Tutorial: Master Key Import in Yoroi

emurgo.io

As of Yoroi 1.3.4 we now have a feature to import your “Daedalus Master Key” into Yoroi. There is a lot of misconception about this feature so let’s spend some time explaining what this feature is and how it works.

Tutorial: Master Key Import in Yoroi

What problem are we trying to solve?

Imagine the following scenario:

1. User has Daedalus installed on their computer
2. They forgot the recovery phrase for their wallet
3. They remember the password for their wallet
4. Daedalus fails to open on their computer

How do you recover your funds?

If you still had the recovery phrase, you could migrate to Yoroi just as in this video or recover your Daedalus wallet on using Daedalus a different machine.

To explain the solution, first we will have to cover some basics.

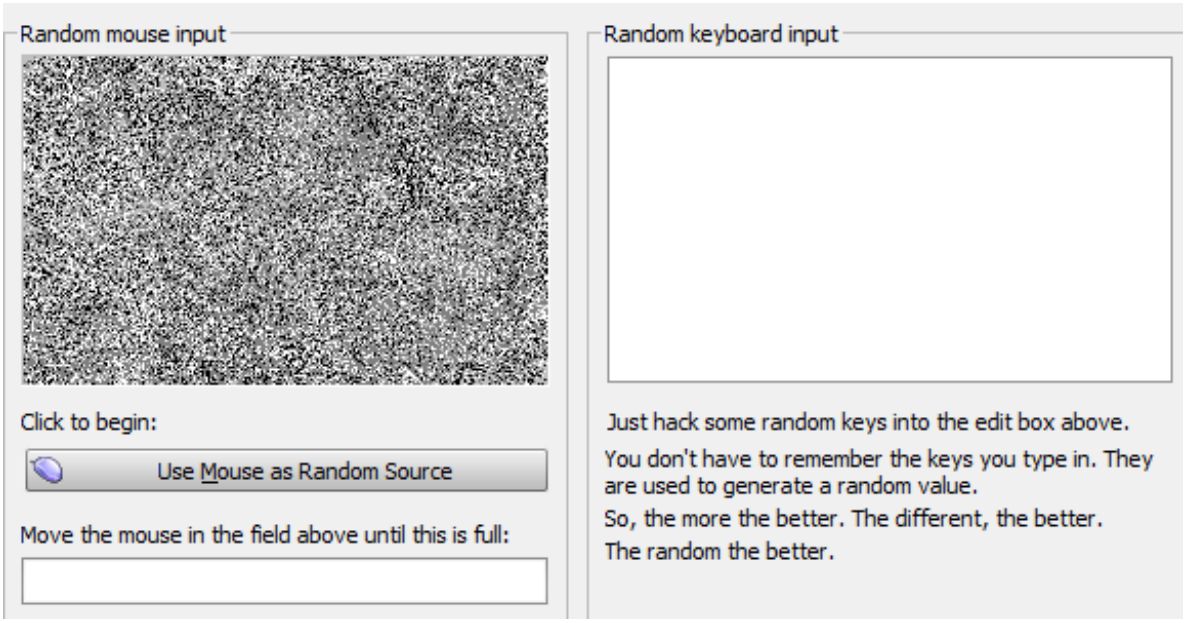
Note: this blog post is intended for an audience with some knowledge of cryptocurrency wallets and how they work. We intend to make more comprehensive posts for beginners going forward, so don’t worry!

Wallet Creation Flow

When you create a wallet, you need to enter 15 words (often called a **recovery phrase** or a **mnemonic**). This mnemonic is to generate your **private key** (in wallets like Yoroi, this is also called a **master key**).

