



# 1E7

## Полный обзор Yubikey и passwordLess уже вчера и практическое использование + TPM

Andry + n0nvme

Andry - Independent researcher, EC1337, CyberProtect

n0nvme - Independent researcher, EC1337

Moscow, April 30, 2022

yubikey + gpg + ssh + otp + u2f(fido/fido2)  
(gpg instead ssl) + git + tpm



# Галопом по европе - или краткий экскурс по:

yubikey + gpg + ssh + otp + u2f(fido/fido2)  
(gpg instead ssl) + git



Без углубления в:

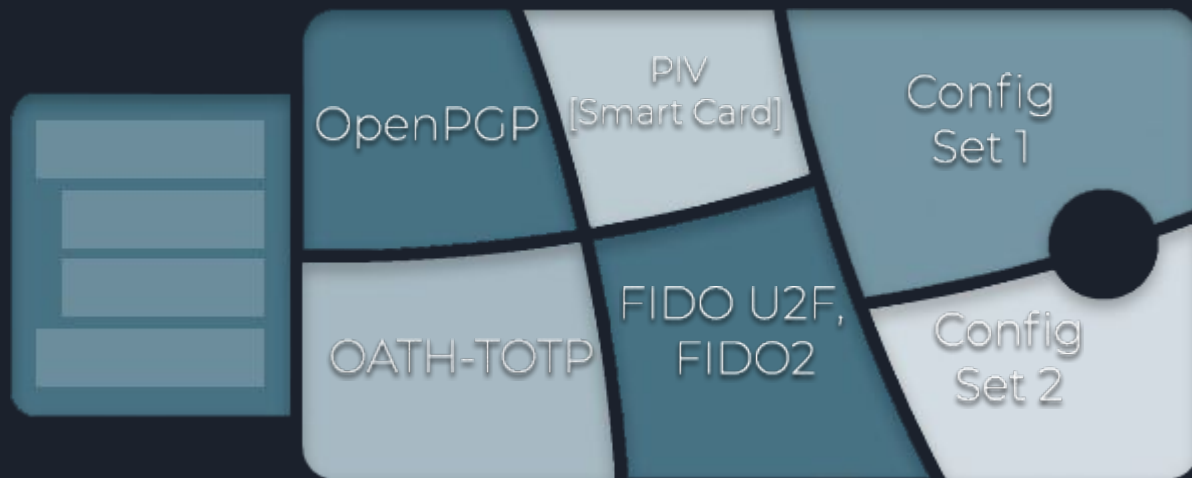
- Правовую часть
- Реализацию

# yubico & YubiKey

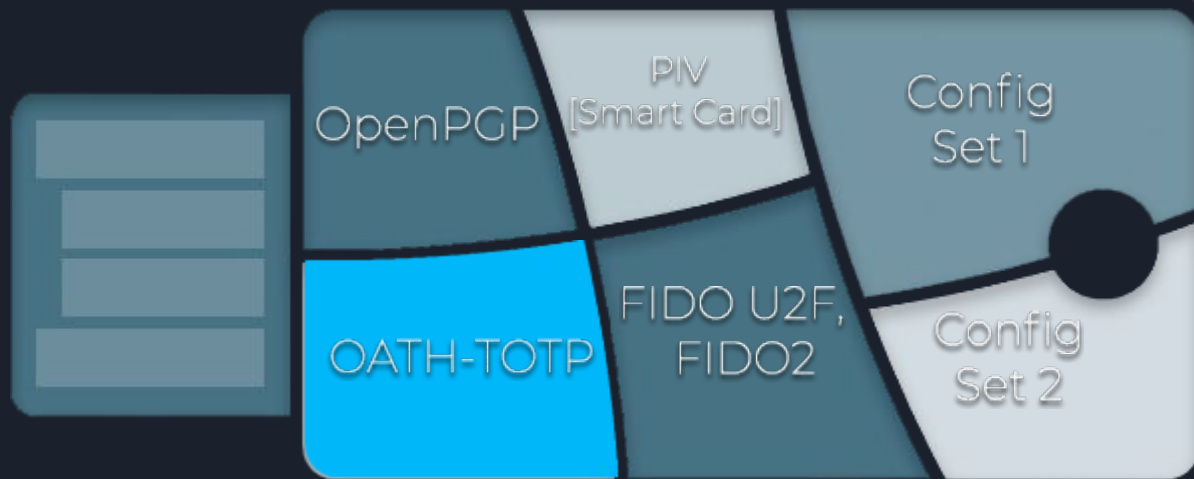
NO  
FF  
ONE  
2022



# План/Что мы сегодня узнаем



# OTP





10:00

LTE

Google Authenticator



Google (surfingfan@gmail.com)  
901 291



Google (hikingfan@gmail.com)  
473 498



NO  
FF  
ONE  
2022

# OTP - One-Time Password

HOTP - HMAC-Based One-Time Password

TOTP - Time - Based One-time Password





# HOTP - HMAC-Based One-Time Password Algorithm

HMAC - hash-based message authentication code

$$\text{HMAC} = \text{SHA-1}(\text{Text1} + \text{Text2})$$

