Bitcoin paper wallet

Bitcoin paper wallet

Bitcoin paper wallet

File Decryption Instructions

Read the QR code and save its content to a file named `secret.b64`.

Alternatively, the content is also written as text in the base64 format. Type it into a text file (`secret.b64`). Convert the base64 file into the binary file (`secret.enc`) using:

```
$ base64 -d secret.b64 > secret.enc
```

This file (`secret.enc`) was encrypted using OpenSSL with AES-256 in CBC mode, PBKDF2 for key derivation, and SHA-512 as the hashing algorithm. Its contents has the backup passphrase seed used to create my bitcoin wallet, what may be used to restore it.

Encryption Command used:

```
$ openssl enc -aes-256-cbc -md sha512 -pbkdf2 -iter 1000000 -salt -in secret.txt -out secret.enc
```

To decrypt this file, follow these steps:

- Ensure you have OpenSSL installed: You'll need OpenSSL to decrypt this file. Most Linux distributions come with it pre-installed. For macOS or Windows, you may need to download it from https://www.openssl.org/.

- Decryption Command: Run the following command, replacing secret.enc with the path to your encrypted file:

  ```
  $ openssl enc -d -aes-256-cbc -md sha512 -pbkdf2 -iter 1000000 -salt -in secret.enc -out secret.txt
  ```

- Enter the Passphrase: You'll be prompted to enter the passphrase used during encryption. Make sure to enter it exactly as set when the file was encrypted.

- Password hint: If necessary, place the password hint here for your Family. Example: "First pet name + Year we moved to our first house + Favorite shared family vacation spot + First word spoken by our firstborn + Color of the first car + Favorite desert."

U2FsdGVkX1/O9WyTC31BzN/w+I74AmfUbu90N1v8awrjYEjyfnyShcV9fIFMkA4IJHxPvlNHxtQW
LtKWnZrRpxjKMKTQoeSm+FGxe2bEG8o=

Wallet Info

- Wallet name: `mywallet`
- File created: `using 4.5.8, on 2024-11-08`
- Keystore type: `standard`
- Script type: `p2wpkh`
- Seed available: `True (segwit)`
- Keystore type: `bip32`
- Lightning: `Enabled`
- Lightning Node ID: `011ec4d6f23ca6cabae58ec23cd061a2ebbd731ee1234567890ba2abc1d456789a`
- Master Public Key: `zpub6npA1st12WxEeLmfZxB7j1AoXq7K3CyrzATSubynHSh2pXQq2QZnbZ1TuPjNnH`
- Master Public Key (cont): `51kCp414fgyo2Xo3vGo9rY67xnEUbHdD9GmMJZ3T9FQvz`
- Derivation path: `m/0h`
- BIP32 Root Fingerprint: `6eb2f3aa`