Example recovery phrase screen when creating a wallet

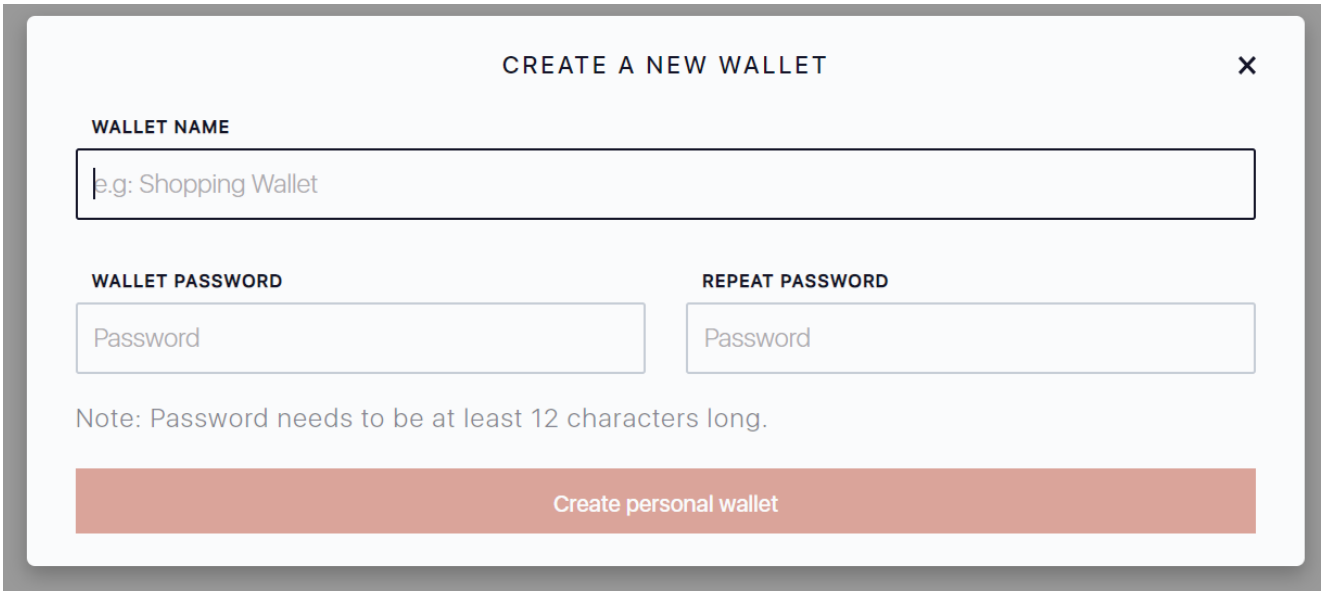
More specifically, the mnemonic generates the **entropy** needed to create your wallet. You may have seen other ways to generate entropy such as moving your cursor or typing on your keyboard.



KeePass generating entropy from mouse+keyboard

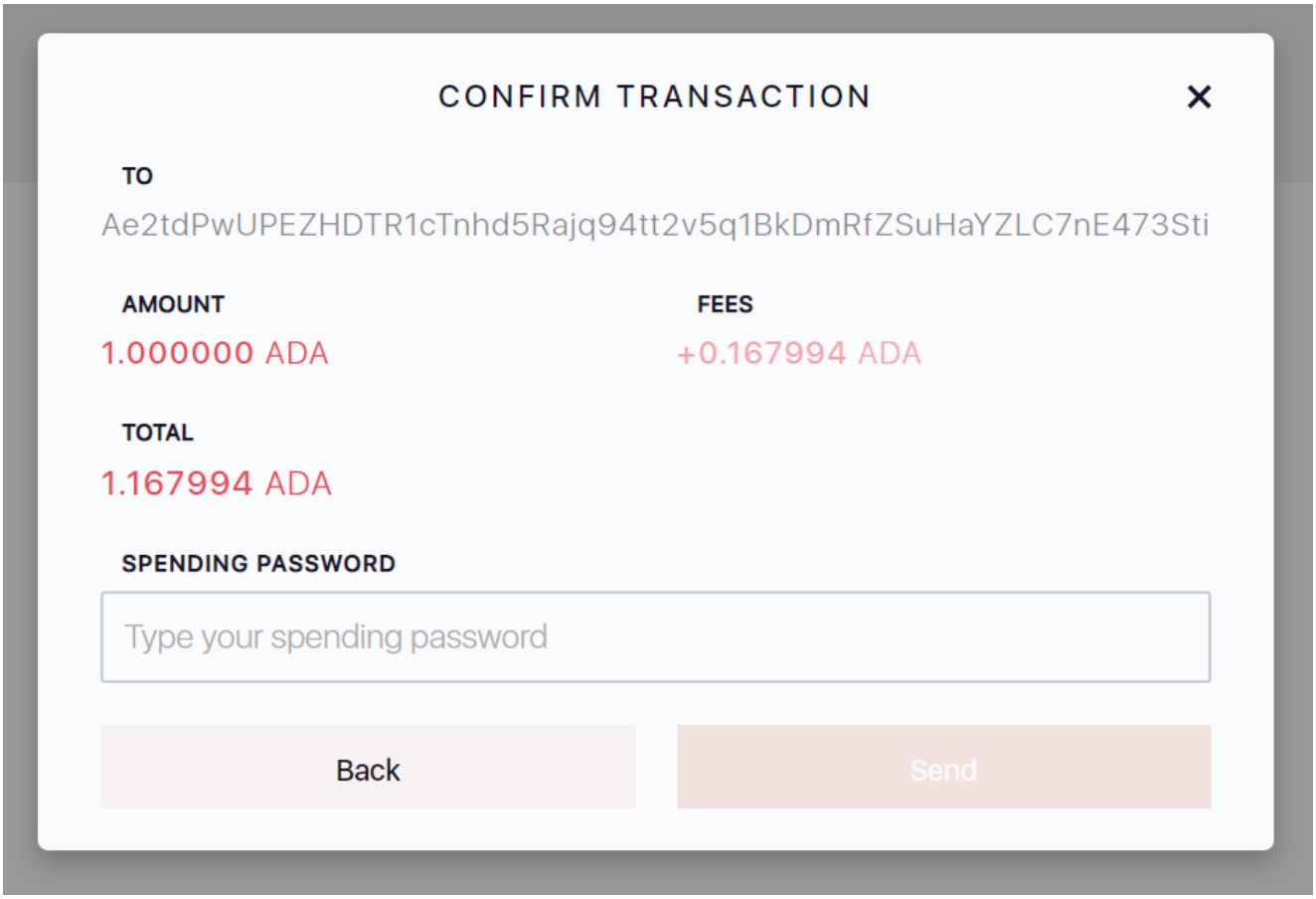
Whoever has the recovery phrase can recover (and take control of) all the money you have on your wallet. Yikes!

