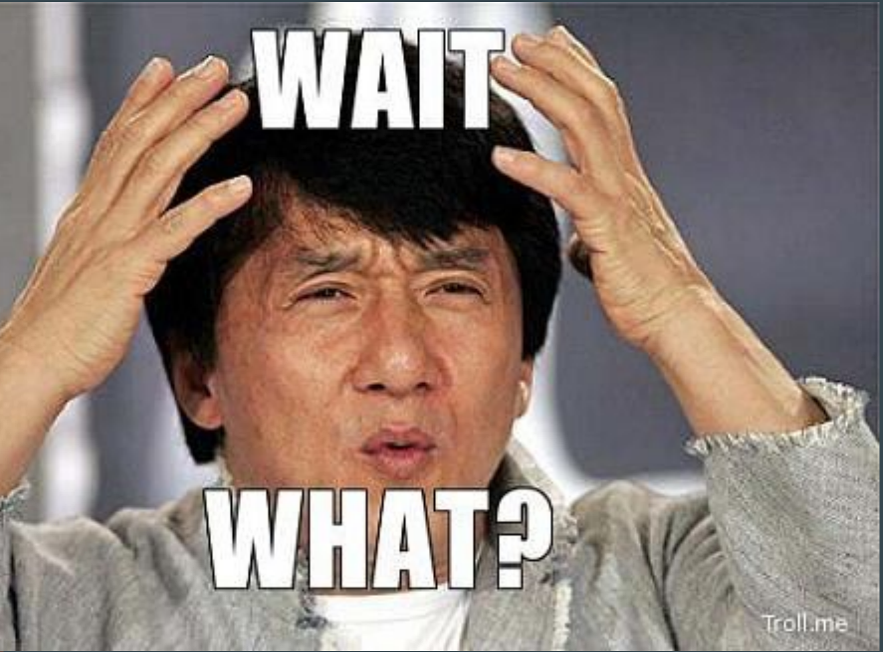
Security i praktyczne zastosowanie fizycznych kluczy bezpieczeństwa

•••

Mniej więcej ...

CLICKBAIT
CLICKBAIT EVERYWHERE!
made on imgur


WAIT
WHAT?
Troll.me

Trochę o mnie

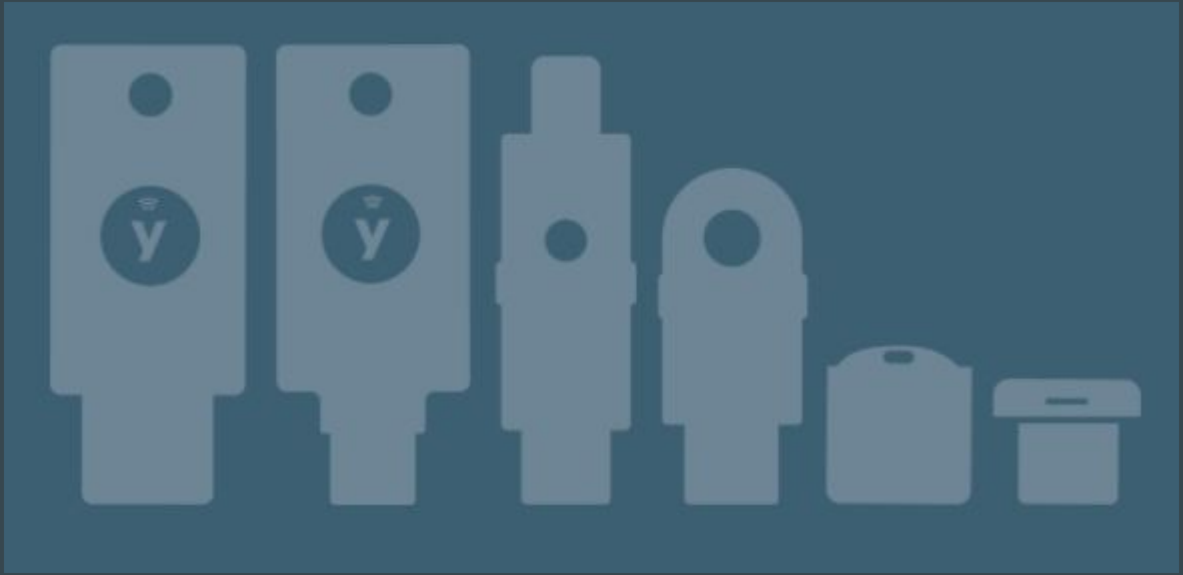
www.linkedin.com/in/maciej-listos

maciej.listos@gmail.com

Billennium

CYBER THREAT
PREVENTION
memes.com

Czym jest Yubikey?



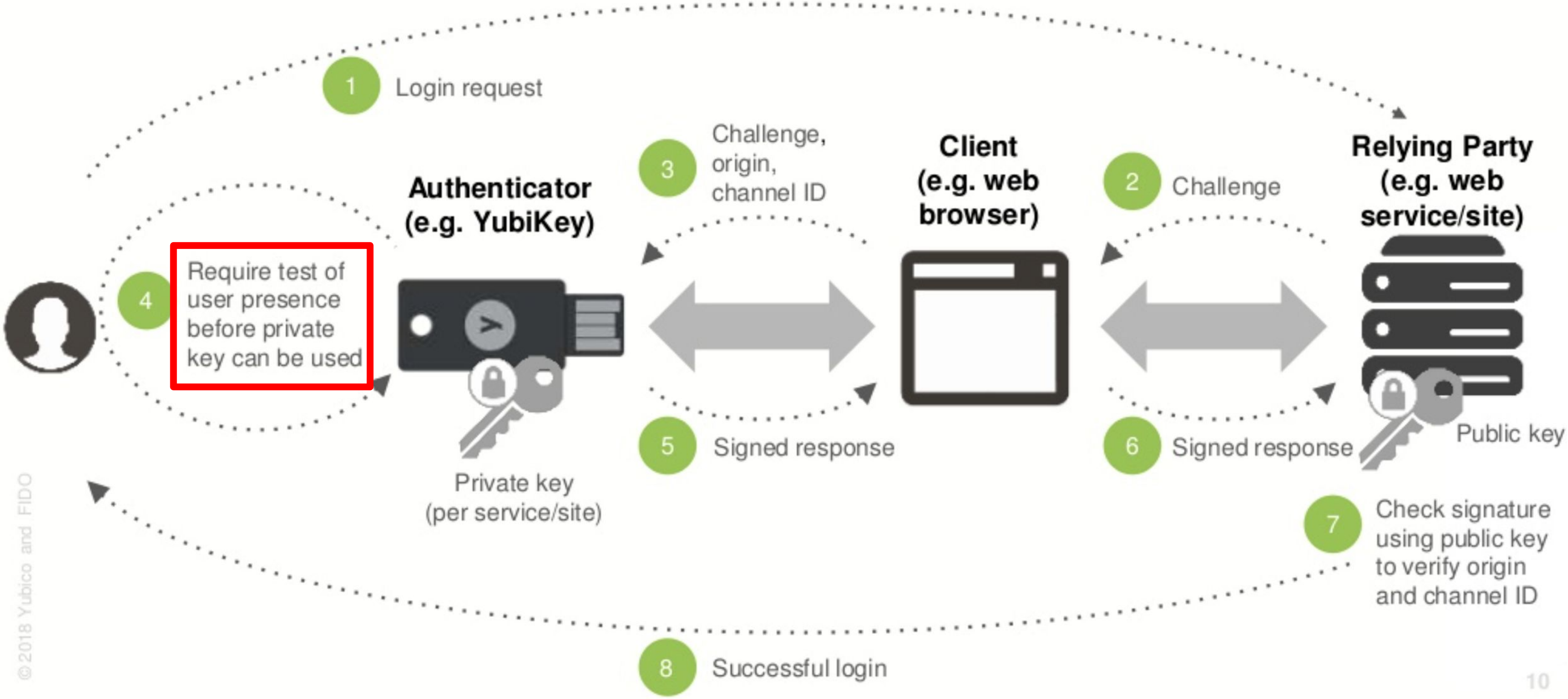
Wersja podstawowa

- Works out of the box with Gmail, Facebook, and hundreds more
- Supports FIDO2/WebAuthn, U2F
- Dust tight and water submersible
- Single key pricing starts at $20

Wersja rozszerzona

- Multi-protocol support; FIDO2/WebAuthn, U2F, Smart card, OpenPGP, OTP
- USB-A, USB-C, NFC, Lightning
- IP68 rated: dust tight and water submersible
- Single key pricing starts at $45
- Now available YubiKey 5C NFC with USB-C and NFC all-in-one to secure online accounts on mobile and desktops

