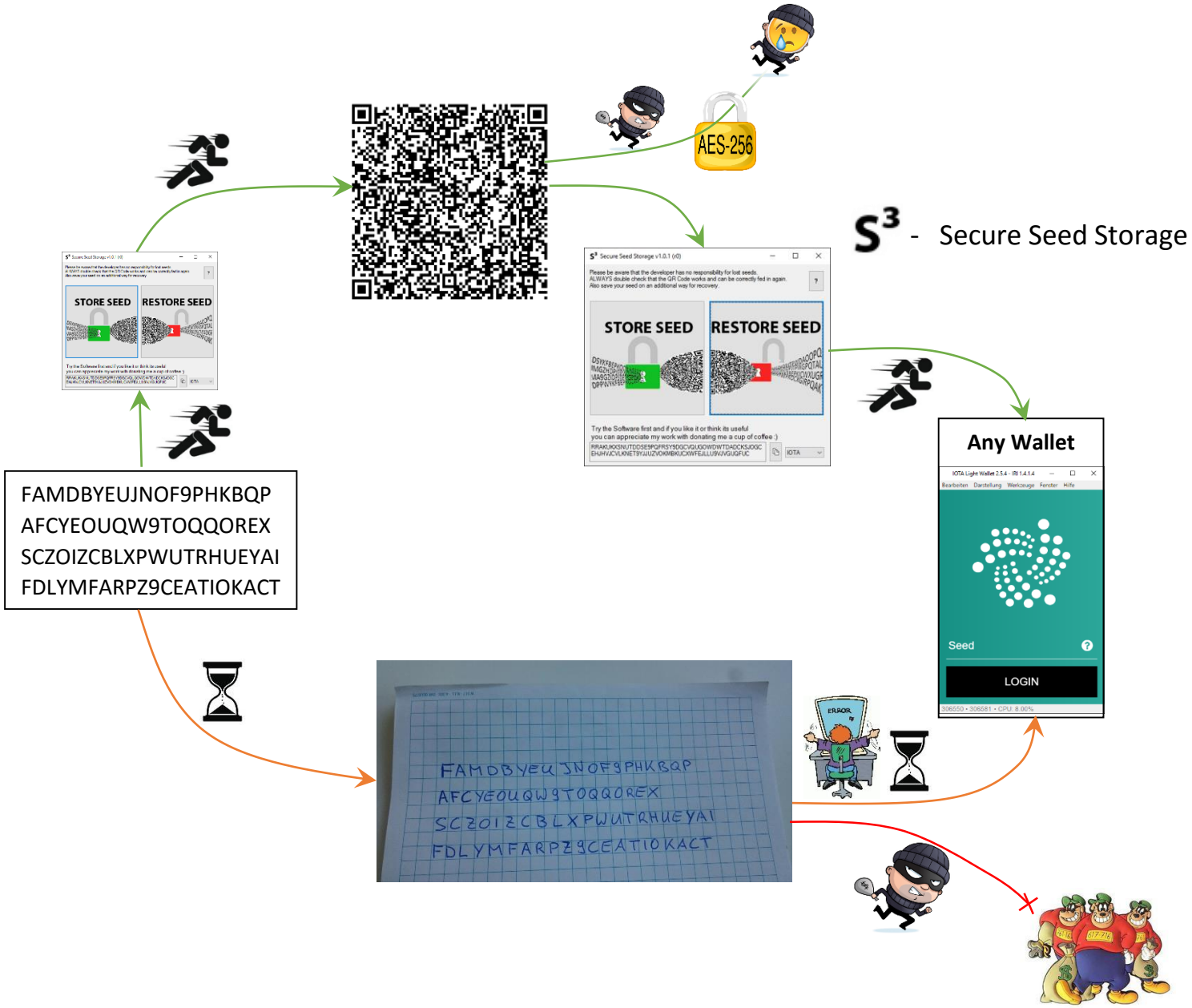

AES-256
STORE SEED
RESTORE SEED
S³ - Secure Seed Storage
Any Wallet
Seed
LOGIN
ERROR
FAMDBYEUJNOF9PHKBQP
AFCYEOUQW9TOQQOREX
SCZOIZCBLXPWUTRHUEYAI
FDLYMFARPZ9CEATIOKACT