We can protect the user by introducing a password



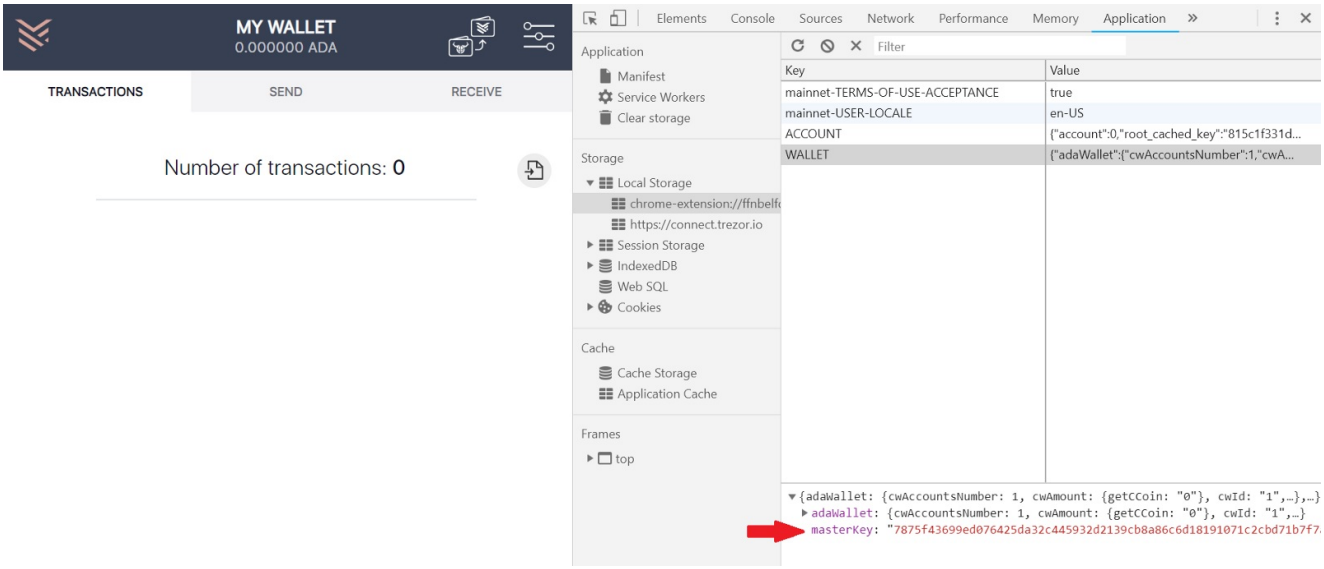
The password encrypts your private key so if somebody gets access to your computer, they cannot access your private key as they don't have the password.

However, your secret key is required to send money, which means you need to decrypt it every time you send money!



Prompt to decrypt your master key in order to send Ada

If you open the Chrome Developer console, you can see your encrypted master key there



Master key for a throwaway wallet

If this is somewhat concerning to you, this is why hardware wallets are so popular! Instead of storing the master key on your machine, it is safely stored within the hardware wallet and Yoroi (or any other application) never gets to see it.

