

# SUPER SHAMIR

## Návod

v1.2 - 9.1.2025

poslední verzi najdete vždy na:  
[bitconovaskola.cz/supershmir](http://bitconovaskola.cz/supershmir)

### Obsah:

<b>1 Úvod</b> .....	2
<b>2 Trezor Suite + hardwarová peněženka Trezor</b> .....	3
<b>3 Utilita trezorctl</b> .....	5
<b>3.1 Windows</b> .....	5
3.1.1 Python - instalace .....	5
3.1.2 trezorctl - instalace .....	6
<b>3.2 macOS (+ Linux)</b> .....	8
3.2.1 Homebrew - instalace .....	8
3.2.2 Python - instalace .....	9
3.2.3 libusb - instalace .....	10
3.2.4 trezorctl - instalace .....	11
<b>4 Super Shamir - spuštění a nastavení</b> .....	12
4.1 Inicializace Peněženky - Windows .....	12
4.2 Inicializace Peneženky - macOS .....	12
4.3 Obecný postup při inicializaci Super Shamiru na Trezoru .....	13
4.4 Konkrétní příklad dle SLIP-0039 .....	14

sepsal: Tarabys



**BITCOINOVÁ  
ŠKOLA.CZ**

Poděkování v satoshi můžete poslat na LN adresu: [tarabys@blink.sv](mailto:tarabys@blink.sv)  
Našli jste chybu? Dejte mi vědět >>> [www.linktr.ee/tarabys](http://www.linktr.ee/tarabys)

## 1 Úvod

Vše dělejte v klidu, s rozvahou a bez časového stresu. Jedná se o vytvoření Peněženky, kterou zřejmě budete využívat spoustu let a opravdu si nepřejete dělat hned na začátku zbytečné chyby, které by navíc mohly vést až ke ztrátě bitcoinů.

Ohledně bitcoinu se vždy vyplatí být opatrný, místy až paranoidní, takže je potřeba vše řádně zkontrolovat aneb dvakrát čti a jednou instaluj... ;)

Celý postup doporučuji dělat na aktualizovaném, čerstvě restartovaném počítači, kde ideálně nepoběží žádné procesy, které nejsou nezbytně nutné pro bezvadné provedení tohoto návodu.

Tímto se vyhnete většině případných technických problémů.

Jedna věc je samotné technické vytvoření zálohy Peněženky pomocí Super Shamiru a druhá, náročnější, je zvážení toho jak si takovou zálohu nastavit a navrhnout - celkový počet skupin, práh obnovy skupin, počet dílů a jejich práh obnovy v rámci jednotlivých skupin. Super Shamir umožňuje extrémně flexibilní nastavení a spoustu možných kombinací, ale s tímto vám bohužel návod nijak zvlášť nepomůže, protože každý má úplně jiné preference a možnosti úschovy jednotlivých dílů (sharů).

Nicméně na konci uvádím konkrétní příklad, který je uveden v samotném standardu SLIP-0039 na Githubu, který může sloužit jako inspirace.



## 2 Trezor Suite a hardwarová peněženka Trezor

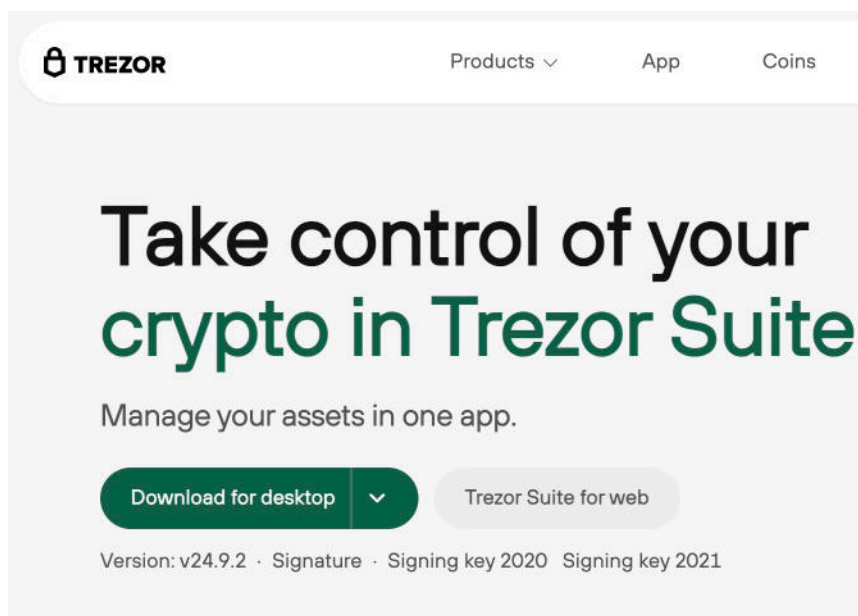
Pro používání Super Shamiru je nutné mít **Trezor Model T, Safe 3 nebo Safe 5**. Super Shamir ani jinou funkcionalitu standardu SLIP-0039 nelze použít s HW peněženkou Trezor One.