Cryptocurrency SEED handling

The Problem

- Unhandy seeds to log into wallet
- Security concerns regarding
  - seed storage
  - copy&paste the seed to the wallet (Spyware)
  - loss of the seed
  - broken Computer
- No secure Seed-Generator for IOTA (probably in the new wallet)

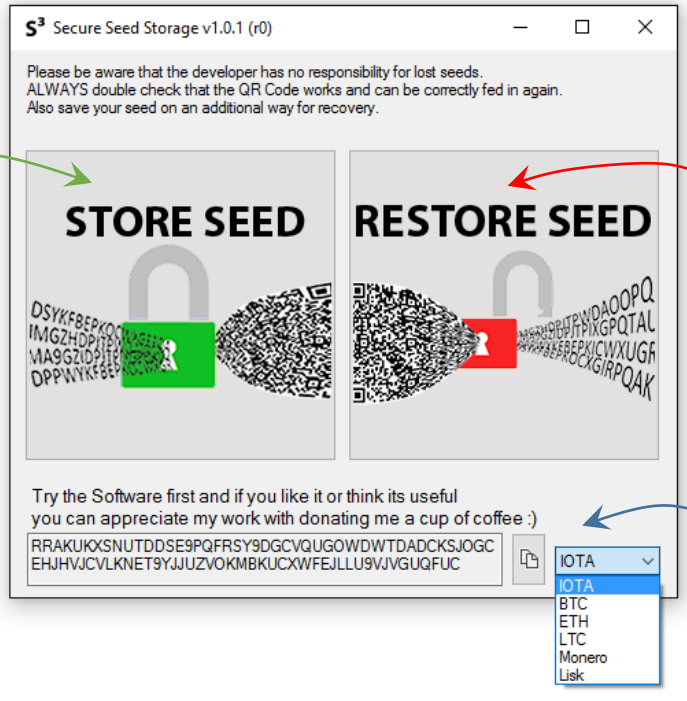
The Solution

S^3 - Secure Seed Storage

- Log into the wallet by simply holding the QR Code in front of your Camera (+optional password)
- Security concerns
  - Easily to store, e.g. within a private folder
  - The software types the seed directly to your wallet without using copy&paste
  - You can print it multiple times and store it on different places (e.g. Friends, as without password you can´t retrieve the seed)
  - You can read it on every computer using this software
    - Also I'll release a step by step guide explaining how to retrieve the seed just with online tools + your password
- Cryptographically secure random Seed-Generator

Go to 'Store Seed' and generate a new seed or convert an existing one into secure QR Code.

1.



2.

After creating a QR Code make sure several times that it is read and decrypted correctly - don´t make to small QR Codes.

After that your QR Code is ready to be used anytime ☺

3.

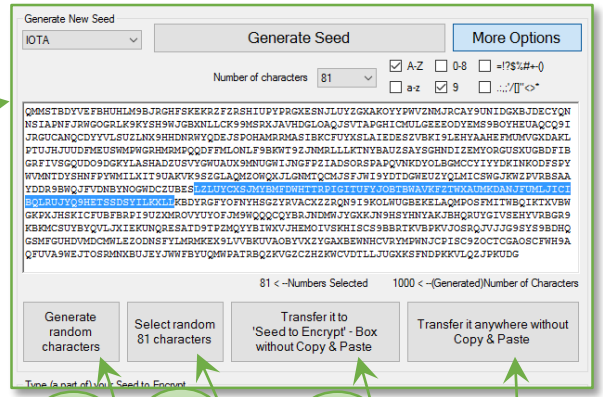
I decided to release this piece of software for free as I'd like to make your seed storage and handling a bit easier and more secure.

