Self-Custody Setup via Keysmith

May 2021

Introduction

In order to receive your ICP token distribution, you will need to generate a native Internet Computer identity, share that identity with the DFINITY Foundation, and pass KYC. The instructions below provide a step-by-step guide to installing Keysmith, a developer tool that lets you generate your native Internet Computer identity. Once generated, you can share your identity with the DFINITY Foundation via a KYC application, or through a secure method, such as SendSafely.

These instructions will be relevant to you if:

- You are a token holder of the ICP utility token **AND**
- Self-custodying your ICP utility tokens

What is Keysmith?

Keysmith is a developer tool that derives cryptographic keys and identifiers for the Internet Computer. Among these identifiers includes: an account identifier, which indicates the source or destination of an ICP token transfer. Keysmith does not sign or send messages to the Internet Computer. Hence, Keysmith does not facilitate ICP token transfer, but rather only ICP token custody. For use cases other than custody, such as payments, consider using Keysmith in conjunction with other software, such as the DFINITY Canister SDK. Other software will not be covered in this document. Here we focus on Keysmith, which allows you to custody your tokens, and gives the best option for integrating with the widest variety of wallet applications.

Secure Your Environment

You will use Keysmith to generate a mnemonic seed. **The safety and security of your mnemonic seed is your responsibility and there is no substitute for planning ahead, bringing the right equipment, having the right skills, and using good judgment.** We strongly recommend you proceed using an air-gapped computer to reduce the risk of having your mnemonic seed compromised. Depending on the hardware available, you might want to physically remove your network controller, microphone, camera, and other components, or disable them in your BIOS. Covert channels can be established through a variety of different mediums, including sound, light, radio-frequency, and physical media. Be sure to evaluate the capabilities of your system before settling on a configuration that makes sense for you. **If you don’t know what you’re doing, then**

you should consult with a computer security expert. Do not contact the DFINITY Foundation for help with securing your environment.

1. Install Keysmith

Download

Download the latest tarball here.
Be sure to select the tarball that matches the operating system and architecture of the computer that will run Keysmith. If you're using an air-gapped computer, then the operating system and architecture may differ from the networked computer you're using to perform the download. How you copy the tarball from your networked computer to your air-gapped computer will depend on your configuration.

Keysmith supports the following operating systems and architectures:

- Darwin / AMD64 – for older Mac models with an Intel chip (how to check)
- Darwin / ARM64 – for newer Mac models with an M1 chip (how to check)
- Linux / AMD64
- Linux / ARM64
- Windows / AMD64

Verify (Optional)

If you want to verify the authenticity of the tarball, then please also download the supplementary `SHA256.SIG` and `SHA256.SUM` files, as well as the release key, which you can find here.

Verify the SHA256 checksum of the tarball.

```
grep "$(openssl dgst -sha256 keysmith-*.tar.gz)" SHA256.SUM
```

Verify the signature on the tarball.

```
openssl dgst -verify public.key -signature SHA256.SIG SHA256.SUM
```

The command above should display the following output.

```
Verified OK
```

Install

Open your terminal.
MacOS: Open your terminal by searching for it with the magnifying glass in the top right corner of your screen. This is where you'll be able to open the "command line"-- a way of inputting instructions directly into your computer without using your mouse or desktop.
WindowsOS: Type cmd into the search bar in your taskbar and start a command prompt by clicking the command prompt icon. Then change to the tool folder by copying and pasting the following command:

To extract the executable from the tarball, enter the following command into your terminal:

```
tar -f keysmith-*.tar.gz -x
```

Next, add the executable to your `PATH` by entering the command below:

```
sudo install keysmith /usr/local/bin
```

You will be prompted to enter your laptop password. The password itself will not appear, simply type it and press enter.

Check

Next, check if Keysmith is properly installed.
Run the executable by entering the command in your terminal:

```
keysmith
```

The command above should display the following output.

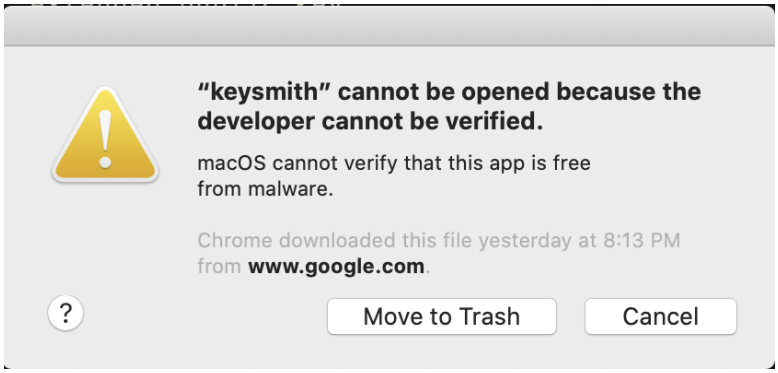
```
usage: keysmith <command> [<args>]

Available Commands:
     account             Print your account identifier.
     generate            Generate your mnemonic seed.
     legacy-address      Print your legacy address.
     principal           Print your principal identifier.
     private-key         Write your private key to a file.
     public-key          Print your public key.
     version             Print the version number.
```

```
x-public-key        Print your extended public key.
```