# HOTP - HMAC-Based One-Time Password Algorithm



- Секретный ключ



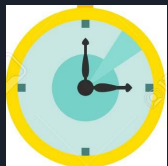
- Счётчик

$$\text{HOTP} = \text{HMAC}(\text{key} + \text{counter})$$

# TOTP - Time-based One-time Password Algorithm



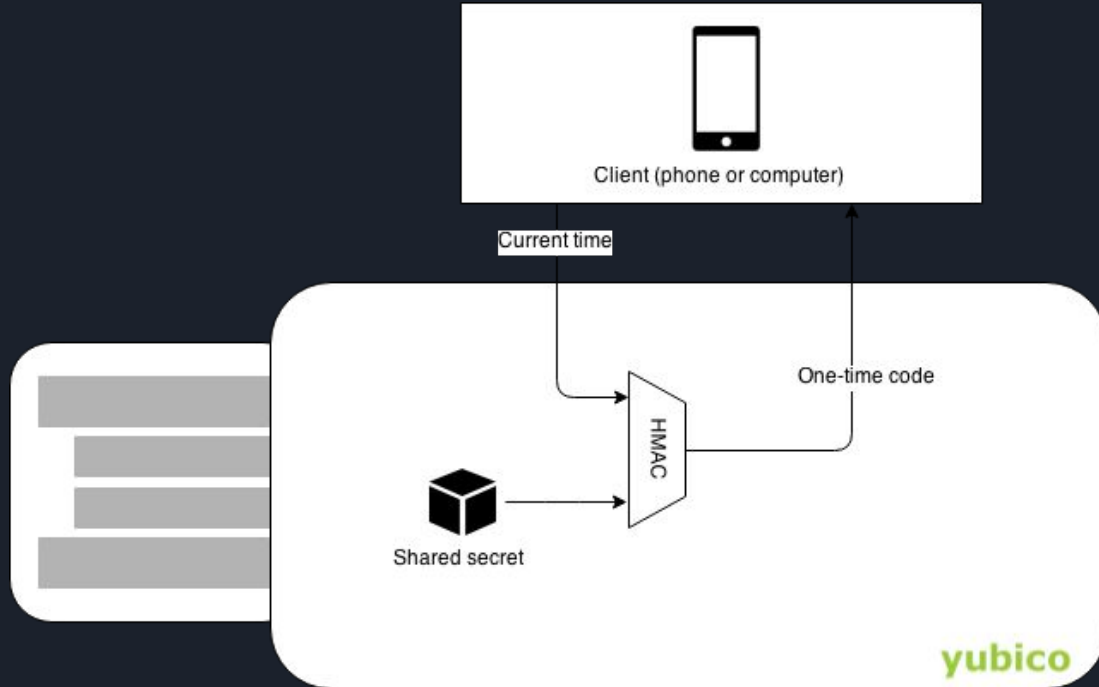
- Секретный ключ



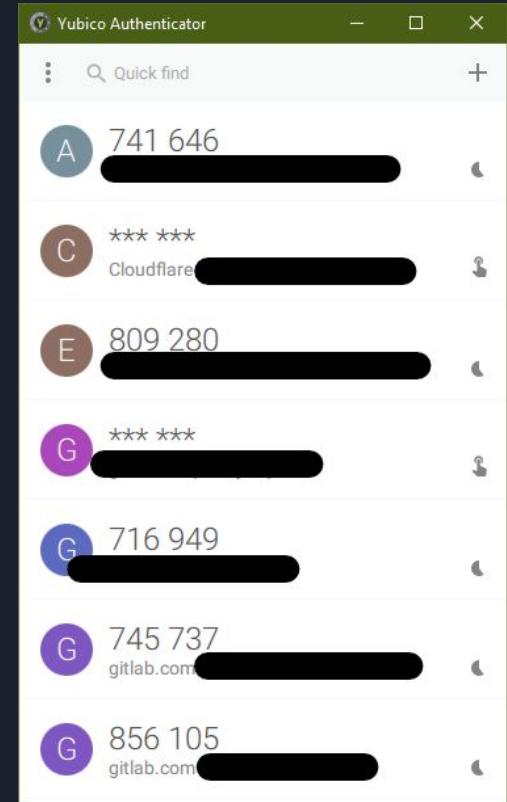
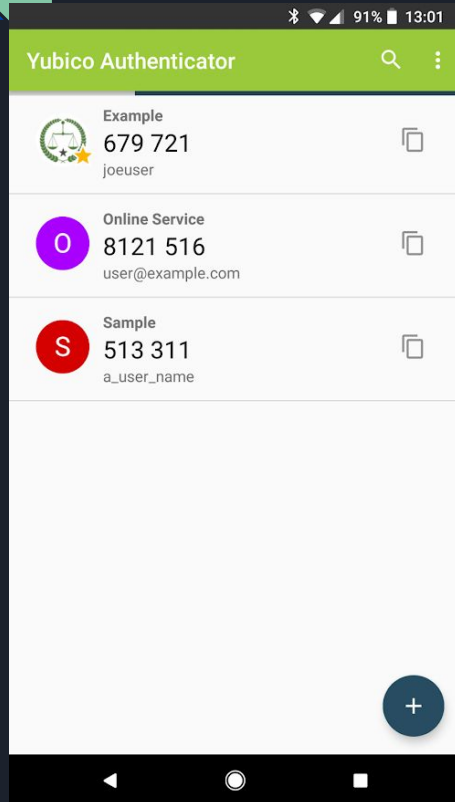
- Время

$$\text{TOTP} = \text{HMAC}(\text{key} + \text{time})$$

# TOTP

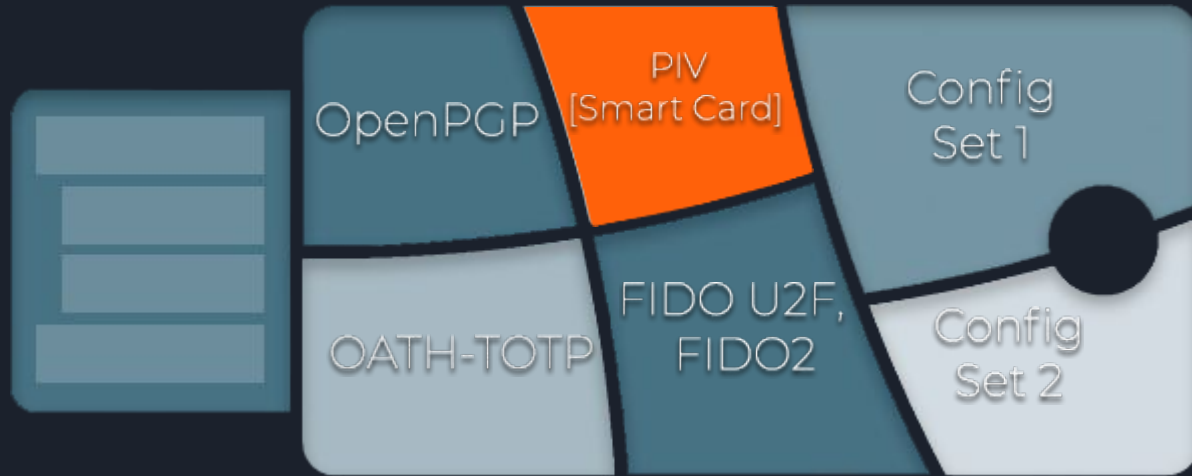


# Yubikey authenticator





# Smart Card



# Smart Card

Slot 9a: PIV Authentication

Slot 9c: Digital Signature

Slot 9d: Key Management

Slot 9e: Card Authentication

Slot 82-95: Retired Key Management





# Config slots



# Config slots

YubiKey Manager

YubiKey 4 [redacted] ? Help i About

**yubico** Home Applications Interfaces

## OTP

Home / OTP

### Short Touch (Slot 1)

This slot is configured

Delete Configure

↔ Swap

### Long Touch (Slot 2)

This slot is empty

Delete Configure

< Back

short press

Long press  
(3 sec)