Back to Daedalus

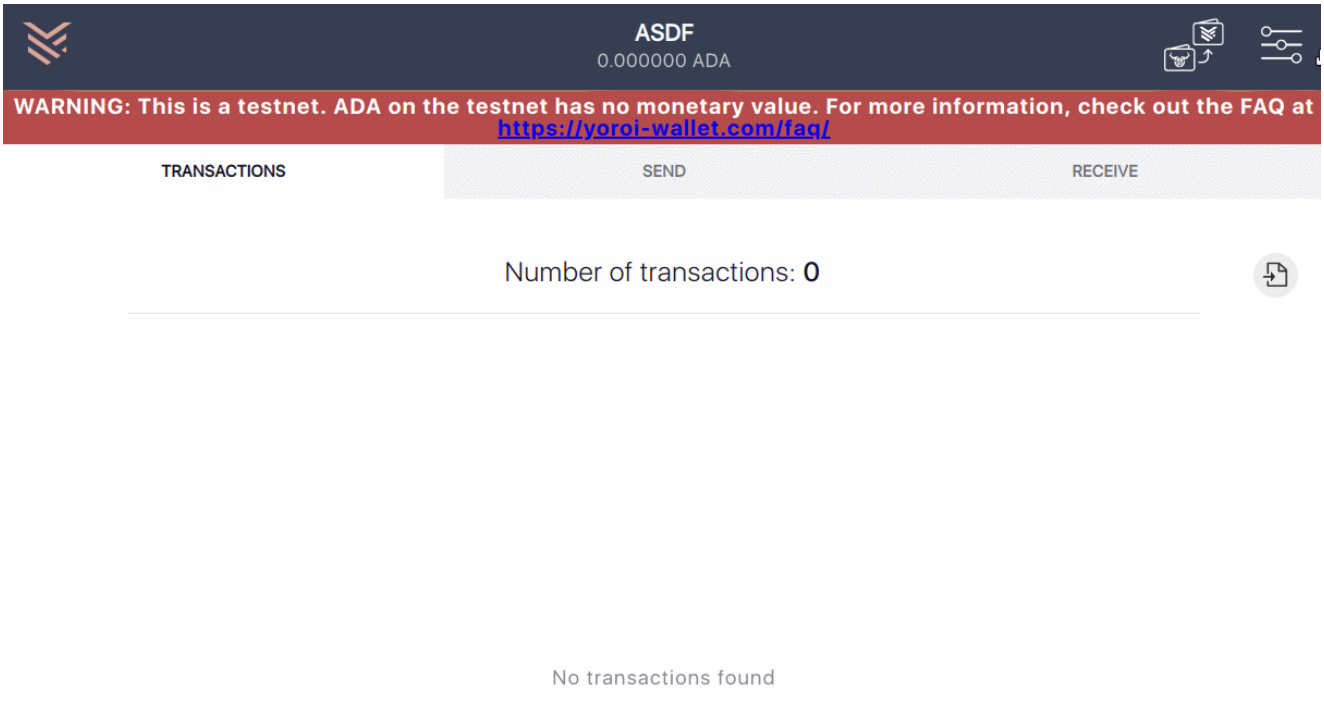
Now that we've covered the basics, let's look at our solution.

Although we do not have the Daedalus mnemonic,**we still have the encrypted master key on our computer**. More specifically, Daedalus stores master keys in a file called*secrets.key* on your hard drive.That means all we need to get our Ada back is use our password!

There is a catch though—Daedalus is actually not the one managing your private key. Here is how Daedalus works (simplified)

Daedalus is just a UI frontend, but all the data is managed by the Cardano Wallet and the Cardano SL fullnode.

This extra complication means we leave it to IOHK to build a tool to extra the master key from*secrets.key* instead of providing one ourselves. However, once you have the master key, importing it into Yoroi is now easy!



Demonstration of restoring by master key

Advantages and looking forward

The advantage of this option (beyond solving the case we outlines) is that you can now also migrate Daedalus wallets to Yoroi that were not created using a mnemonic. As I mentioned before, mnemonics are just one way to generate entropy but it's not the only way and so we should support all users!

Going forward, we will implement a way to restore Yoroi wallets from a secret key also so if you'd like the generate a wallet with a different source of entropy, you'll find a nice home in Yoroi!

About EMURGO
EMURGO drives the adoption of Cardano and adds value to ADA holders by building, investing in, and advising projects or organizations that adopt Cardano's decentralized blockchain ecosystem. EMURGO leverages its expertise in blockchain R&D as well as its global network of related blockchain and industry partners to support ventures globally.

EMURGO is the official commercial and venture arm of the Cardano project, registered in Tokyo, Japan since June 2017 and in Singapore since May 2018. EMURGO is uniquely affiliated and works closely with IOHK to grow Cardano's ecosystem globally and promote the adoption of the Cardano blockchain. To learn more about the project, visit the EMURGO website.

|| **Click here to subscribe to the EMURGO Newsletter** ||

Follow EMURGO on Social Media

- Official Homepage: emurgo.io
- Twitter (English): @emurgo_io
- Twitter (Japanese): @Emurgo_Japan
- Youtube: EMURGO
- Telegram: EMURGO Announcements
- Facebook: @emurgo.io
- Instagram: @emurgo_io
- LinkedIn: @emurgo_io

About Yoroi Wallet

- Yoroi Twitter: @YoroiWallet
- Yoroi Homepage: https://yoroi-wallet.com/

About Cardano

- Cardano Forum: https://forum.cardano.org/
- Cardano Telegram: https://t.me/CardanoGeneral
- Cardano Reddit: