as S1. Not your name. Not the word Bitcoin.
2. Read the plate back against the paper. A wrong letter is a dead backup.
3. Restore from the plate on Tails, networking off. The first addresses must match. Then destroy the paper and the bit notes.

The plate that stays home

The 24 words alone open a small wallet. Leave a little bitcoin there. The same words plus a passphrase open a different wallet for modest spending. Do not stamp the passphrase. Do not keep it in the same drawer. Do not put a passphrase on the 2-of-3. The fund still needs any two plates.

Three places

Plate A, Seed 1, home. Plate B, Seed 2, a second address. Plate C, Seed 3, a third address. Two keys in one house and the lock is gone. The map may sit with one plate. Never with all three.

After the descriptor exists

The map watches the money. It is not a seed. Plain text still shows the balance. On Tails, networking off:

1. Save the descriptor as map.txt. Do not write the public keys on paper.
2. Run: `gpg --symmetric map.txt`
3. Use a long passphrase. It is not on the plates. Write it on separate paper, away from the plates.
4. Keep map.txt.gpg. Delete map.txt. Store the encrypted file on two sticks.
5. Decrypt it once later and confirm it opens. If this passphrase is lost, the coins are not gone. Two plates can rebuild the map. The path is `m/48'/0'/0'/2'`. That path is not a secret.

Read this before you touch a plate

- Do not type the words into a phone, a website, or a photo.
- One plate cannot spend the fund. You need two plates, from two places.
- Find the map. If it asks for a passphrase, that paper is stored away from the plates.
- Buy a Jade from Blockstream's own shop. Buy a BitBox from BitBox's own shop.
- Put one plate into each device. Never put both plates in one device.
- Load the map. Send a small test first.
- The fund is 2 of 3. The path is m/48'/0'/0'/2'. That line is not a secret.