Předpokládejme, že máte nainstalovanou obslužnou aplikaci k peněženkám Trezor s názvem **Trezor Suite**. Pokud ne, najdete ji na webu Trezoru:

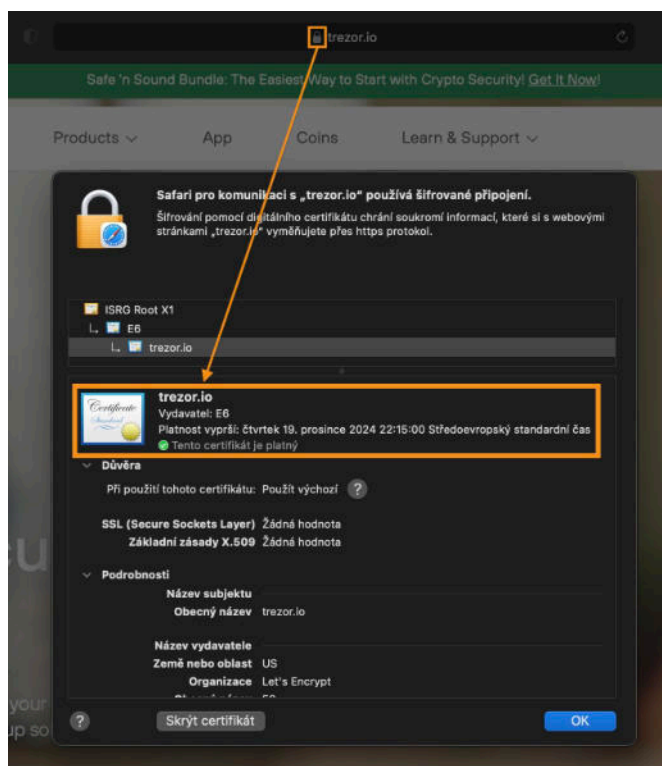
<https://trezor.io/>

Tuto adresu raději ručně přepište přímo do adresního řádku vašeho prohlížeče - ale stačí i zadat jen **trezor.io**, stiskněte Enter a na webu přejděte na záložku App, kde už najdete ke stažení Trezor Suite ve verzi pro váš operační systém.

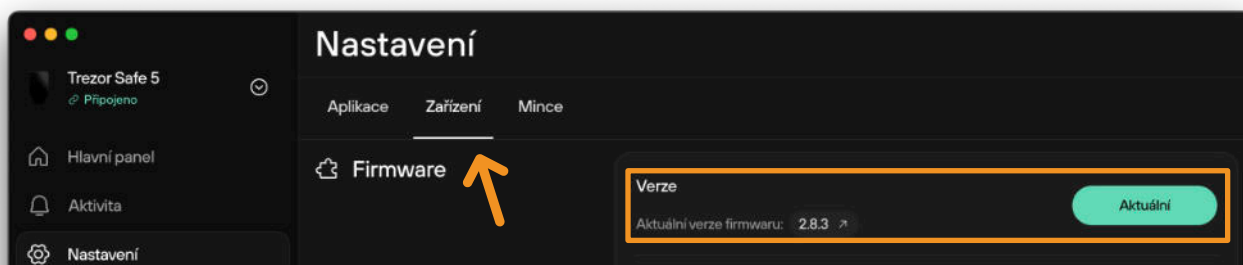
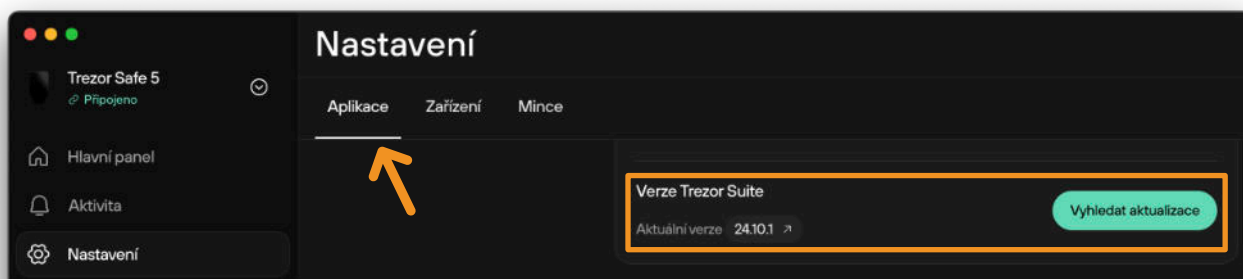
Nedávejte pouze vyhledat (pomocí Google apod.) výraz Trezor Suite, Trezor apod. protože je velká pravděpodobnost, že na prvních místech vyhledávání na vás vyskočí odkaz na některé podvodné weby, kde byste stáhli upravenou verzi Trezor Suite (dále jen TS) a to opravdu nechcete!



