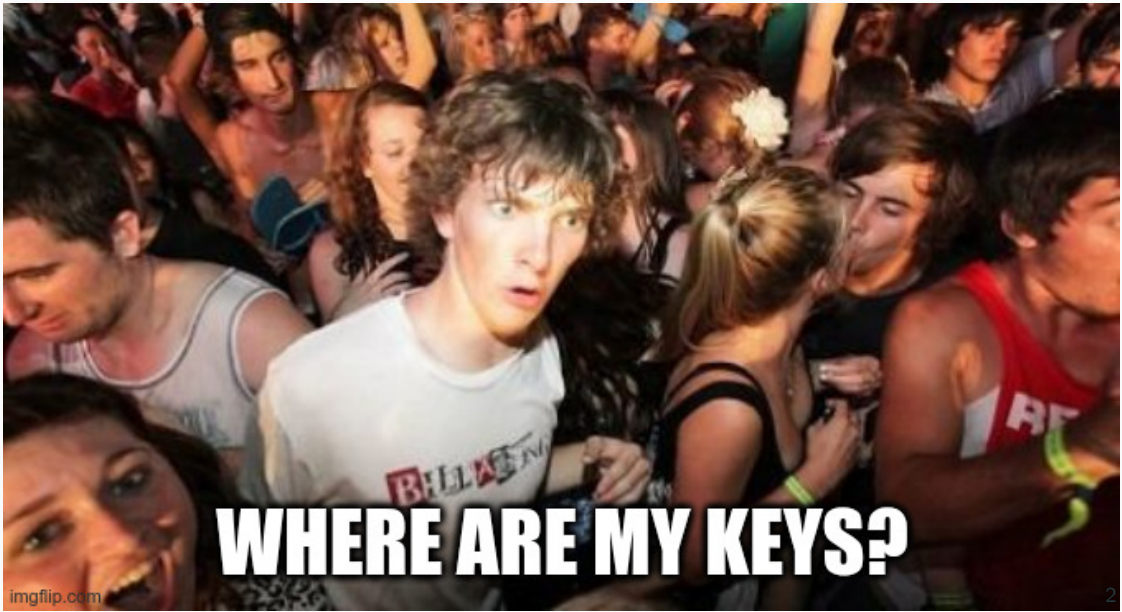
# USBKey

Karel Kočí

7.10.2023


WHERE ARE MY KEYS?
imgflip.com

# Požadavky

- Jednoduché ovládání
- Minimum hesel
- Stále k dispozici
- Zálohované
- Práce na více počítačích
- Možnost umístit soubory nespravované nástrojem
- Nezávislé na nastavení systému (FAT)
- Nenahradit pass

# První implementace

- 200 řádek kódu v Bash
- Podpora OpenVPN a SSH
- Synchronizace pomocí Rsync
- Hardcoded UUID mých klíčenek

```
#!/bin/sh
set -e
UUID_KKEY="a960e5b8-364f-4604-9d1b-f4f6407a0330"
UUID_WKEY="9fcaf42a-86d5-4e70-828d-fd90aad2d964"
CRYPT_NAME="usbkey"
MOUNT_PATH="/media/usbkey"
op_mount() {
        # First check if we have key drive
        if [ ! -e "/dev/disk/by-uuid/$UUID_KKEY" ]; then
```

# Nová implementace

- Rozšířitelná pomocí modulů
- Historie a synchronizace pomoci Git
- Konfigurační soubor
- Podpora dalších klíčů
- Zbytek požadavků stejných jako stará verze

# Pojďme na to

Minimální závislosti: bash, core-utils, util-linux, sudo, cryptsetup, exfat, git

```
$ git clone https://github.com/Cynerd/usbkey
$ ln -sf $PWD/usbkey/usbkey ~/.local/bin/usbkey
$ usbkey -h
Usage: usbkey [OPTION].. OPERATION ..
USB key manager
...
$ truncate -s 1G usbkey.img
$ sudo losetup -Pf usbkey.img
$ lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINTS
loop0         7:0    0     1G  0 loop
$ usbkey format /dev/loop0
```

# Přistupujeme

```
$ lsblk --fs
NAME        FSTYPE      FSVER LABEL UUID                                 FS
loop0       crypto_LUKS 2           76dfcb49-343f-4601-aa04-bf749464db1b
$ echo 'uuid_keys+=( "76dfcb49-343f-4601-aa04-bf749464db1b" )' > ~/.usbkey
$ usbkey mount
$ ls -a /media/usbkey/
.  ..  .git
$ usbkey umount
$ usbkey git status
```

# SSH

```
$ usbkey mount
$ usbkey ssh -n test
Comment: Some
...
$ ls /media/usbkey/ssh
test  test.pub
$ usbkey git log
$ usbkey ssh test
$ ls ~/.ssh
test  test.pub
```

# Synchronizace

```
$ truncate -s 1G usbkey_back.img
$ sudo losetup -Pf usbkey_back.img
$ usbkey format /dev/loop1
$ echo 'uuid_keys+=( "76dfcb49-343f-4601-aa04-bf749464db1b" )' >> ~/.usbkey
$ usbkey sync
$ usbkey umount
$ sudo losetup -d /dev/loop0
$ usbkey mount
```

# Syncthing

```
$ usbkey syncthing -n test
$ ls /media/usbkey/syncthing/test/
cert.pem  deviceid  key.pem
$ usbkey syncthing test
$ usbkey syncthing -p test
AKXQ23B-XLB7W55-TIV4GD6-L2XYHNT-KHBQNY6-CZG7UCX-XIWHI4X-QSTL3QR
```

# Wireguard

```
$ usbkey wireguard -n test
$ ls /media/usbkey/wireguard/test/
key  pub
$ usbkey wireguard -p test
JAK2lKo7mFBS86zb83IO2UNHrZvYXKMz8UgicS8eMh0=
$ usbkey wireguard -s test
cCnFVNaMFJkNvPWEZwUYHJzKKlp3Ed44fqJxmhGc+kY=
$ usbkey wireguard -ng home test
$ usbkey wireguard -eg home test
6Vsz5f40pAkre59BrfTH80+Rx0rjEmcMJPMFHMHdmCA=
```

# OpenVPN

```
$ usbkey openvpn -n test
$ usbkey openvpn test
$ ls openvpn-test
ca.crt  test.crt  test.key
$ usbkey openvpn -s servrik
```

# pass (passwordstore)

```
$ usbkey pass -u
$ ls /media/usbkey
openvpn  ssh  syncthing  wireguard
$ usbkey gitg
```

# GPG

```
$ usbkey gpg -n
$ ls /media/usbkey/gpg
59AC9766C3CDD8059699F2B57EB58B6FEC61207C.key
```

# Bezpečnost

- Při propojení má ke klíčům přístup root a celý uživatelský účet
- Klíče se importují na počítač bez hesla
- Vše je pod jedním heslem
- Certifikáty na 50 let
- USBKey není jediná cesta jak data zpřístupnit

# Závěr

- ~1500 řádek v Bashi
- Podpora SSH, GPG, OpenVPN, Wireguard, Syncthing, Pass
- Uložené na discích šifrovaných pomocí LUKS a exFAT
- Možnost přidávat další moduly

`https://gitlab.com/cynerd/usbkey`

Děkuji za pozornost.

`git.cynerd.cz`

`https://gitlab.com/cynerd`