How FIDO Authentication Works



1 Login request

2 Challenge

3 Challenge, origin, channel ID

4 Require test of user presence before private key can be used

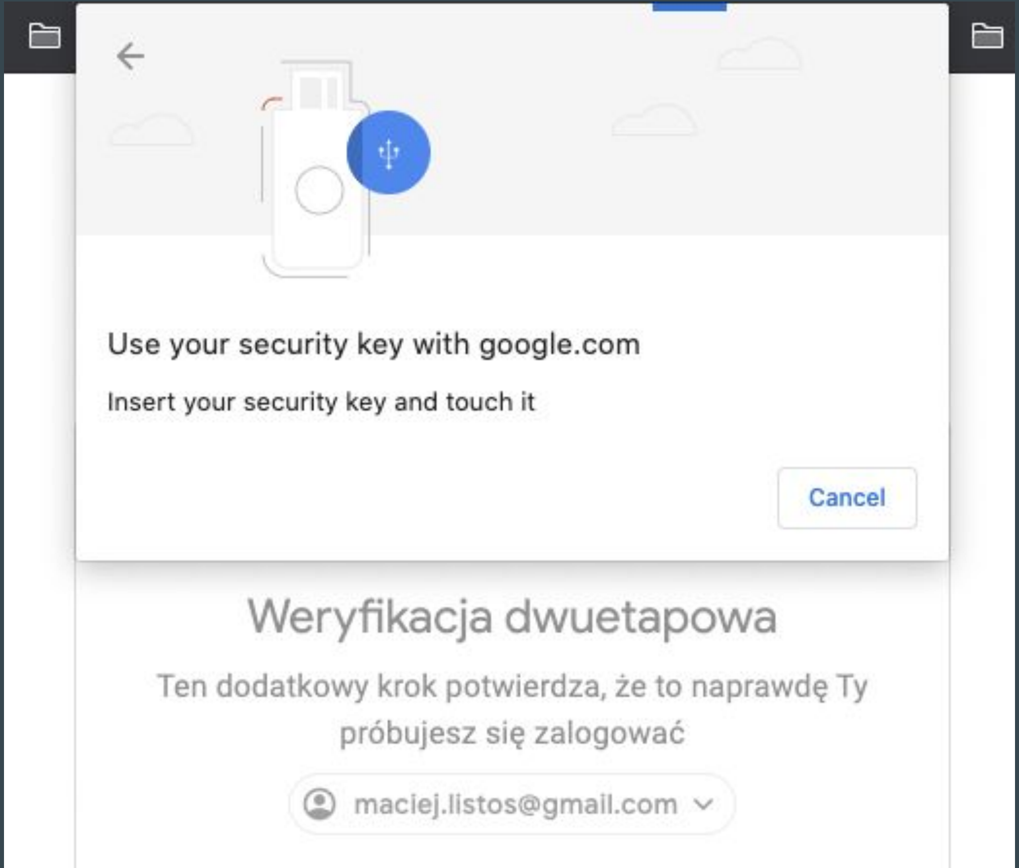
5 Signed response

6 Signed response

7 Check signature using public key to verify origin and channel ID

8 Successful login

FIDO w akcji



Use your security key with google.com

Insert your security key and touch it

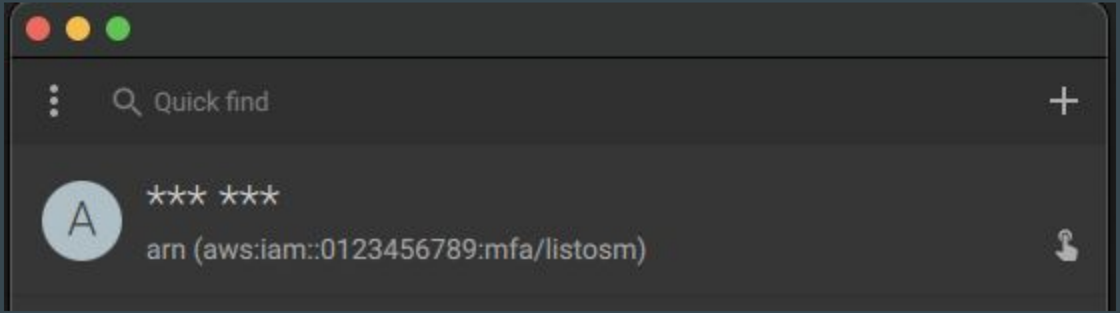
Weryfikacja dwuetapowa

Ten dodatkowy krok potwierdza, że to naprawdę Ty próbujesz się zalogować

maciej.listos@gmail.com

Yubico Authenticator

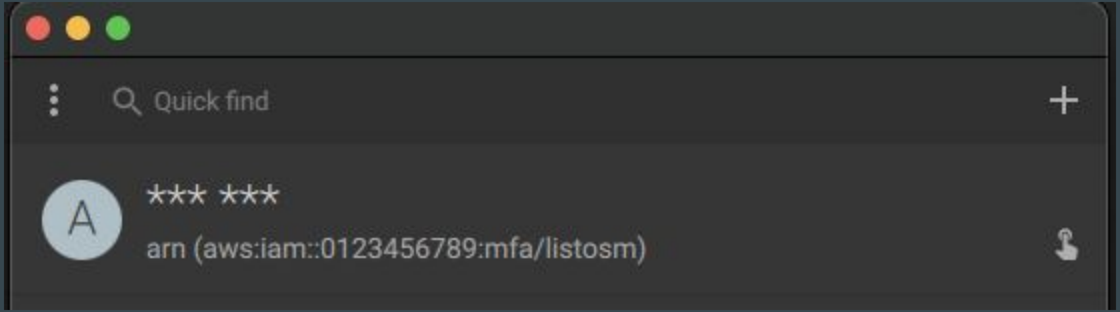
Dedykowana aplikacja do TOTP



*** ***

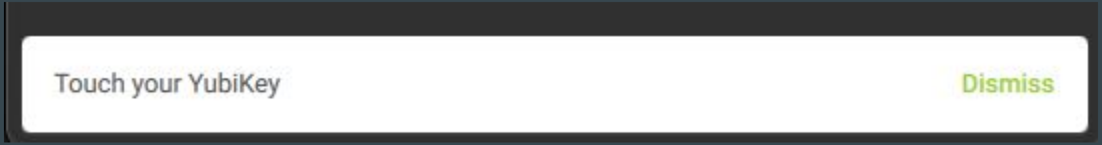
arn (aws:iam::0123456789:mfa/listosm)

Dedykowana aplikacja do TOTP



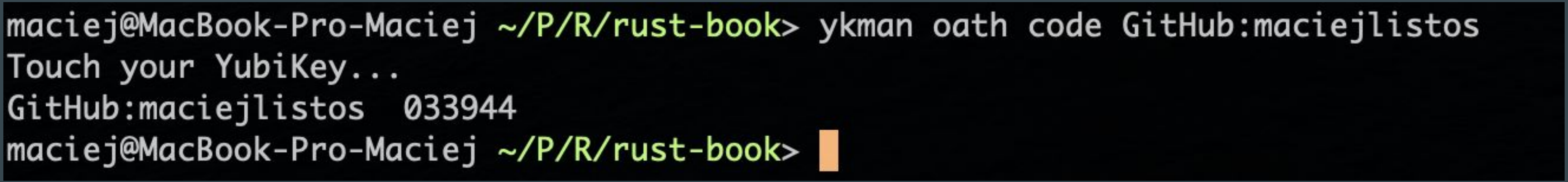
*** ***

arn (aws:iam::0123456789:mfa/listosm)



Touch your YubiKey

Działa również z command line

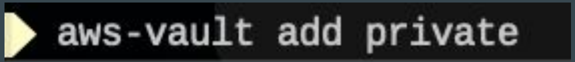


```
maciej@MacBook-Pro-Maciej ~/P/R/rust-book> ykman oath code GitHub:maciejlistos
Touch your YubiKey...
GitHub:maciejlistos  033944
maciej@MacBook-Pro-Maciej ~/P/R/rust-book> 
```

aws-vault

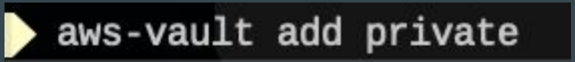
- integruje się z systemowymi serwisami do przechowywania haseł
- wsparcie dla MFA
- łatwy w obsłudze

aws-vault

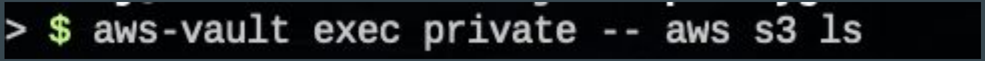


```
aws-vault add private
```

aws-vault

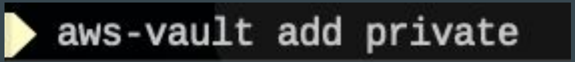


```
aws-vault add private
```

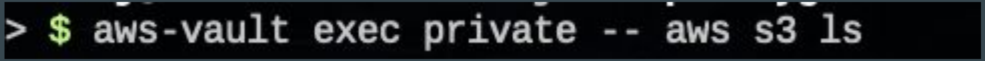


```
> $ aws-vault exec private -- aws s3 ls
```

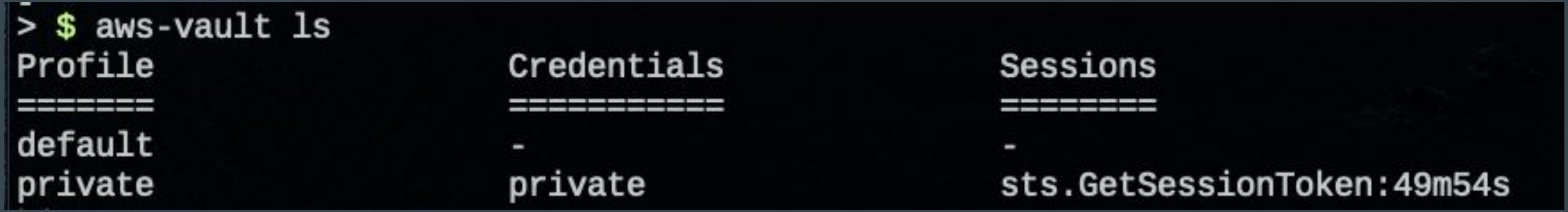
aws-vault



```
aws-vault add private
```

