ssh & git made easy w/ fido2

Luke Burciu

DevOps Engineer, Versent

problem statement

- When I use git + ssh across different environments - how can I remain secure, contribute to open source and protect my accounts?

currently:

- I use github
- I store my keys locally
- I work w/ different customers, w/ different security maturities
- i have a fido2 key (yubikey)

background

- different methods exist for managing ssh keys

1 - ssh-keygen (rsa / ecdsa / ed25519)

- **convenience** w/ a risk of key exposure
  - initial setup effort
  - mismanagement is a risk
  - revoking is a big task

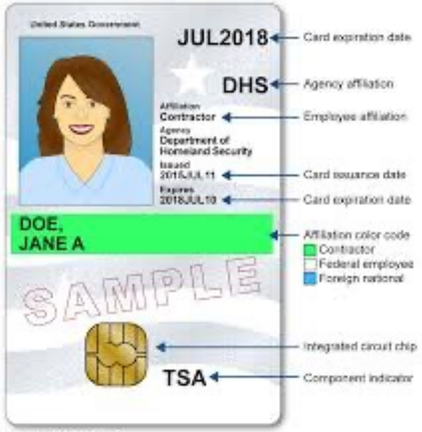
```
# creating a new key
$ ssh-keygen -t rsa -b 4096 –f ~/.ssh/id_rsa
$ ssh-copy-id -i ~/.ssh/id_rsa user@host
$ ssh user@host
```

2 – PIV & SSH User Certificates

- great for orgs w/ existing PKI

but..

- not zero trust
- costly to manage



Source: GAO. | GAO-19-130

3 - DrDuh’s Yubikey-Guide

secured by a:

- non-exportable GPG key
- physical touch requirement

limited by:

- set up requirements (took me hours)
- liveboot recommended for key generation
- requires a yubikey

4 – FIDO2 + SSH

A new way to go about it:

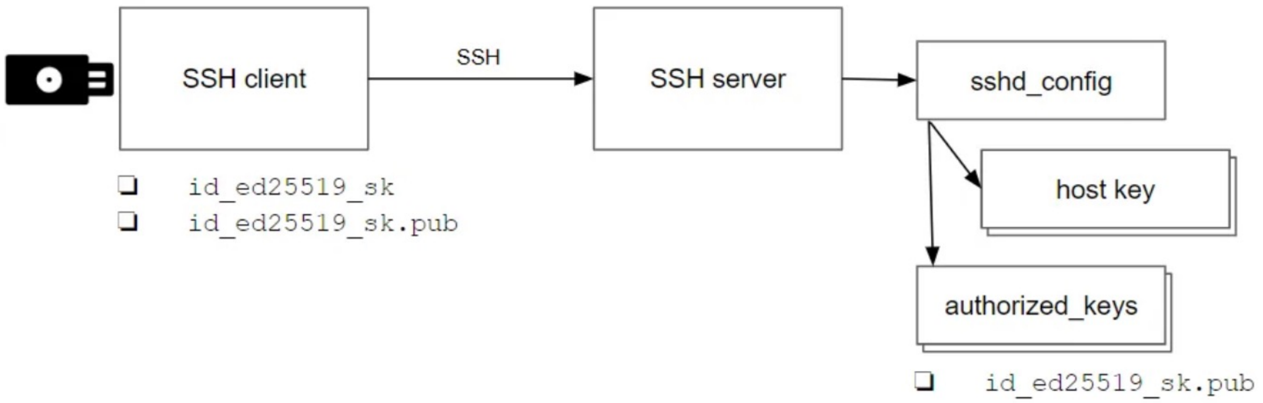
- OpenSSH now supports FIDO2
- 2 new encryption algos
  - ed25519-sk
  - ecdsa-sk
  - [-sk] = security key
- Different options
  - resident
  - non-resident

fido ALLIANCE

4 – FIDO2 + SSH

Under the hood

- direct generation from a security key via fido2
  - 1x public key
  - 1x “private key”
    - effectively a reference to the security key



4- FIDO2 + SSH

benefits

- requires physical touch and/or a pin
- supports any fido2 device
- different keypairs for different services
- portable or non-portable ssh keys
- more than just webauthn/passkeys

4 – FIDO2 + SSH

naïve approach

- via ssh-keygen

```
# creating a new key
$ ssh-keygen -t ”ed25519-sk" -f ”~/.ssh/ed25519-sk.pub" -C ”My Key"
```

4 – FIDO2 + SSH

how I do it

- via keycutter:
  - https://github.com/bash-my-aws/keycutter

DEMO

more reading…

- https://fy.blackhats.net.au/blog/2023-02-02-how-hype-will-turn-your-security-key-into-junk/
- https://www.openssh.com/agent-restrict.html
- https://developers.yubico.com/SSH/Securing_SSH_with_FIDO2.html
- https://github.com/bash-my-aws/keycutter