Guide 2: Regenerating the Wallet Descriptor from the Public Keys (Part 1)

WARNING:

There is a copy of the Wallet Descriptor in each Recovery Package, in the ORANGE envelope. It allows you to easily regenerate the Vault in any Wallet Management Interface (see Guide 1.)

If the Recovery Packages were correctly secured and protected, you shouldn’t have to follow this guide.

In the event that you don’t have access to the Wallet Descriptor anymore, you’ll have to regenerate it from the 5 Public Keys.

Reminder: Each Public Key is derived from its corresponding Signing Key. Each Signing Key is the combination of Seed and Passphrase.

Necessary items:

- Wallet management interface
- Internet-connected device (phone or computer)
- 5 Seeds
- Passphrase
- Offline signing device

The wallet management interface app can be downloaded on your computer or your phone. I suggest you use:

- On computer: Sparrow Wallet
- On phone: Blue Wallet

The offline signing device can be purchased on the internet, assembled or non-assembled. In these instructions we’ll use SeedSigner.

These apps and tools might be obsolete by the time you read these instructions. Regardless of the tools you choose to use, the process remains the same.

Whichever device and application you decide to use, be sure to get informed and train before you proceed with the Vault.

Guide 2: Regenerating the Wallet Descriptor from the Public Keys (Part 2)

Procedure:

1. Create a new multisignature 3-of-5 wallet in the wallet management interface
2. Load Seed 1 onto the signing device and verify the Fingerprint without Passphrase
3. Load the Passphrase onto the device and verify the Fingerprint with Passphrase
4. On the signing device, export Public Key 1, derived from Signing Key 1
5. Scan Public Key 1’s QR code with the wallet management interface
6. Repeat the operation for each of the 5 Public Keys, derived from each of the 5 Signing Keys
7. Create the wallet in the wallet management interface

You can use the Wallet Regeneration Flowchart as a guide.

Congratulations - you've regenerated the Wallet Descriptor from the Public Keys. You now have access to your Bitcoin vault.

Now you need to back up the Wallet Descriptor again, so you don't have to recreate the vault every time you change computers.