Pro jistotu zkontrolujte i pravost webu - v adresním řádku prohlížeče je vždy vedle dané URL i symbol zámku (nebo něco podobného), kde lze prohlédnout certifikáty o pravosti webu apod. (viz ilustrační obr. níže)



Pokud už aplikaci TS máte, tak proveďte aktualizaci. Jak samotného TS tak i firmwaru vašeho Trezoru na poslední dostupné verze.



Na Trezoru musí být nainstalován firmware, ale není nutno ručně odstraňovat aktuální Peněženku tzn. dělat wipe zařízení

## 3 Utilita trezorcti

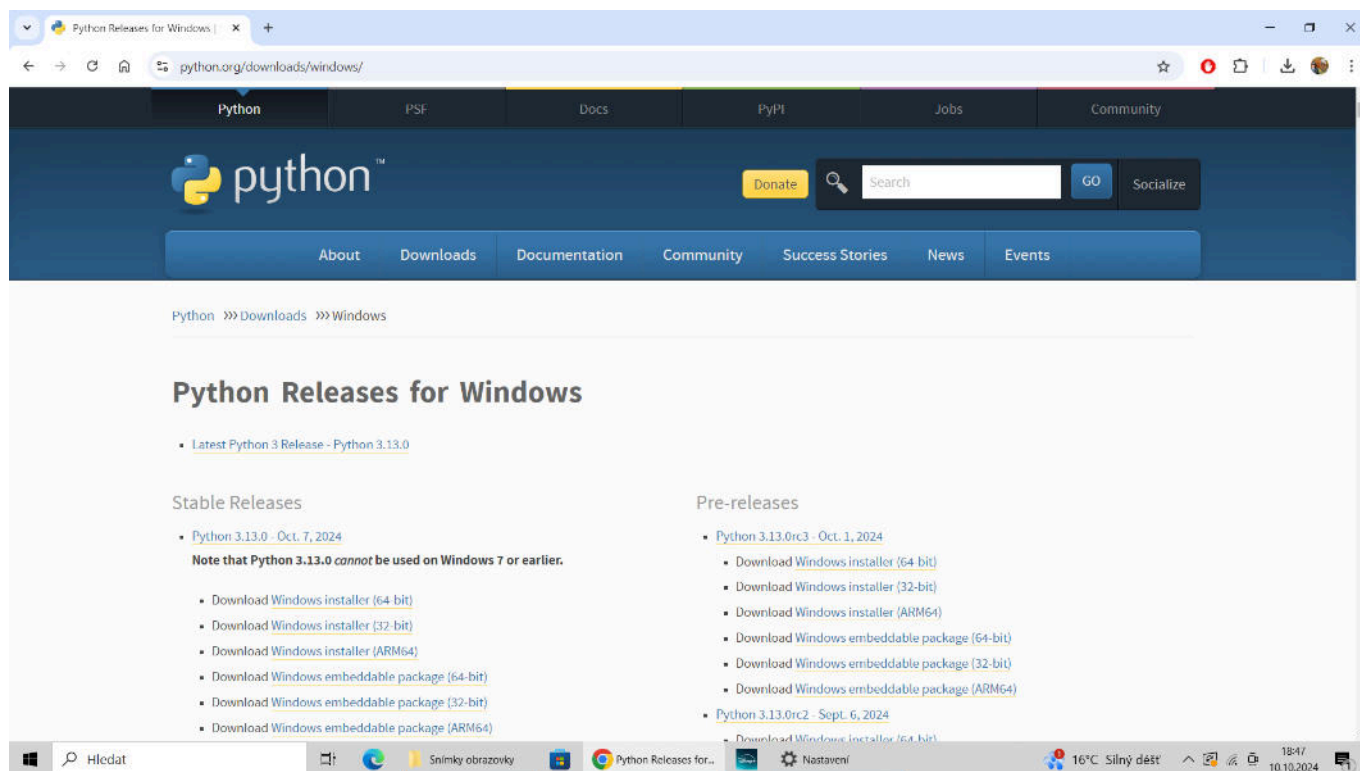
V následujících krocích nainstalujeme všechny nutné podpůrné aplikace pro pozdější spuštění inicializace Super Shamiru.

Přestože je princip a postup skoro stejný, tak jsou jednotlivé body v této části rozděleny zvlášť pro **Windows** a zvlášť pro **macOS**. Návod přímo pro uživatele **Linuxu** není nutný, protože většina Linuxových distribucí již Python obsahuje a ti tak můžou přeskočit až k bodu 3.2.3 pro macOS.