If you want to check out transactions on different blockchains or tangle, my receiving address is stated and ready to receive a digital cup of coffee or a beer ;-)

1. Select the character-set you want to use for seed generation.
Actually supported:
   - IOTA (A-Z, 9)
   - All Characters (A-Z, a-z, 0-9, =!?$%#+-().:,;'/[]"<>*)
   - Custom

2.a Generate a seed with chosen setting

2.b

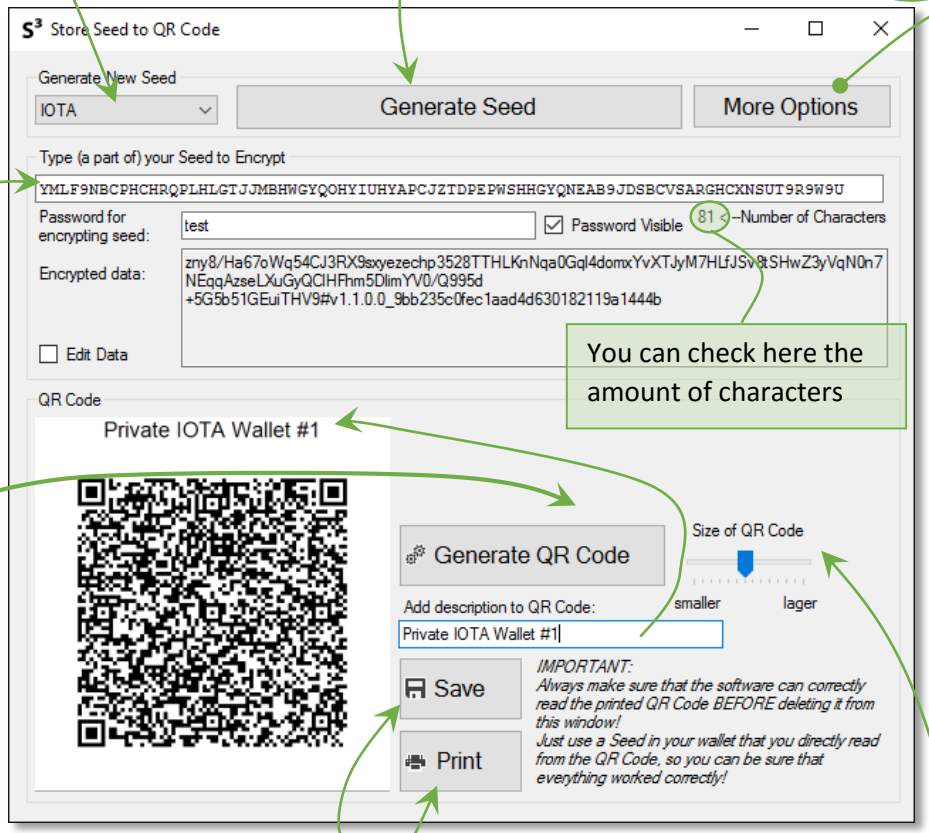


Fill the textbox with 1000 random chars from the selected charset

Highlight 81 random chars

Insert highlighted text into seed-textbox without copy&paste

You can also transfer the seed anywhere you can type a text with your keyboard.
(Further description on (5.) 'Restore Seed' Page)



3. The generated seed (step 2) appears in this field – here you can modify it as much as you want.

Or you can skip step 1 & 2 and type your own seed directly here. Then modify it as much as you want.