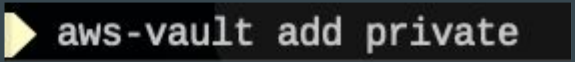


```
> $ aws-vault exec private -- aws s3 ls
```

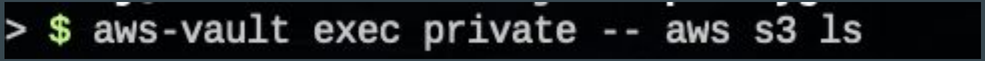


```
> $ aws-vault ls
Profile                  Credentials              Sessions
=======                  ===========              ========
default                  -                        -
private                  private                  sts.GetSessionToken:49m54s
```

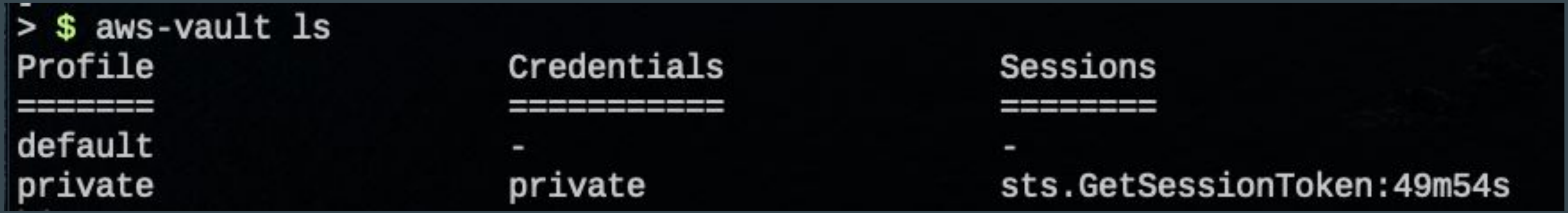
aws-vault



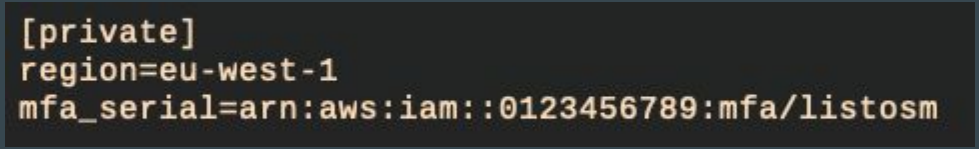
```
aws-vault add private
```



```
> $ aws-vault exec private -- aws s3 ls
```

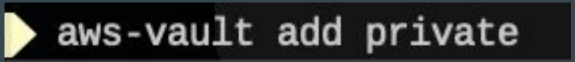


```
> $ aws-vault ls
Profile                    Credentials               Sessions
=======                    ===========               ========
default                    -                         -
private                    private                   sts.GetSessionToken:49m54s
```

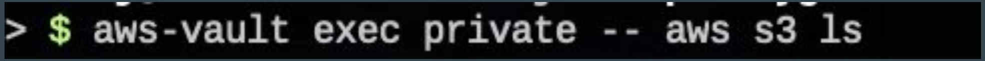


```
[private]
region=eu-west-1
mfa_serial=arn:aws:iam::0123456789:mfa/listosm
```

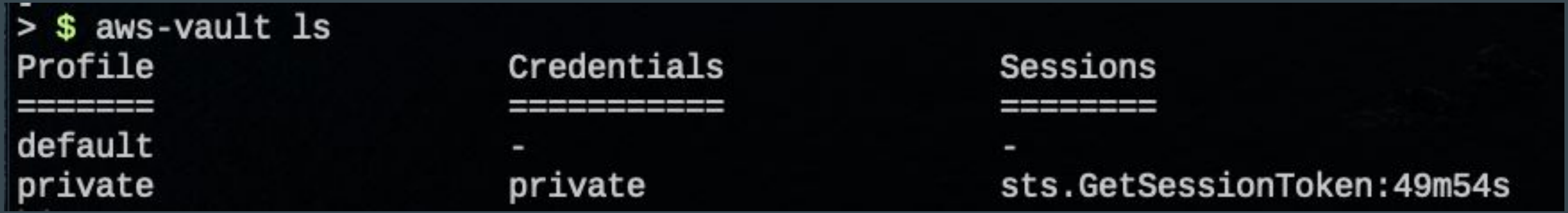
aws-vault



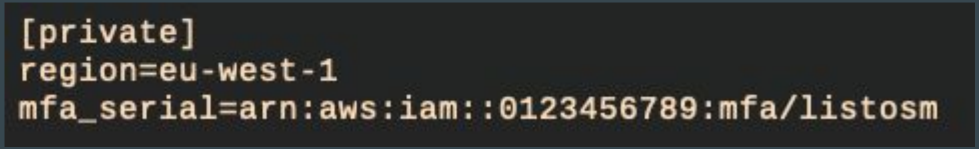
```
aws-vault add private
```



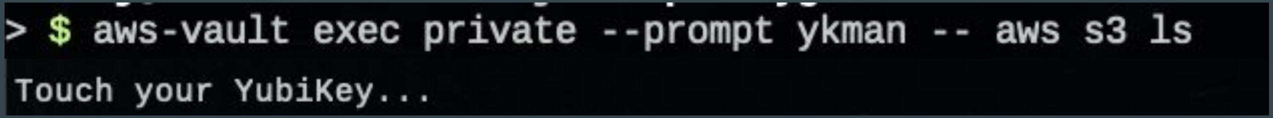
```
> $ aws-vault exec private -- aws s3 ls
```



```
> $ aws-vault ls
Profile                  Credentials              Sessions
=======                  ===========              ========
default                  -                        -
private                  private                  sts.GetSessionToken:49m54s
```

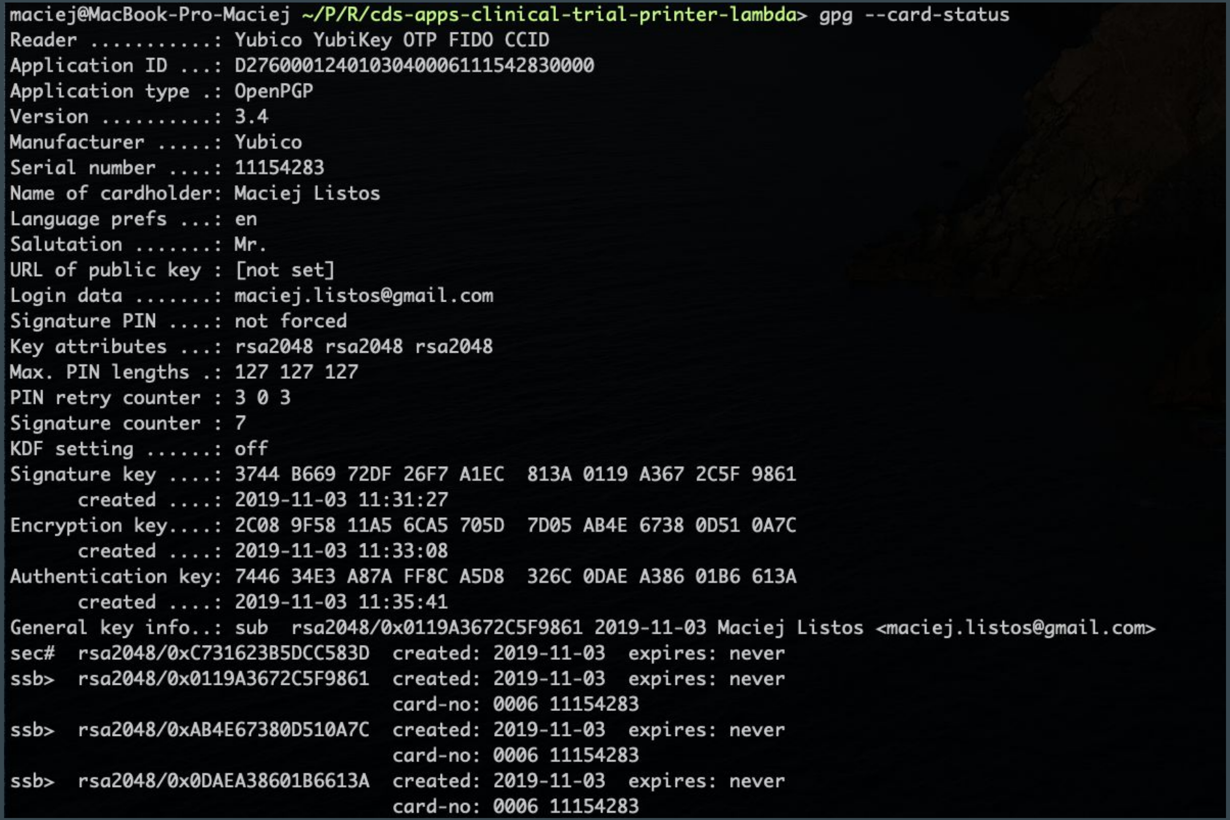


```
[private]
region=eu-west-1
mfa_serial=arn:aws:iam::0123456789:mfa/listosm
```



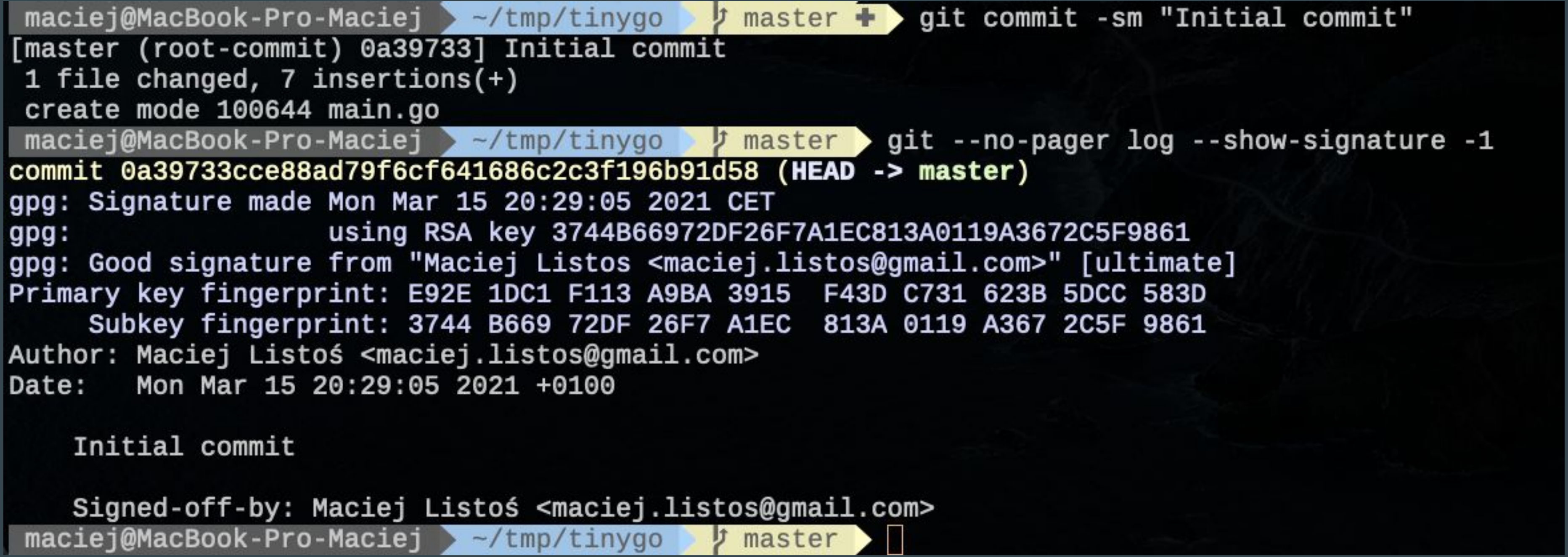
```
> $ aws-vault exec private --prompt ykman -- aws s3 ls
Touch your YubiKey...
```

SmartCard



```
maciej@MacBook-Pro-Maciej ~/P/R/cds-apps-clinical-trial-printer-lambda> gpg --card-status
Reader ...........: Yubico YubiKey OTP FIDO CCID
Application ID ...: D2760001240103040006111542830000
Application type .: OpenPGP
Version ..........: 3.4
Manufacturer .....: Yubico
Serial number ....: 11154283
Name of cardholder: Maciej Listos
Language prefs ...: en
Salutation .......: Mr.
URL of public key : [not set]
Login data .......: maciej.listos@gmail.com
Signature PIN ....: not forced
Key attributes ...: rsa2048 rsa2048 rsa2048
Max. PIN lengths .: 127 127 127
PIN retry counter : 3 0 3
Signature counter : 7
KDF setting ......: off
Signature key ....: 3744 B669 72DF 26F7 A1EC  813A 0119 A367 2C5F 9861
      created ....: 2019-11-03 11:31:27
Encryption key....: 2C08 9F58 11A5 6CA5 705D  7D05 AB4E 6738 0D51 0A7C
      created ....: 2019-11-03 11:33:08
Authentication key: 7446 34E3 A87A FF8C A5D8  326C 0DAE A386 01B6 613A
      created ....: 2019-11-03 11:35:41
General key info..: sub  rsa2048/0x0119A3672C5F9861 2019-11-03 Maciej Listos <maciej.listos@gmail.com>
sec#  rsa2048/0xC731623B5DCC583D  created: 2019-11-03  expires: never
ssb>  rsa2048/0x0119A3672C5F9861  created: 2019-11-03  expires: never
                                  card-no: 0006 11154283
ssb>  rsa2048/0xAB4E67380D510A7C  created: 2019-11-03  expires: never
                                  card-no: 0006 11154283
ssb>  rsa2048/0x0DAEA38601B6613A  created: 2019-11-03  expires: never
                                  card-no: 0006 11154283
```

Integracja z git

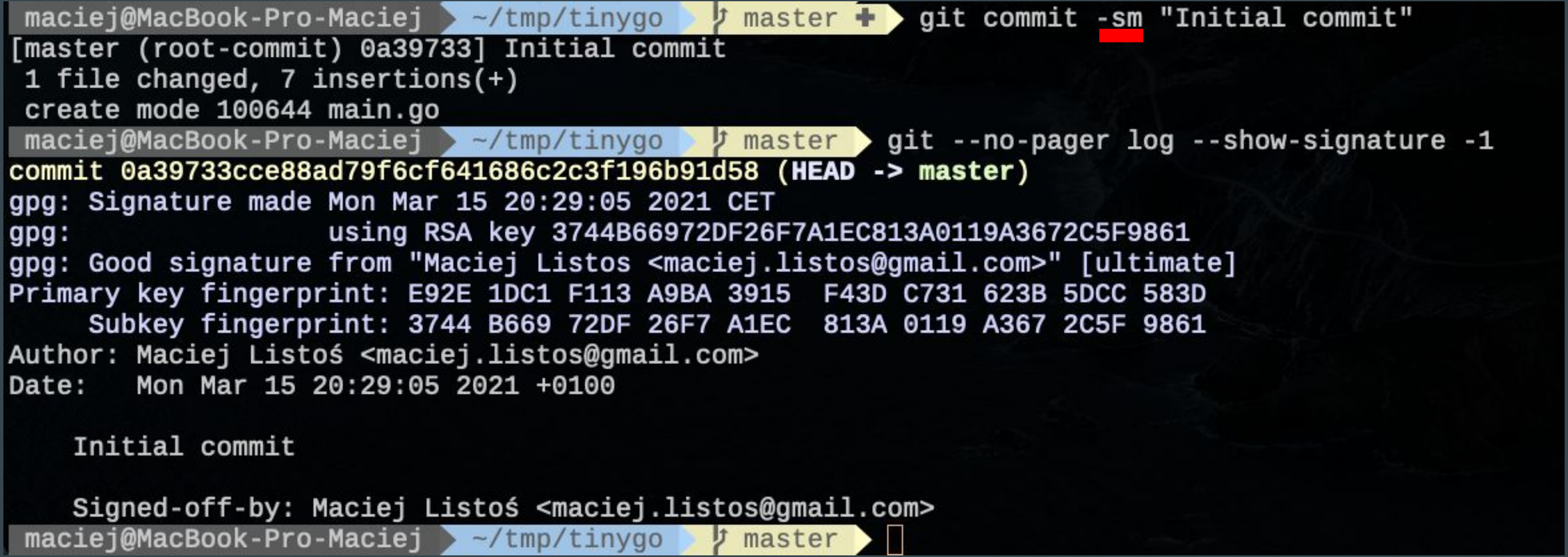


```
maciej@MacBook-Pro-Maciej  ~/tmp/tinygo  master ✚  git commit -sm "Initial commit"
[master (root-commit) 0a39733] Initial commit
 1 file changed, 7 insertions(+)
 create mode 100644 main.go
maciej@MacBook-Pro-Maciej  ~/tmp/tinygo  master  git --no-pager log --show-signature -1
commit 0a39733cce88ad79f6cf641686c2c3f196b91d58 (HEAD -> master)
gpg: Signature made Mon Mar 15 20:29:05 2021 CET
gpg:                using RSA key 3744B66972DF26F7A1EC813A0119A3672C5F9861
gpg: Good signature from "Maciej Listos <maciej.listos@gmail.com>" [ultimate]
Primary key fingerprint: E92E 1DC1 F113 A9BA 3915  F43D C731 623B 5DCC 583D
     Subkey fingerprint: 3744 B669 72DF 26F7 A1EC  813A 0119 A367 2C5F 9861
Author: Maciej Listoś <maciej.listos@gmail.com>
Date:   Mon Mar 15 20:29:05 2021 +0100

    Initial commit

    Signed-off-by: Maciej Listoś <maciej.listos@gmail.com>
maciej@MacBook-Pro-Maciej  ~/tmp/tinygo  master 
```

Integracja z git

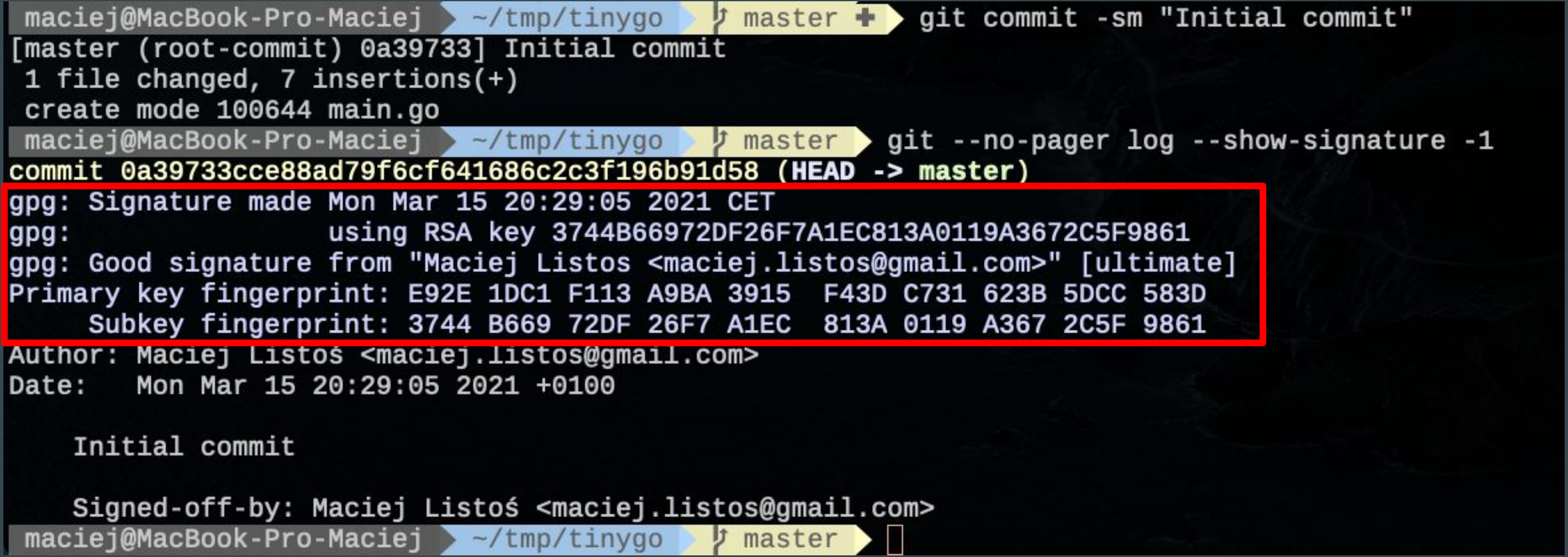


```
maciej@MacBook-Pro-Maciej  ~/tmp/tinygo  ⎇ master ✚  git commit -sm "Initial commit"
[master (root-commit) 0a39733] Initial commit
 1 file changed, 7 insertions(+)
 create mode 100644 main.go
maciej@MacBook-Pro-Maciej  ~/tmp/tinygo  ⎇ master  git --no-pager log --show-signature -1
commit 0a39733cce88ad79f6cf641686c2c3f196b91d58 (HEAD -> master)
gpg: Signature made Mon Mar 15 20:29:05 2021 CET
gpg:                using RSA key 3744B66972DF26F7A1EC813A0119A3672C5F9861
gpg: Good signature from "Maciej Listos <maciej.listos@gmail.com>" [ultimate]
Primary key fingerprint: E92E 1DC1 F113 A9BA 3915  F43D C731 623B 5DCC 583D
     Subkey fingerprint: 3744 B669 72DF 26F7 A1EC  813A 0119 A367 2C5F 9861
Author: Maciej Listoś <maciej.listos@gmail.com>
Date:   Mon Mar 15 20:29:05 2021 +0100

    Initial commit

    Signed-off-by: Maciej Listoś <maciej.listos@gmail.com>
maciej@MacBook-Pro-Maciej  ~/tmp/tinygo  ⎇ master 
```

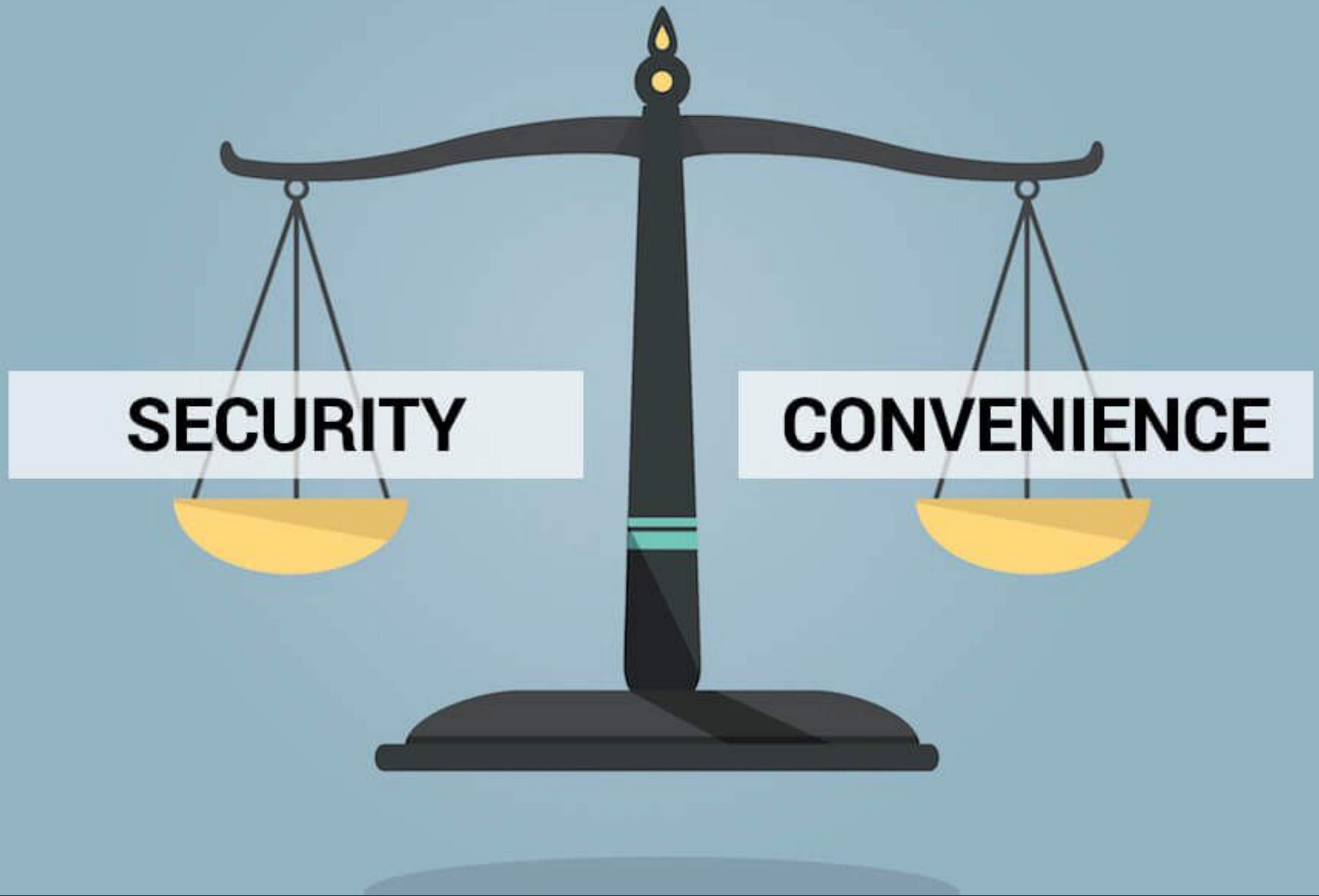
Integracja z git

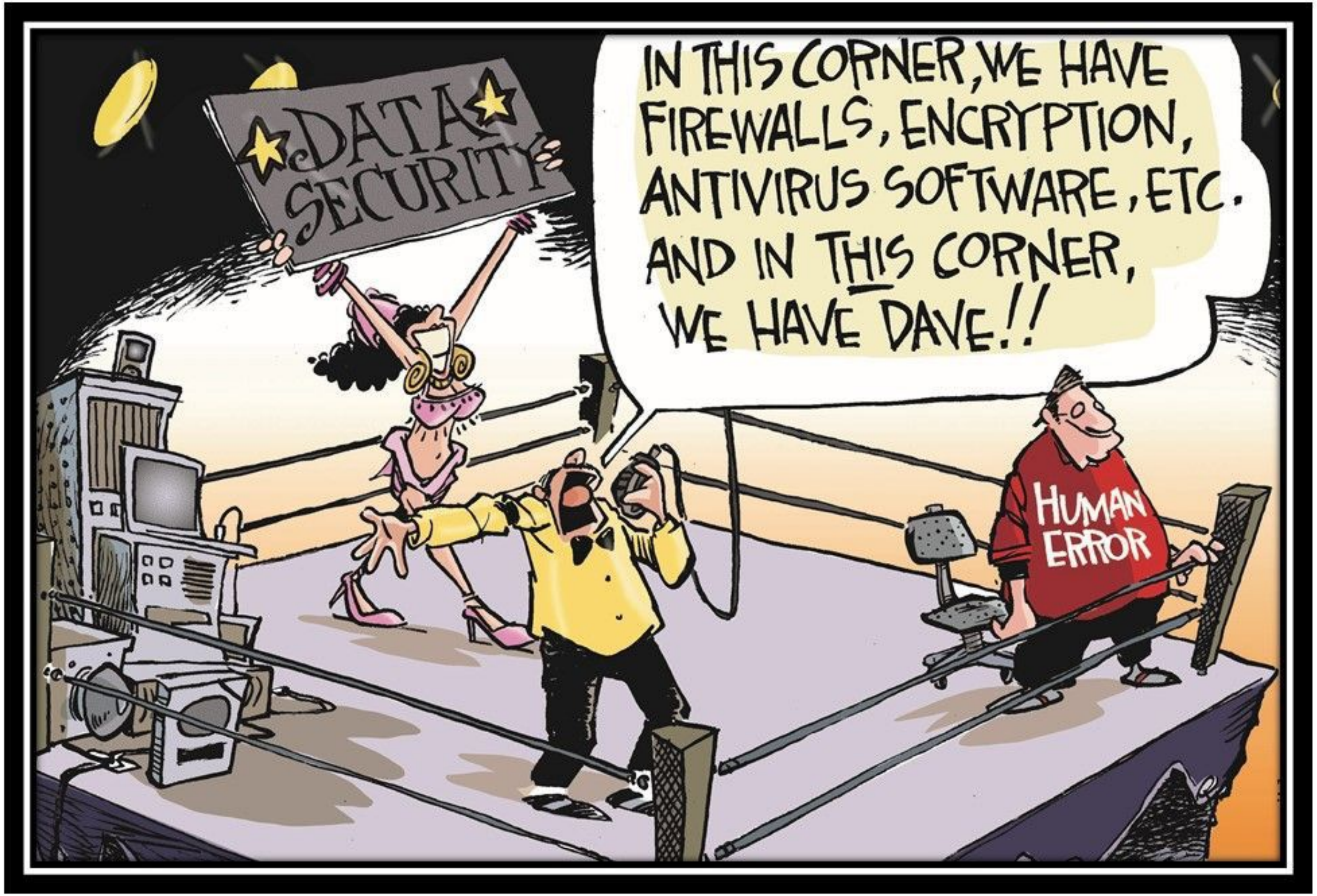


```
 maciej@MacBook-Pro-Maciej  ~/tmp/tinygo   master ✚  git commit -sm "Initial commit"
[master (root-commit) 0a39733] Initial commit
 1 file changed, 7 insertions(+)
 create mode 100644 main.go
 maciej@MacBook-Pro-Maciej  ~/tmp/tinygo   master  git --no-pager log --show-signature -1
commit 0a39733cce88ad79f6cf641686c2c3f196b91d58 (HEAD -> master)
gpg: Signature made Mon Mar 15 20:29:05 2021 CET
gpg:                using RSA key 3744B66972DF26F7A1EC813A0119A3672C5F9861
gpg: Good signature from "Maciej Listos <maciej.listos@gmail.com>" [ultimate]
Primary key fingerprint: E92E 1DC1 F113 A9BA 3915  F43D C731 623B 5DCC 583D
     Subkey fingerprint: 3744 B669 72DF 26F7 A1EC  813A 0119 A367 2C5F 9861
Author: Maciej Listoś <maciej.listos@gmail.com>
Date:   Mon Mar 15 20:29:05 2021 +0100

    Initial commit

    Signed-off-by: Maciej Listoś <maciej.listos@gmail.com>
 maciej@MacBook-Pro-Maciej  ~/tmp/tinygo   master 
```


SECURITY
CONVENIENCE


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

Pomocne linki

- Yubikey i GPG - https://github.com/drduh/YubiKey-Guide
- GPG i SSH - https://www.edmundofuentes.com/blog/2018/06/27/yubikey-gpg-ssh/
- TOTP i Yubikey - https://developers.yubico.com/yubikey-manager/
- aws-vault i Yubikey - https://github.com/99designs/aws-vault/blob/master/USAGE.md#using-a-yubikey