### 3.1 Windows

#### 3.1.1 Python - instalace (Windows)

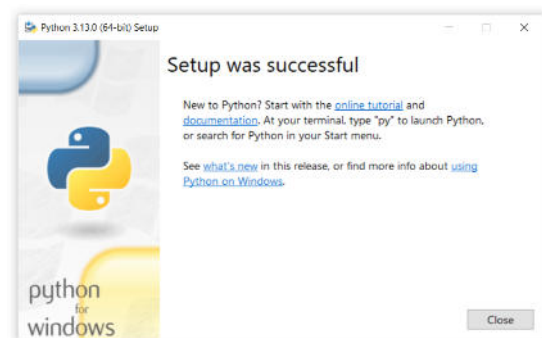
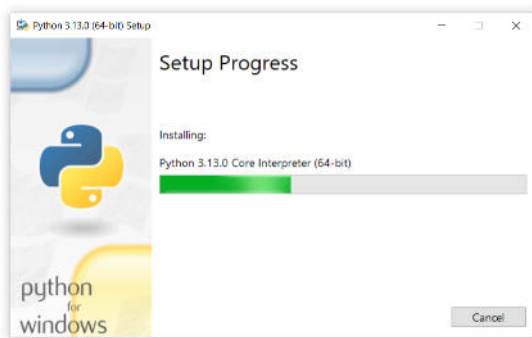
V prohlížeči běžte na <https://www.python.org/downloads/windows/> a stáhněte si pokud možno poslední stabilní verzi (Stable Releases) pro svou verzi Windows - verze ale musí být minimálně 3.5 nebo vyšší.



Spustíte instalaci - je nutné mít zatrhnutou možnost:  
**„Add python.exe to PATH“**



Počkejte na kompletní instalaci a pro jistotu PC restartujte.



Tímto je hotova instalace jazyka Python.

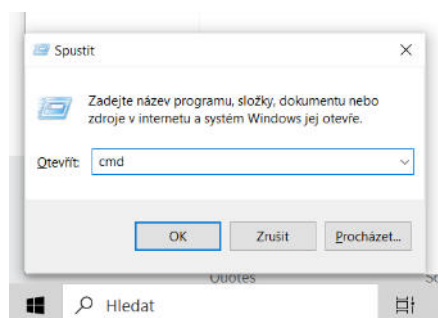
### 3.1.2 trezorctl - instalace (Windows)

Spustíte příkazový řádek:  
pomocí současného stisku kláves Win (■) a R (Win+R) otevřete utilitu Spustit

Zde napište do pole Otevřít příkaz:

`</>` cmd

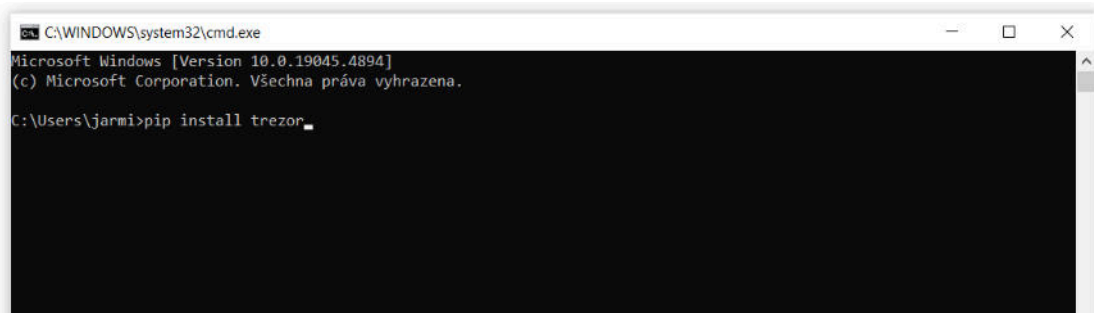
a stiskněte OK



V otevřeném okně napište za znak > příkaz:

```
</> pip install trezor
```

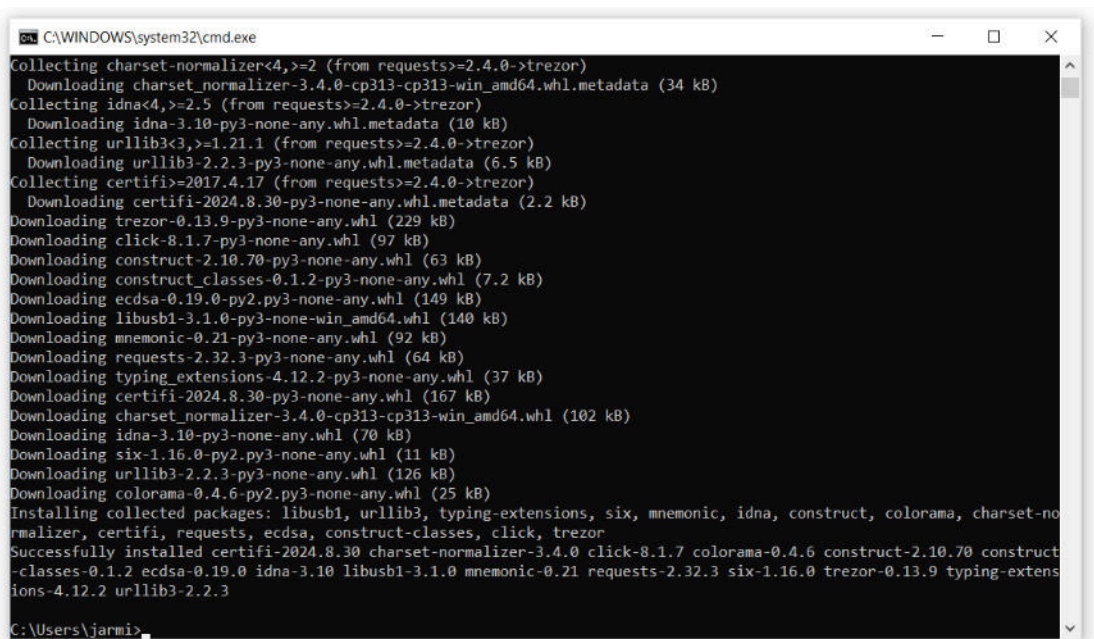
a stiskněte klávesu Enter



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\jarmi>pip install trezor_
```


Spustí se instalace, tu nechte kompletně proběhnout



```
C:\WINDOWS\system32\cmd.exe
Collecting charset-normalizer<4,>=2 (from requests>=2.4.0->trezor)
  Downloading charset_normalizer-3.4.0-cp313-cp313-win_amd64.whl.metadata (34 kB)
Collecting idna<4,>=2.5 (from requests>=2.4.0->trezor)
  Downloading idna-3.10-py3-none-any.whl.metadata (10 kB)
Collecting urllib3<3,>=1.21.1 (from requests>=2.4.0->trezor)
  Downloading urllib3-2.2.3-py3-none-any.whl.metadata (6.5 kB)
Collecting certifi>=2017.4.17 (from requests>=2.4.0->trezor)
  Downloading certifi-2024.8.30-py3-none-any.whl.metadata (2.2 kB)
Downloading trezor-0.13.9-py3-none-any.whl (229 kB)
Downloading click-8.1.7-py3-none-any.whl (97 kB)
Downloading construct-2.10.70-py3-none-any.whl (63 kB)
Downloading construct_classes-0.1.2-py3-none-any.whl (7.2 kB)
Downloading ecdsa-0.19.0-py2.py3-none-any.whl (149 kB)
Downloading libusb1-3.1.0-py3-none-win_amd64.whl (140 kB)
Downloading mnemonic-0.21-py3-none-any.whl (92 kB)
Downloading requests-2.32.3-py3-none-any.whl (64 kB)
Downloading typing_extensions-4.12.2-py3-none-any.whl (37 kB)
Downloading certifi-2024.8.30-py3-none-any.whl (167 kB)
Downloading charset_normalizer-3.4.0-cp313-cp313-win_amd64.whl (102 kB)
Downloading idna-3.10-py3-none-any.whl (70 kB)
Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Downloading urllib3-2.2.3-py3-none-any.whl (126 kB)
Downloading colorama-0.4.6-py2.py3-none-any.whl (25 kB)
Installing collected packages: libusb1, urllib3, typing-extensions, six, mnemonic, idna, construct, colorama, charset-normalizer, certifi, requests, ecdsa, construct-classes, click, trezor
Successfully installed certifi-2024.8.30 charset-normalizer-3.4.0 click-8.1.7 colorama-0.4.6 construct-2.10.70 construct-classes-0.1.2 ecdsa-0.19.0 idna-3.10 libusb1-3.1.0 mnemonic-0.21 requests-2.32.3 six-1.16.0 trezor-0.13.9 typing-extensions-4.12.2 urllib3-2.2.3

C:\Users\jarmi>
```

Tímto už je vše připraveno na spuštění utility trezorctl a inicializaci nastavení Peněženky v módu Super Shamir.

Můžete přejít na sekci 4 > 4.1 na straně 12 

## 3.2 macOS

### 3.2.1 Homebrew - instalace (macOS)

Spustíte aplikaci Terminál (aplikace/příkazová řádka v macOS) - to můžete provést více způsoby, ale nejjednodušší je stisknout klávesu CMD a mezerníku (⌘+mezerník) napsat: Terminál a zvolit Otevřít

V samotném Terminálu napište/zkopírujte níže uvedený příkaz:



čas od času se následující příkaz mírně pozmění - pro jistotu si ověřte aktuální a přesné znění na webu **brew.sh**, kde je hned v horní části vidět aktuální a funkční příkaz

```
</> /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

a stiskněte Enter

```
tarabys — zsh — 134x36
Last login: Fri Sep 27 17:44:24 on ttys000
tarabys@Macbook ~ % /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Budete vyzváni na zadání hesla k vašemu Macu. Heslo se při psaní nezobrazuje a nezobrazuje se ani počet znaků, takže jej musíte napsat "naslepo". Po jeho zadání stiskněte Enter