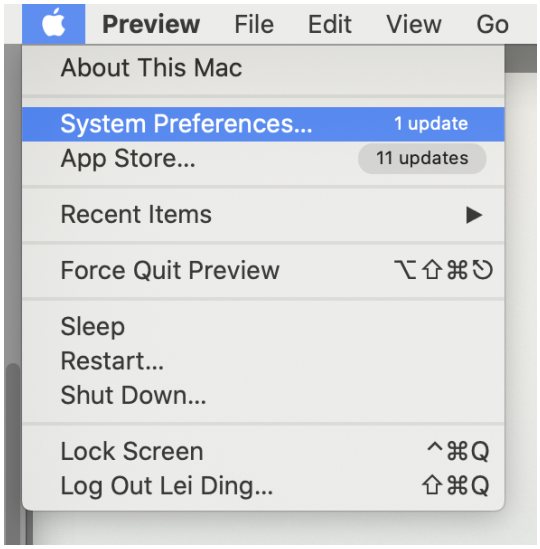
If you're using MacOS and you encountered an error, then continue with the section below. Otherwise, skip it.

Additional Instructions for macOS Users

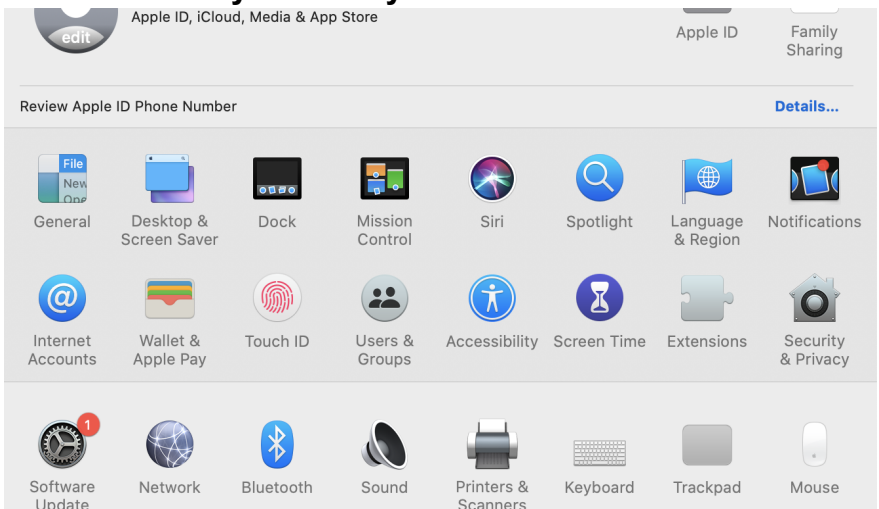
If you're using macOS, then you may get blocked when trying to run the executable.



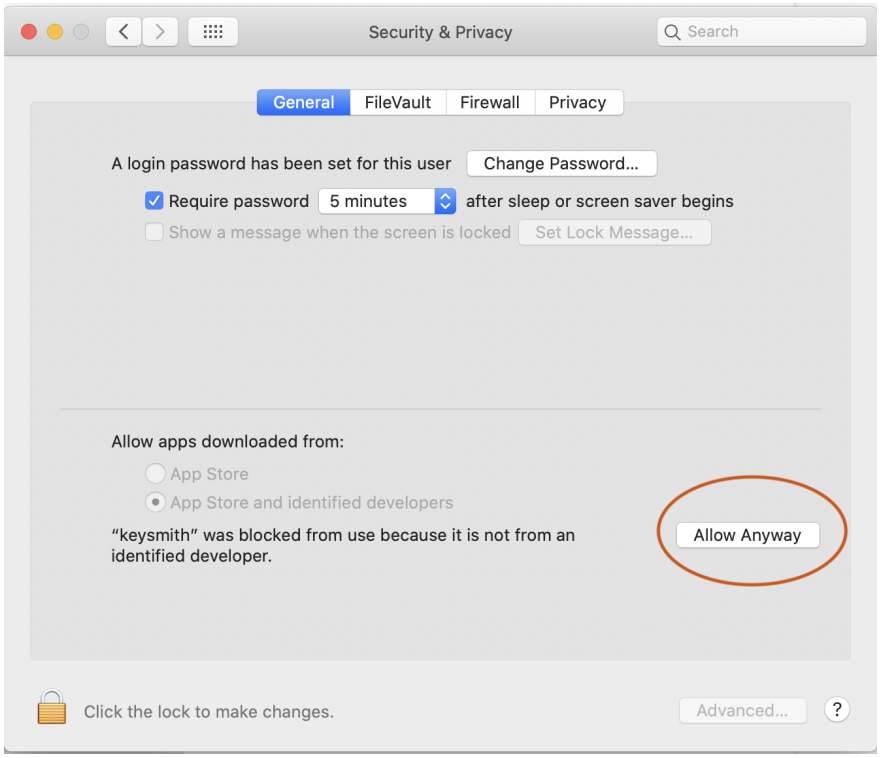
Click on **Cancel**. You will need to update your security settings.
Click on the top left Mac icon on your screen, and then click **System Preferences**.