You can check here the amount of characters

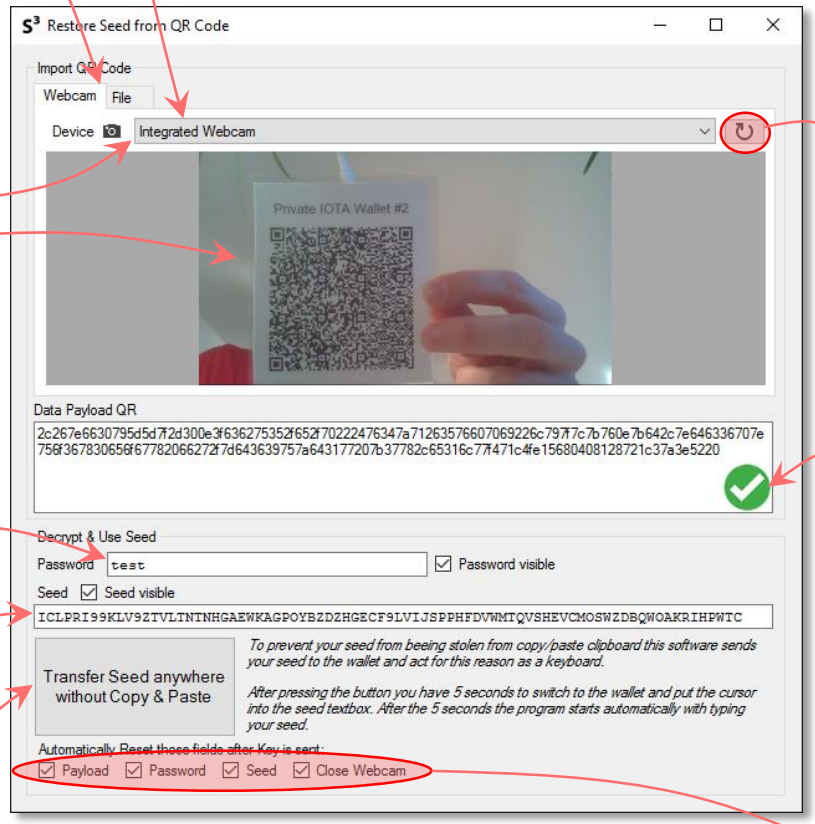
4. Finally generate a QR Code from the encrypted data above

5. Save or better **print** your seed directly.
IMPORTANT: Before closing this window, check on the 'Restore Seed'-Window if it correctly decrypts the seed

Here you can adjust the size of the QR Code produced– e.g. when the code don´t fit on the printed page. **Don´t make it too small in order to not get problems with decryption.**

RESTORE SEED

1. Select the source how you want to feed your QR Code.
Options:
- Camera Device
- File (Picture or PDF)
- Screenshot (QR opened somewhere on the screen)



Select the camera to scan the QR Code and wait until you see the preview stream

Reload the camera device list

2. Make sure that you have a green sign. That ensures that the data is complete and not corrupt

3. Type your password you have used to encrypt the data before

4. Check if you got correct seed here

5. With this button you can send the data to any text inputfield on your computer. For this the software works as kind of keyboard and just types your seed directly where you set keyboard cursor (the flashing vertical line).

After pressing the button you have 5 seconds to change window and set the cursor in the appropriate inputbox - so open your wallet before ;) – then the software starts typing the seed directly there. So you don´t have to use copy&paste.

After your seed is sent all the databoxes selected here are resetted in order to not forget to leave the visible seed here

Some additional safety hacks:

- Remove the last xx characters from the seed and note it handwritten on the backside of the printed QR
- Same as above but replace it with a word you remember
- Use a password that can**not** be guessed
- Don´t store your QR somewhere online or on your PC
- Never let a software doing something like this one connect to the internet

Easy handling laminated

Easy to arrange

THE ENCRYPTION

Your seed:

ROWUGVZRCEZEY

Your password:

test

MD5 Hash of encrypted Data:

fe578651e224fb6ac88a96a96e14c7f7

AES256 CBC with Salt encrypted:

59/B8xI+KB7/6h74des/SicsUC5mcFqV1T0ocTrSka0=

Payload for QR Code:
AES256 + MD5 Hash

59/B8xI+KB7/6h74des/SicsUC5mcFqV1T0ocTrSka0=fe578651e224fb6ac88a96a96e14c7f7

This is a sample QR Code

QR Code:

Error Correction Level High so up to 30% of QR may be corrupted and it's still possible to retrieve the data

for interested people ☺