```
tarabys — sudo - bash -c #!/bin/bash\012\012# We don't need return codes for "$(command)", only stdout is needed.\012# Allow '[' -...
Last login: Fri Sep 27 17:44:24 on ttys000
tarabys@Macbook ~ % /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
==> Checking for `sudo` access (which may request your password)...
Password: [ ]
```

Ukáže se seznam instalovaných položek, který potvrdíte Enterem

```
tarabys — bash -c #!/bin/bash\012\012# We don't need return codes for "$(command)", only stdout is needed.\012# Allow '[' -n "$(c...
Last login: Fri Sep 27 17:44:24 on ttys000
tarabys@Macbook ~ % /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
==> Checking for `sudo` access (which may request your password)...
Password: [ ]
==> This script will install:
/opt/homebrew/bin/brew
/opt/homebrew/share/doc/homebrew
/opt/homebrew/share/man/man1/brew.1
/opt/homebrew/share/zsh/site-functions/_brew
/opt/homebrew/etc/bash_completion.d/brew
/opt/homebrew
Press RETURN/ENTER to continue or any other key to abort:
[ ]
```



Počkejte na kompletní instalaci.

Pokud se vám na konci objeví položka **Next steps**: (viz screenshot), tak tyto tři příkazy (na vašem Macu budou vypadat trochu jinak!) po jednom zkopírujte, vložte v příkazovém řádku za znak % a stiskněte Enter.

```
tarabys ~ -zsh - 128x49
Instructions on how to configure your shell for Homebrew
can be found in the 'Next steps' section below.
==> Installation successful!

==> Homebrew has enabled anonymous aggregate formulae and cask analytics.
Read the analytics documentation (and how to opt-out) here:
https://docs.brew.sh/Analytics
No analytics data has been sent yet (nor will any be during this install run).

==> Homebrew is run entirely by unpaid volunteers. Please consider donating:
https://github.com/Homebrew/brew#donations

==> Next steps:
- Run these commands in your terminal to add Homebrew to your PATH:
  echo >> /Users/tarabys/.zprofile
  echo 'eval "$(/opt/homebrew/bin/brew shellenv)"' >> /Users/tarabys/.zprofile
  eval "$(/opt/homebrew/bin/brew shellenv)"
- Run brew help to get started
- Further documentation:
  https://docs.brew.sh
```

```
==> Next steps:
- Run these commands in your terminal to add Homebrew to your PATH:
  echo >> /Users/tarabys/.zprofile
  echo 'eval "$(/opt/homebrew/bin/brew shellenv)"' >> /Users/tarabys/.zprofile
  eval "$(/opt/homebrew/bin/brew shellenv)"
- Run brew help to get started
- Further documentation:
  https://docs.brew.sh

tarabys@Macbook ~ % echo >> /Users/tarabys/.zprofile
tarabys@Macbook ~ % echo 'eval "$(/opt/homebrew/bin/brew shellenv)"' >> /Users/tarabys/.zprofile
tarabys@Macbook ~ % eval "$(/opt/homebrew/bin/brew shellenv)"
```

### 3.2.2 Python - instalace (macOS)

V aplikaci Terminál napište/zkopírujte příkaz:

```
</> brew install python3
```

a stiskněte Enter

```
man brew
https://docs.brew.sh
tarabys@Macbook ~ % brew install python3
```

Nechte proběhnout kompletní instalaci.

Zadejte příkaz

```
</> exit
```

a stiskněte Enter. Poté Terminál ukončete (⌘+Q).

```
python3, python3-config, pip3 etc., respectively, have been installed into
/opt/homebrew/opt/python@3.12/libexec/bin

See: https://docs.brew.sh/Homebrew-and-Python
tarabys@Macbook ~ % exit
```

### 3.2.3 libusb - instalace (macOS)

Opět spustte aplikaci Terminál a napište/zkopírujte příkaz:

```
</> brew install libusb
```

a stiskněte Enter

```
tarabys — -zsh — 128x52
Last login: Fri Sep 27 18:09:11 on ttys000
tarabys@Macbook ~ % brew install libusb
```

Nechte proběhnout kompletní instalaci

```
tarabys — -zsh — 128x52
Last login: Fri Sep 27 18:09:11 on ttys000
tarabys@Macbook ~ % brew install libusb
==> Downloading https://ghcr.io/v2/homebrew/core/libusb/manifests/1.0.27
##### 100.0%
==> Fetching libusb
==> Downloading https://ghcr.io/v2/homebrew/core/libusb/blobs/sha256:5d14898869c8bb7d12f6a8091b16c2db76909293b579d10b0ee84624845
##### 100.0%
==> Pouring libusb--1.0.27.arm64_ventura.bottle.tar.gz
📦 /opt/homebrew/Cellar/libusb/1.0.27: 23 files, 620.5KB
==> Running `brew cleanup libusb`...
Disable this behaviour by setting HOMEBREW_NO_INSTALL_CLEANUP.
Hide these hints with HOMEBREW_NO_ENV_HINTS (see `man brew`).
tarabys@Macbook ~ %
```



## 3.2.4 trezorctl - instalace (macOS)

V aplikaci Terminál napište/zkopírujte příkaz:

```
</> pip3 install trezor
```

a stiskněte Enter

```
Hide these hints with HOMEBREW_NO_ENV_HINTS (see 'man brew').  
macbook@10 ~ % pip3 install trezor
```

V případě chyby - viz screenshot níže - zadejte v Terminálu příkaz:

```
</> pip3 install trezor --break-system-packages
```

a stiskněte Enter. Nechte proběhnout až do konce...

```
Disable this behaviour by setting HOMEBREW_NO_INSTALL_CLEANUP.  
Hide these hints with HOMEBREW_NO_ENV_HINTS (see 'man brew').  
macbook@10 ~ % pip3 install trezor  
error: externally-managed-environment  
  
* This environment is externally managed  
↳ To install Python packages system-wide, try brew install  
xyz, where xyz is the package you are trying to  
install.  
  
If you wish to install a Python library that isn't in Homebrew,  
use a virtual environment:  
  
python3 -m venv path/to/venv  
source path/to/venv/bin/activate  
python3 -m pip install xyz  
  
If you wish to install a Python application that isn't in Homebrew,  
it may be easiest to use 'pipx install xyz', which will manage a  
virtual environment for you. You can install pipx with  
  
brew install pipx  
  
You may restore the old behavior of pip by passing  
the '--break-system-packages' flag to pip, or by adding  
'break-system-packages = true' to your pip.conf file. The latter  
will permanently disable this error.  
  
If you disable this error, we STRONGLY recommend that you additionally  
pass the '--user' flag to pip, or set 'user = true' in your pip.conf  
file. Failure to do this can result in a broken Homebrew installation.  
  
Read more about this behavior here: <https://peps.python.org/pep-0668/>  
  
note: If you believe this is a mistake, please contact your Python installation or OS distribution provider. You can override this, at the risk of breaking your Python installation or OS, by passing --break-system-packages.  
hint: See PEP 668 for the detailed specification.  
macbook@10 ~ %
```

```
macbook@10 ~ % pip3 install trezor --break-system-packages  
Collecting trezor  
  Downloading trezor-0.13.9-py3-none-any.whl.metadata (44 kB)  
Collecting ecdsa>=0.9 (from trezor)  
  Downloading ecdsa-0.19.0-py2.py3-none-any.whl.metadata (29 kB)  
Collecting mnemonic>=0.20 (from trezor)  
  Downloading mnemonic-0.21-py3-none-any.whl.metadata (3.4 kB)  
Collecting requests>=2.4.0 (from trezor)  
  Downloading requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)  
Collecting click<8.2,>=7 (from trezor)  
  Downloading click-8.1.7-py3-none-any.whl.metadata (3.0 kB)  
Collecting libusb1>=1.6.4 (from trezor)  
  Downloading libusb1-3.1.0-py3-none-any.whl.metadata (15 kB)  
Collecting construct!=2.10.55,>=2.9 (from trezor)  
  Downloading construct-2.10.70-py3-none-any.whl.metadata (4.2 kB)  
Collecting typing-extensions>=4.7.1 (from trezor)  
  Downloading typing_extensions-4.12.2-py3-none-any.whl.metadata (3.0 kB)  
Collecting construct-classes>=0.1.2 (from trezor)  
  Downloading construct_classes-0.1.2-py3-none-any.whl.metadata (4.5 kB)  
Collecting six>=1.9.0 (from ecdsa>=0.9->trezor)  
  Downloading six-1.16.0-py2.py3-none-any.whl.metadata (1.8 kB)  
Collecting charset-normalizer<4,>=2 (from requests>=2.4.0->trezor)  
  Downloading charset_normalizer-3.3.2-cp312-cp312-macosx_11_0_arm64.whl.metadata (33 kB)  
Collecting idna<4,>=2.5 (from requests>=2.4.0->trezor)  
  Downloading idna-3.10-py3-none-any.whl.metadata (10 kB)
```

## 4 Super Shamir - spuštění a nastavení

### 4.1 Inicializace Peněženky - Windows

Spustte příkazový řádek:

pomocí současného stisku kláves Win (⊞) a R (Win+R) otevřete utilitu Spustit

Zde napište do pole Otevřít příkaz:

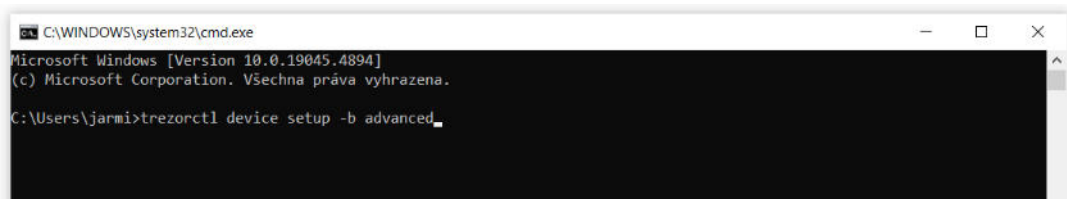
```
</> cmd
```

a stiskněte OK

V otevřeném okně napište za znak > příkaz:

```
</> trezorctl device setup -b advanced
```

a stiskněte klávesu Enter



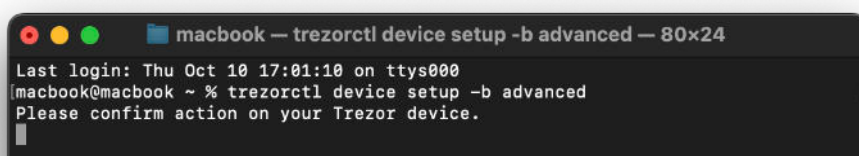
Toto je poslední krok na Windows PC - dále již pokračujte na Trezoru.

### 4.2 Inicializace Peněženky - macOS

V aplikaci Terminál napište/zkopírujte příkaz:

```
</> trezorctl device setup -b advanced
```

a stiskněte Enter



Toto je poslední krok na Macu - dále již pokračujte na Trezoru.

### 4.3 Obecný postup při inicializaci Super Shamiru na Trezoru

Nastavení Super Shamir schématu začíná nastavením třech základních bodů:

1. výběrem celkového množství skupin - volba od 2 do 16 skupin
2. výběrem prahu obnovení těchto skupin - volba 1 až 16
3. nastavení celkového počtu dílů a prahu obnovy pro každou skupinu

Dále se vám již budou ukazovat slova jednotlivých dílů (vždy 20) pro danou skupinu - tyto slova si postupně opisujete přesně v tomto daném pořadí (1. až 20. slovo).

Po zobrazení všech 20 slov právě vytářeného dílu vás Trezor vyzve celkem 3x k zadání slova na konkrétní náhodné pozici (dá vám na výběr ze 3 slov) aby si tak ověřil, že jste si seznam pečlivě opsali a máte ho zálohovaný.



Pokud zvolíte slovo, které se na dané pozici v seznamu nevyskytuje = uděláte chybu, tak vás Trezor vrátí na obrazovku seznamu slov, můžete si ho znovu projít a zkontrolovat, případně opravit chybu.

Tento proces se opakuje pro všechny skupiny a pro všechny díly v rámci každé skupiny.



## 4.4 Konkrétní příklad dle SLIP-0039

Super Shamir je extrémně flexibilní a nelze doporučit nějaké konkrétní nastavení. V principu jde nastavit celkový počet skupin (2 až 16), práh obnovy těchto skupin (1 až 16) tzn. kolik je potřeba obnovených skupin k úspěšnému obnovení HD Peněženky. Dále se pokračuje nastavením jednotlivých skupin tzn. kolik dílů (sharů, 1 až 16) bude daná skupina mít a kolik těchto dílů (sharů, 1 až 16) stačí k obnovení dané skupiny.

V samotném SLIP-0039 se vyskytuje tento případ:

Jsou vytvořeny celkem **4** skupiny (**A, B, C a D**) a práh obnovy skupin je nastaven na **2** neboli **2/4** = obnovení kterýchkoli 2 skupin ze 4 stačí k obnově této HD Peněženky.

Skupina **A** je nastavena jako **1/1** (celkem 1 díl, k obnově stačí 1).

Skupina **B** je nastavena stejně, tedy shamirovo schéma **1/1**.

Skupina **C** je **3/5** (5 dílů, kde 3 stačí k obnově) a

skupina **D** je **2/6** (6 dílů, kde 2 stačí k obnově).

**Rozdělení dílů** je zde uvažováno takto:

skupiny A a B (tzn. 1 a 1 díl) si nechá majitel peněženky u sebe, díly skupiny C rozdává mezi přátele a díly skupiny D rozdává rodinným příslušníkům, čímž diverzifikuje riziko ztráty Peněženky a zároveň je dostatečně ochráněn proti vykradení, protože by se museli domluvit 3 přátelé se 2 rodinnými příslušníky. Ale tito o sobě vůbec nemusí vědět a tak je jejich domluva vysoce nepravděpodobná.

K obnově HD Peněženky s tímto konkrétním nastavením Super Shamir schématu existuje celkem 6 kombinací a potřebujete tedy obnovit:

**A + B,**

**A + C,**

**A + D,**

**B + C,**

**B + D** nebo

**C + D**



díly z jedné skupiny se při obnově nedají použít v jiné skupině tzn. že například pro obnovu skupiny C nemůžeme použít 2 díly z ní a 1 díl ze skupiny D