Click on **Security & Privacy**.

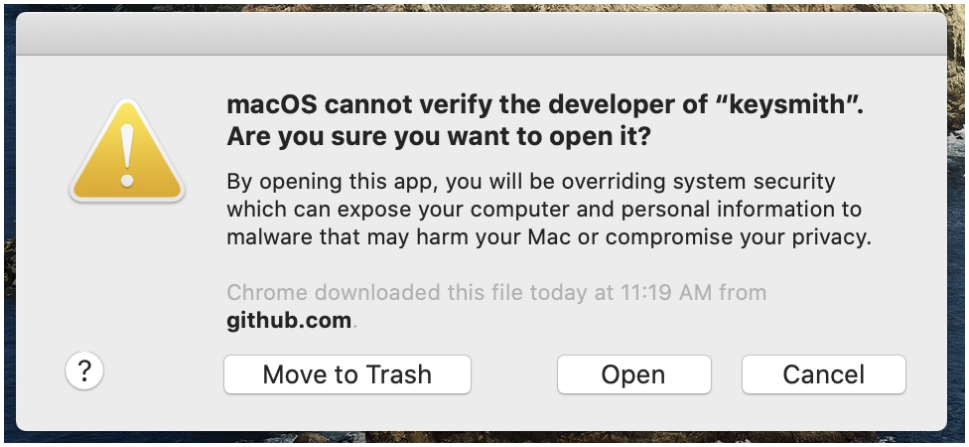


Click on the **General** tab, and then click **Allow Anyway**.



You may be asked to enter your credentials or use TouchId at this point.

If you are prompted to confirm whether you still want to open the file, click **Open**.



Once complete, return to your terminal and run `keysmith` again.

2. Generate Your Mnemonic Seed

Once you have installed Keysmith, **and you are confident that your environment is secure**, then you are ready to generate your mnemonic seed.

Enter the following command to generate your mnemonic seed.

```
keysmith generate
```

A `seed.txt` file will be created which holds your mnemonic seed.

To view your mnemonic seed in the terminal, enter the following below:

```
cat seed.txt
```

The command above will display your mnemonic seed, which should look something like this:

```
panther air swamp vacuum draft erode license fun record toast lazy
element
```

Write down your mnemonic seed on a piece of paper and never lose it! Be careful that the ink or pressure from your pen does not bleed through to other sheets of paper or the table, which could inadvertently create copies of your mnemonic seed without your knowledge.

3. Derive Your Principal Identifier

Enter the following command to derive your principal identifier.

```
keysmith principal
```

The command above will display your principal identifier, which should look something like this:

```
a56gn-wnhrl-i76df-ewgfe-23jfd-dfh03-ergrg-fesr1-1jhs9-reg2o-ure
```

4. Save your Principal Identifier

To save your Principal Identifier, copy your principal identifier to a word document or text application, and transfer it (via USB) from your air-gapped computer to your networked computer. You will need to share this key with DFINITY in the next step. The Principal Identifier is a public key that can be shared in this method.

5. Share your Principal Identifier

Depending on your onboarding process, you may be asked to do either of the following:

1. If you're generating your principal identifier **before** submitting your KYC application to Acuant, then you will enter it in the required field on the application itself.

2. If you're generating your principal identifier **after** submitting your KYC application, then you will receive a SendSafely link to securely share your principal identifier with the DFINITY Foundation.

Reach out to our Support Portal with any questions.