# Config slots

**yubico** [Home](#) [Applications](#) [Interfaces](#)

---

## Select Credential Type

[Home](#) / [OTP](#) / Short Touch (Slot 1)

☒ Yubico OTP

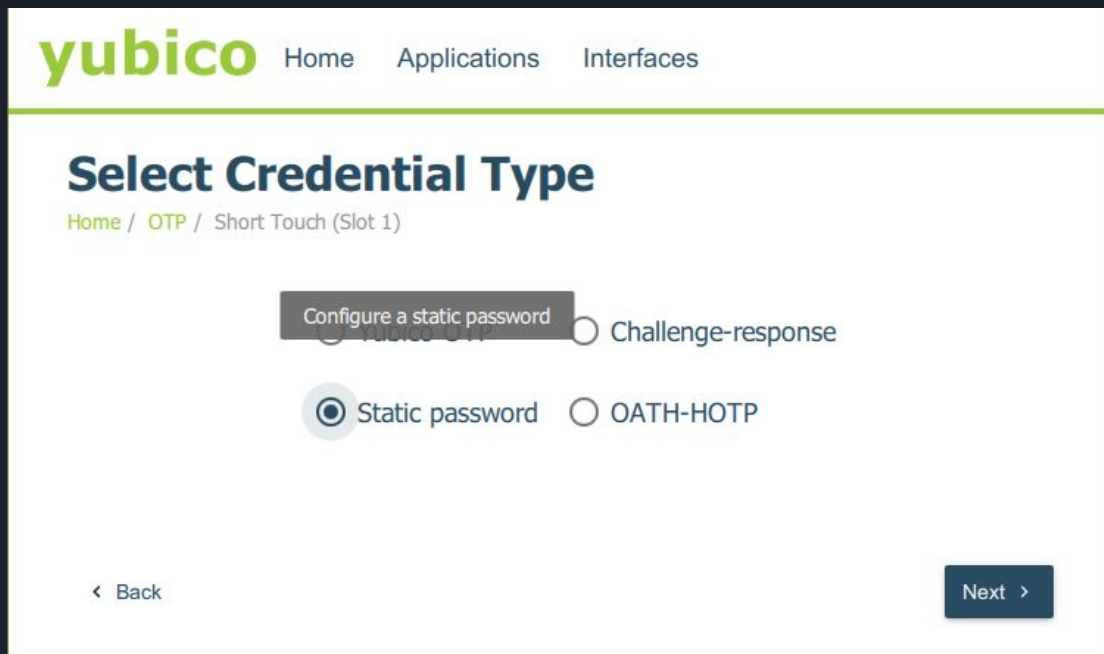
☐ Challenge-response

☐ Static password

☐ OATH-HOTP

OTP ≠ Yubico OTP

# Config slots



The screenshot shows the Yubico web interface. At the top, there is a navigation bar with the Yubico logo and links for Home, Applications, and Interfaces. Below this, the main heading is "Select Credential Type". A breadcrumb trail indicates the current path: Home / OTP / Short Touch (Slot 1). The interface presents two main options: "Configure a static password" and "Challenge-response". Under "Configure a static password", there are two sub-options: "Static password" (which is selected with a radio button) and "OATH-HOTP". At the bottom left, there is a "< Back" link, and at the bottom right, there is a "Next >" button.

yubico Home Applications Interfaces

## Select Credential Type

Home / OTP / Short Touch (Slot 1)

☒ Configure a static password ☐ Challenge-response

☒ Static password ☐ OATH-HOTP

< Back Next >



# Static Password



P|

# Config slots

**yubico** [Home](#) [Applications](#) [Interfaces](#)

---

## Select Credential Type

[Home](#) / [OTP](#) / Short Touch (Slot 1)

☐ Yubico OTP

☐ Challenge-response

☐ Static password

☒ OATH-HOTP

[< Back](#)

[Next >](#)

# OATH-HOTP

**yubico** [Home](#) [Applications](#) [Interfaces](#)

---

## OATH-HOTP

[Home](#) / [OTP](#) / [Short Touch \(Slot 1\)](#) / OATH-HOTP

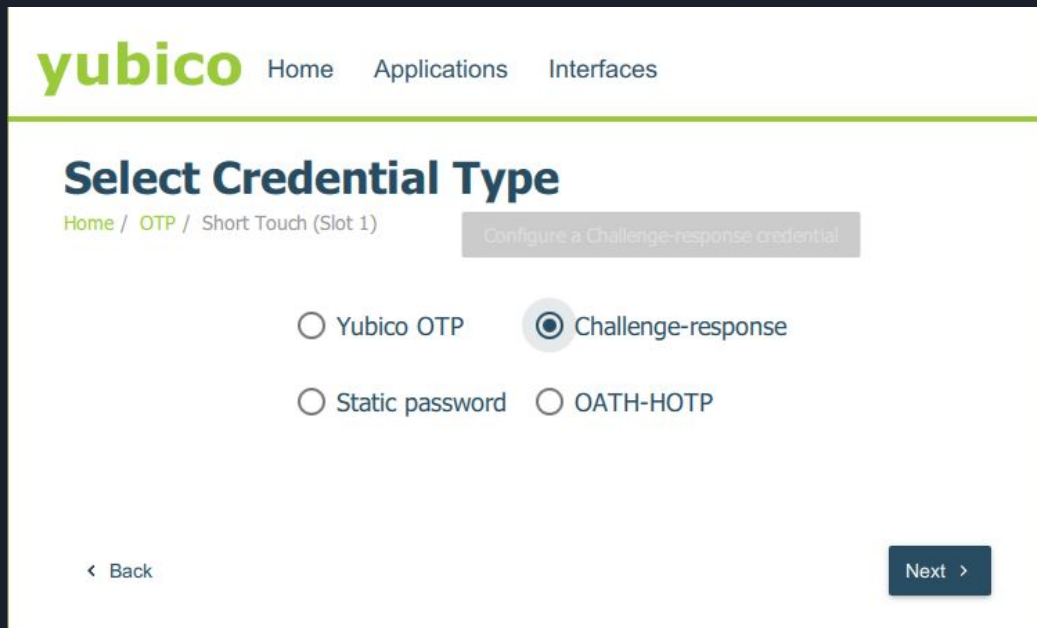
Secret key

Digits

[< Back](#) [✓ Finish](#)



# Config slots



The screenshot shows the Yubico web interface for configuring a slot. The header includes the Yubico logo and navigation links for Home, Applications, and Interfaces. The main heading is "Select Credential Type". Below it, a breadcrumb trail shows "Home / OTP / Short Touch (Slot 1)". A grey button labeled "Configure a Challenge-response credential" is visible. There are four radio button options: "Yubico OTP", "Challenge-response" (which is selected), "Static password", and "OATH-HOTP". At the bottom, there are "Back" and "Next" navigation buttons.

yubico Home Applications Interfaces

## Select Credential Type

Home / OTP / Short Touch (Slot 1)

Configure a Challenge-response credential

☐ Yubico OTP ☒ Challenge-response

☐ Static password ☐ OATH-HOTP

< Back

Next >



challenge-response

HMAC(  + challenge)

os authentication



# PAM (Pluggable Authentication Modules) - linux

yubikey as second factor (otp / Challenge-response / u2f / passwordless)

yubikey as second in ssh (otp / Challenge-response)

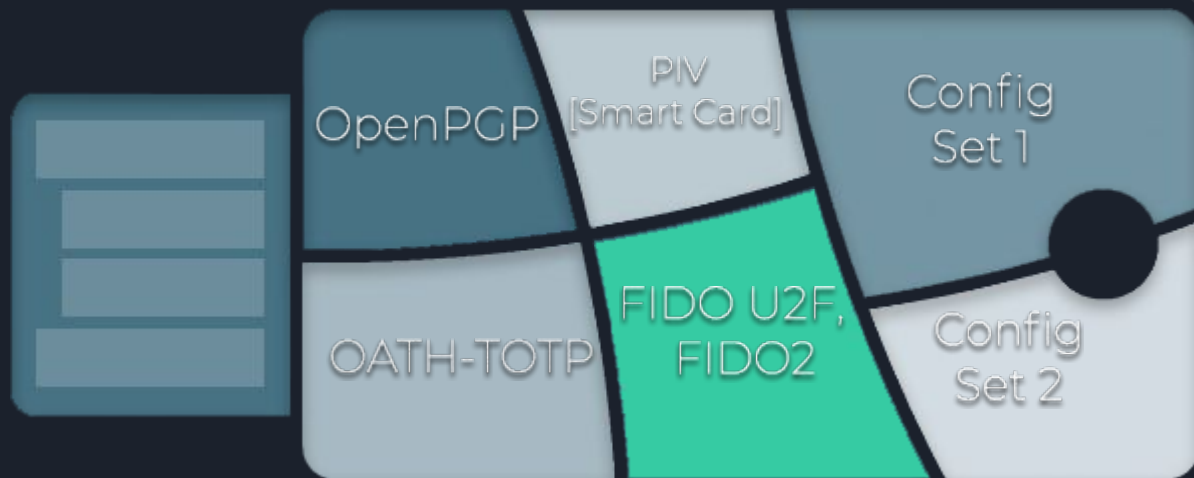
# Mac OS (certificate)



Introducing YubiKey  
and macOS Sierra

yubico

# FIDO “passwordless”





# 2FA

2FA - Two-factor authentication

SMS:

1. Нужно иметь номер телефона - я верю что их не станет также как и паролей
2. Not secure

OTP

Smart card

FIDO



Фидонет

Фидонет



Fido



# Fido

**Fido** - Альянс FIDO (Fast IDentity Online)-консорциум технологических компаний, которые собирались создать новый протокол беспарольной онлайн-аутентификации.

**CTAP** - Client to Authenticator Protocol - Низкоуровневое описание взаимодействие операционной системы с устройствами аутентификации BLE/NFC/USB

**CTAP1** - A formal name of U2F protocol.

**U2F** - Universal 2nd Factor

**CTAP2** - A name for second version of the CTAP protocol

**FIDO2** - passwordless authentication protocol

**WebAuthn** - API Authentication



Fido



NO  
FF  
ONE  
2022

# Fido

**Fido** - Альянс FIDO (Fast IDentity Online)-консорциум технологических компаний, которые собирались создать новый протокол беспарольной онлайн-аутентификации.

**CTAP** - Client to Authenticator Protocol - Низкоуровневое описание взаимодействие операционной системы с устройствами аутентификации BLE/NFC/USB

**CTAP1** - A formal name of U2F protocol.

**U2F** - Universal 2nd Factor

**CTAP2** - A name for second version of the CTAP protocol

**FIDO2** - passwordless authentication protocol

**WebAuthn** - API Authentication

# Fido

CTAP1 - A formal name of U2F protocol.

U2F - Universal 2nd Factor



2FA (U2F)



CTAP2 - A name for second version of the CTAP protocol

FIDO2 - passwordless authentication protocol



Passwordless

WebAuthn - API Authentication

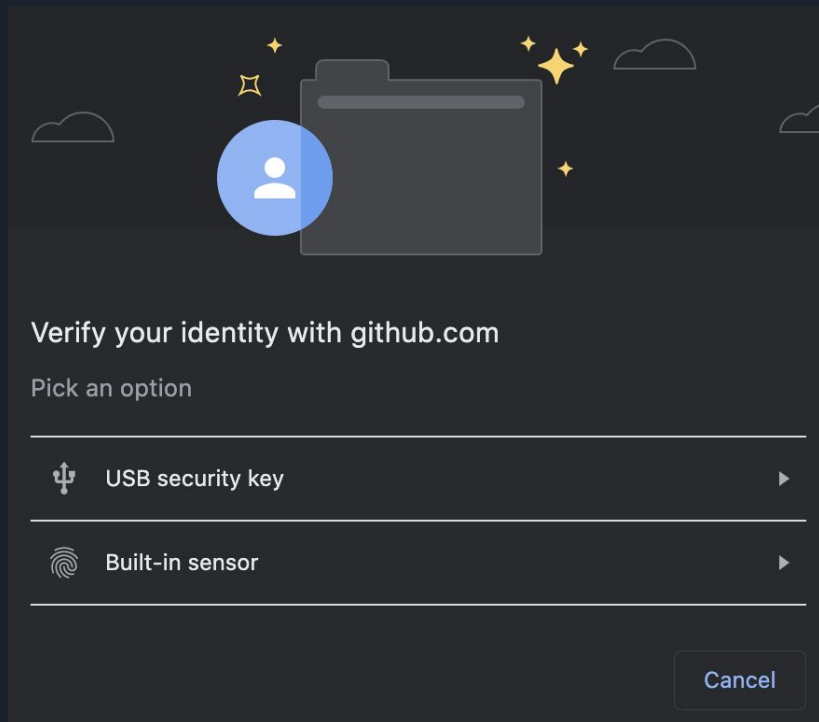
# Fido2 Passwordless

Login + Token

Single f: Username + FIDO2 credential

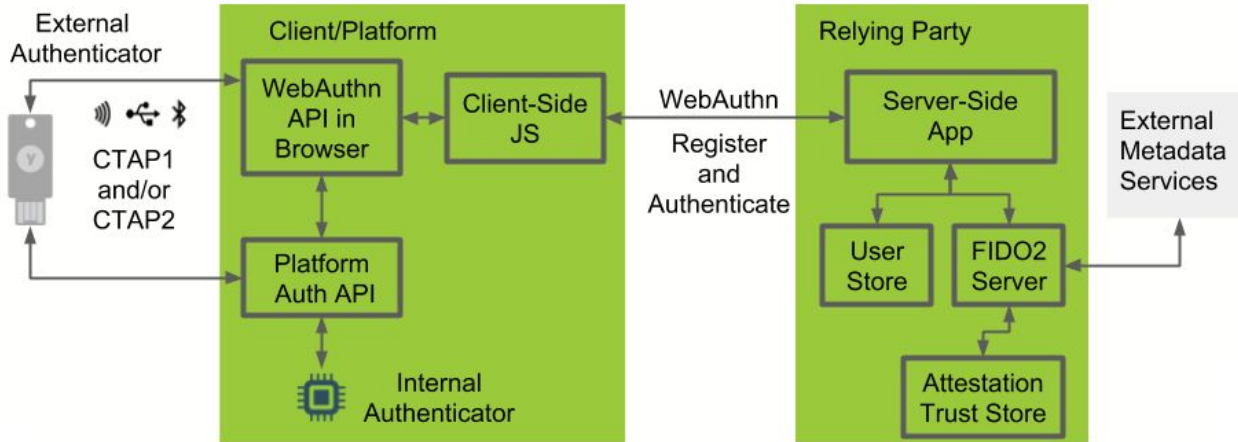
Second f: Username + password + FIDO2 credential

Passwordless MFA: FIDO2 resident key credential + PIN

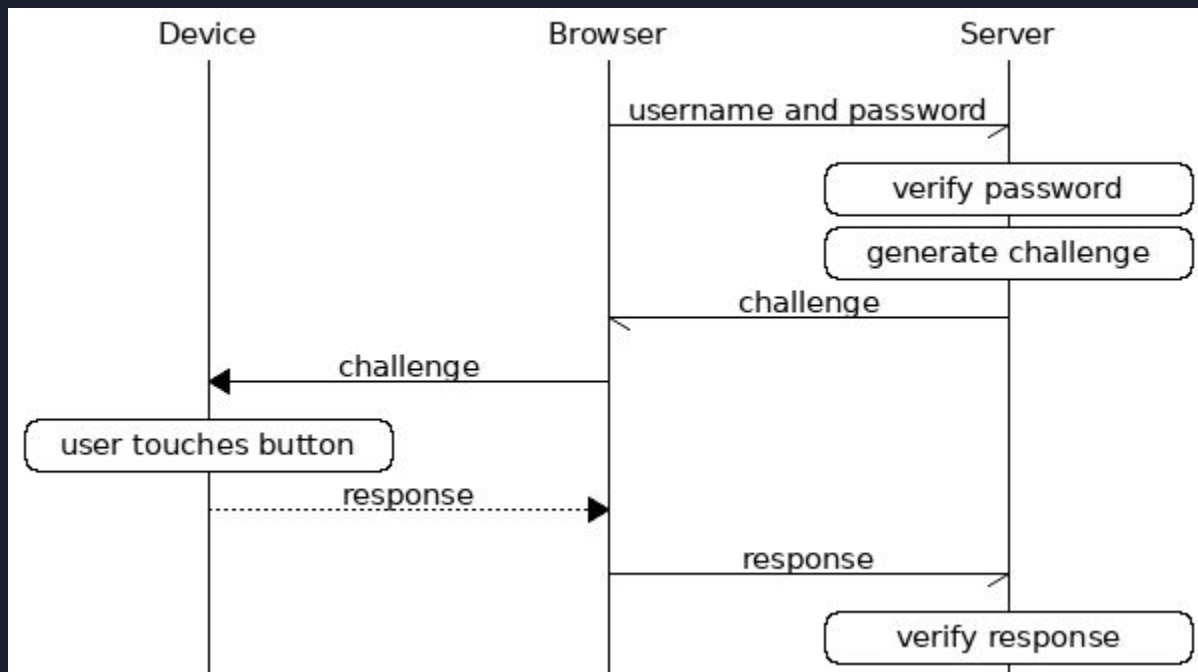




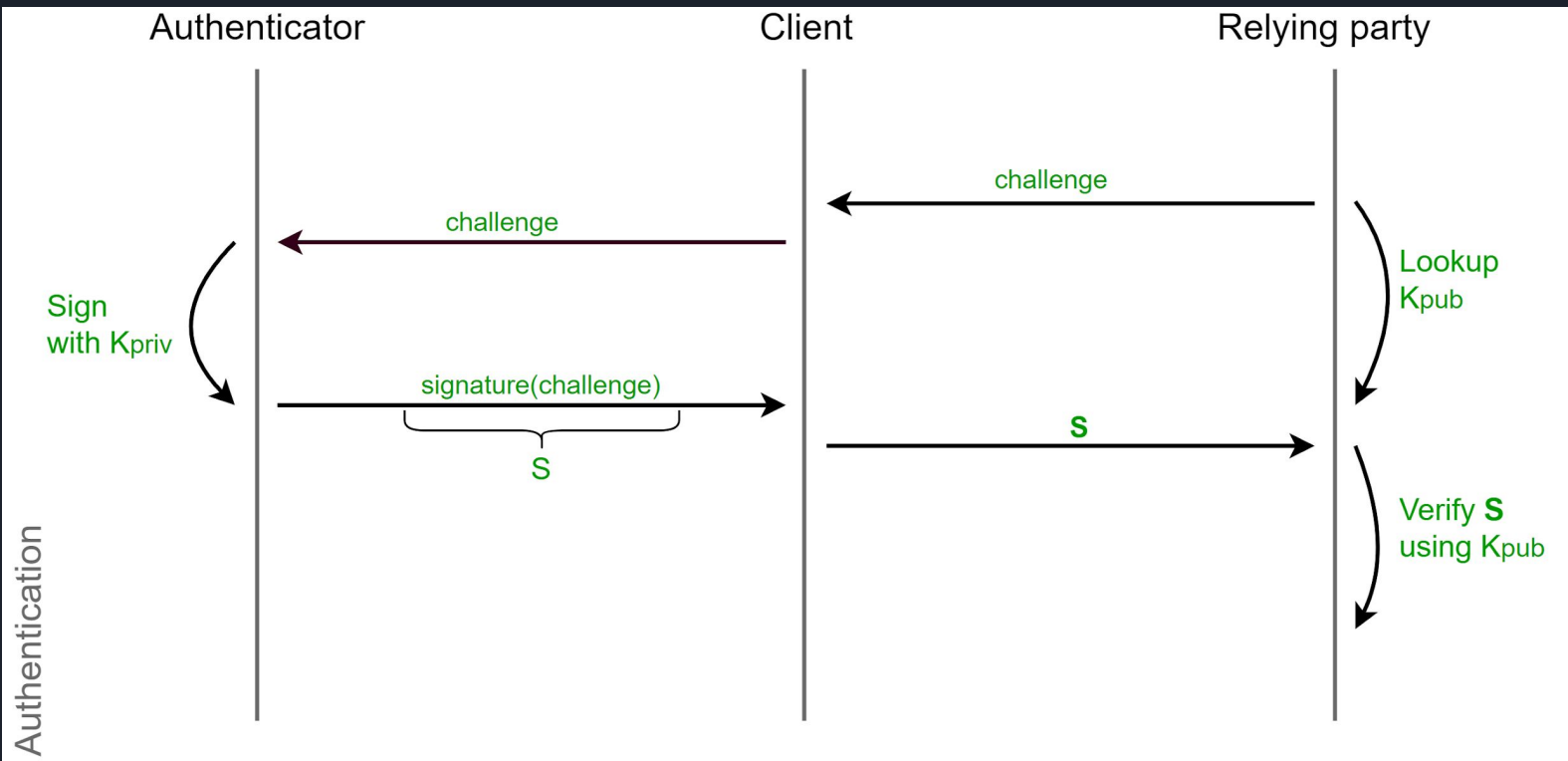
## FIDO2 Application Architecture



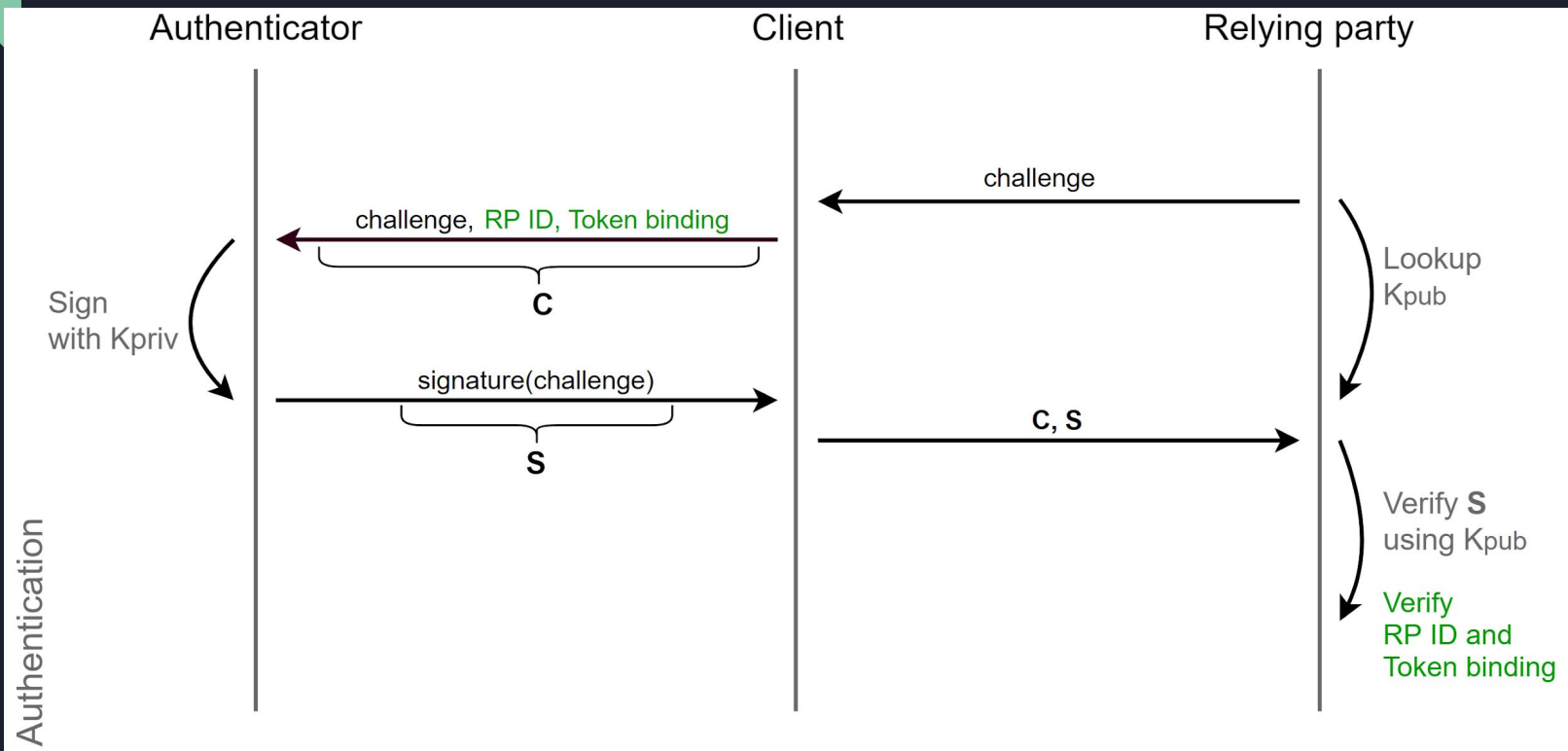
# U2F / FIDO2 - 0 User presence test



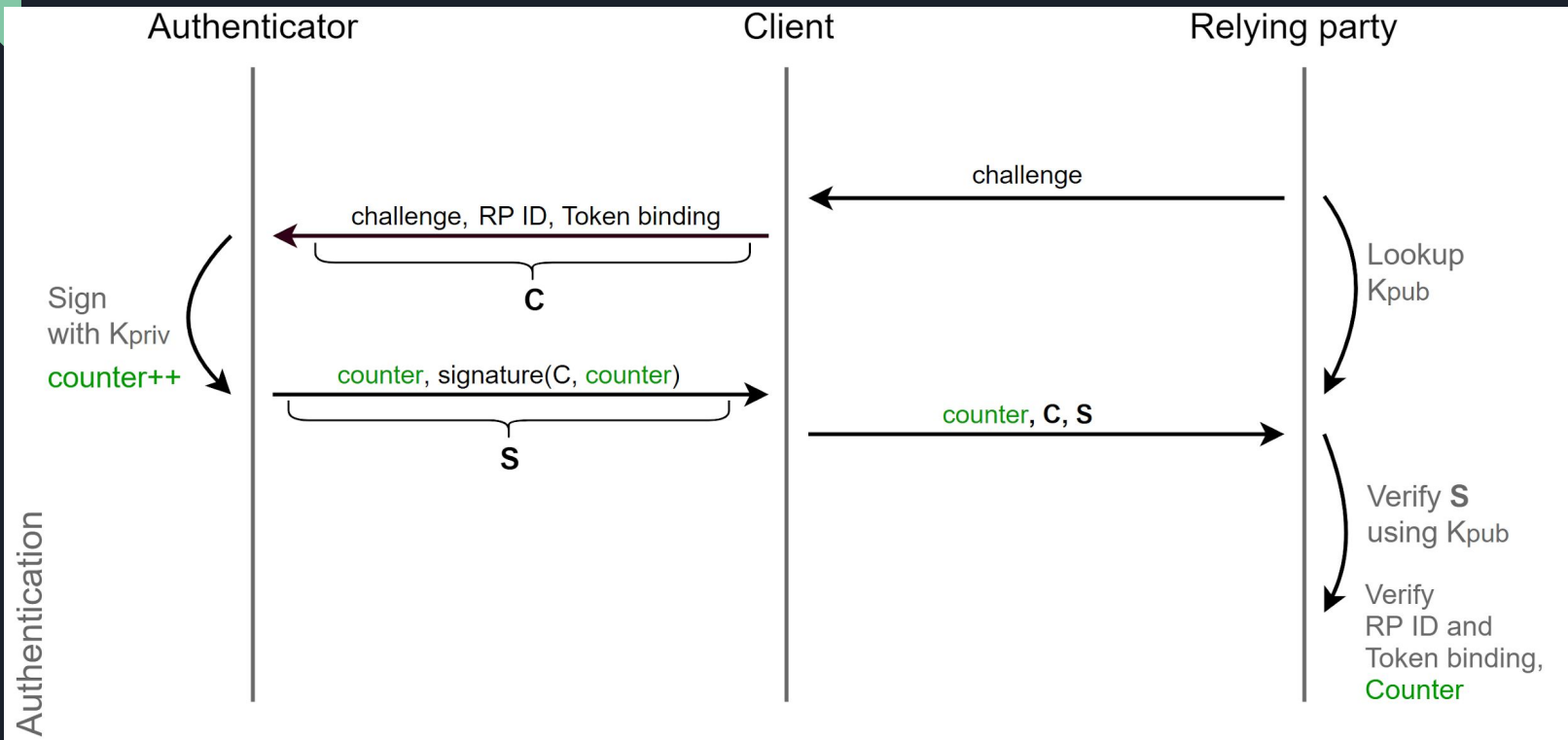
# U2F / FIDO2 - 1 Challenge-response



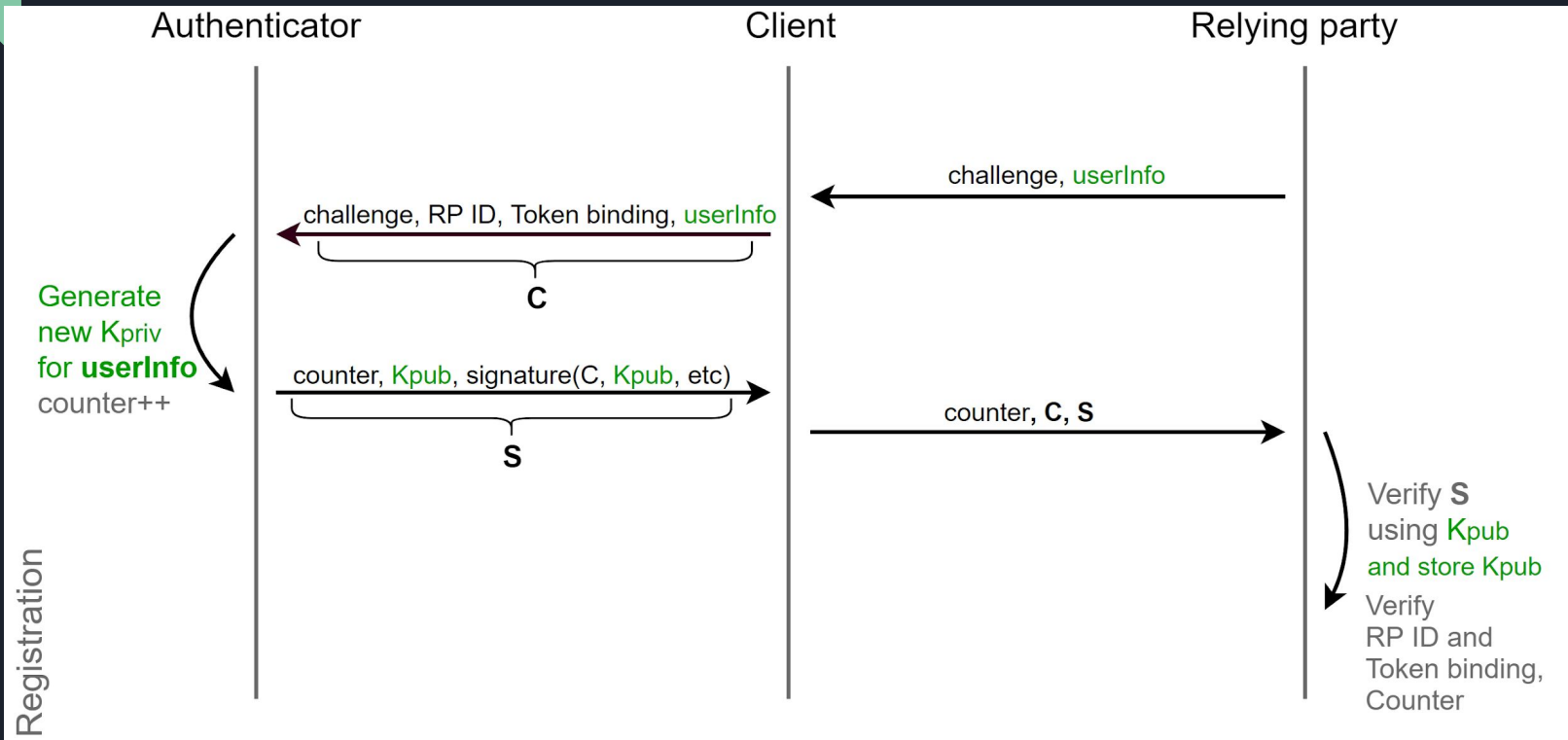
# U2F / FIDO2 - 2 Phishing and MitM protection



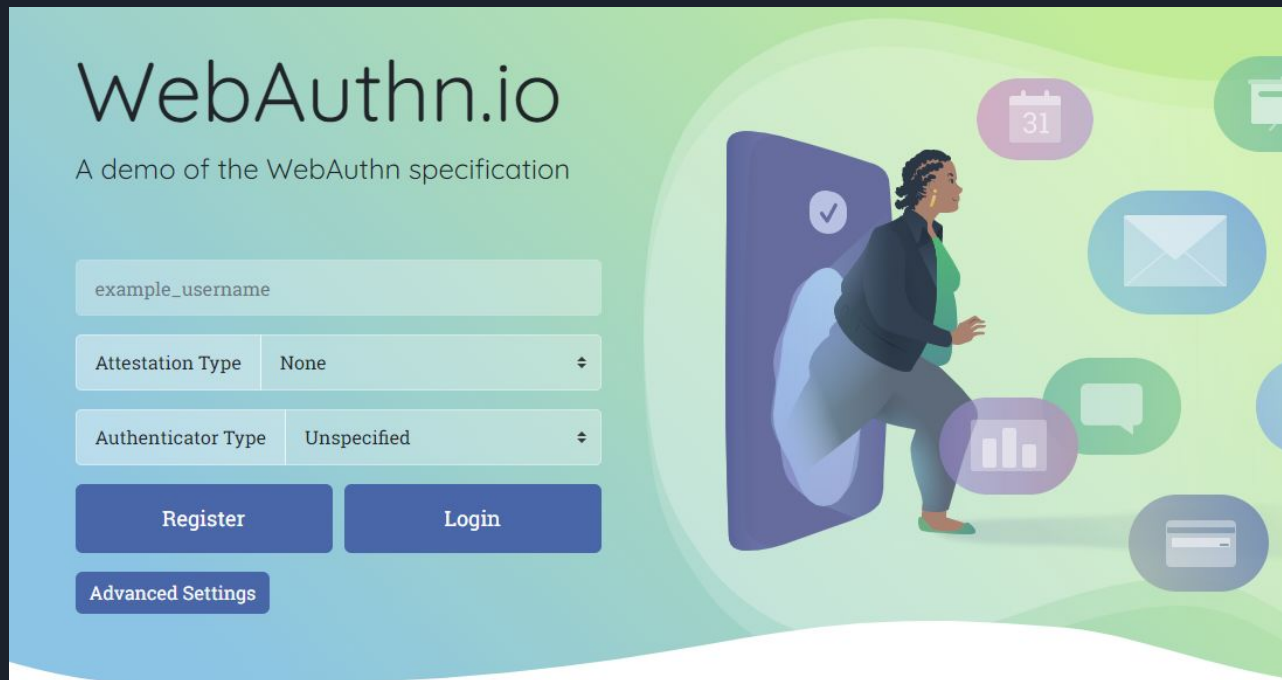
# U2F / FIDO2 - 3 Device cloning detection



# FIDO2 - 4 Privacy



<https://webauthn.io/>



The image shows a demo interface for WebAuthn.io. On the left, there is a registration form with a text input for 'example\_username', a dropdown for 'Attestation Type' set to 'None', and another dropdown for 'Authenticator Type' set to 'Unspecified'. Below these are three buttons: 'Register', 'Login', and 'Advanced Settings'. On the right, there is an illustration of a person standing next to a large smartphone. The smartphone screen shows a checkmark. Surrounding the person and phone are various icons in rounded rectangles: a calendar with '31', an envelope, a bar chart, a speech bubble, and a server rack.

# WebAuthn.io

A demo of the WebAuthn specification

example\_username

Attestation Type None

Authenticator Type Unspecified

Register Login

Advanced Settings

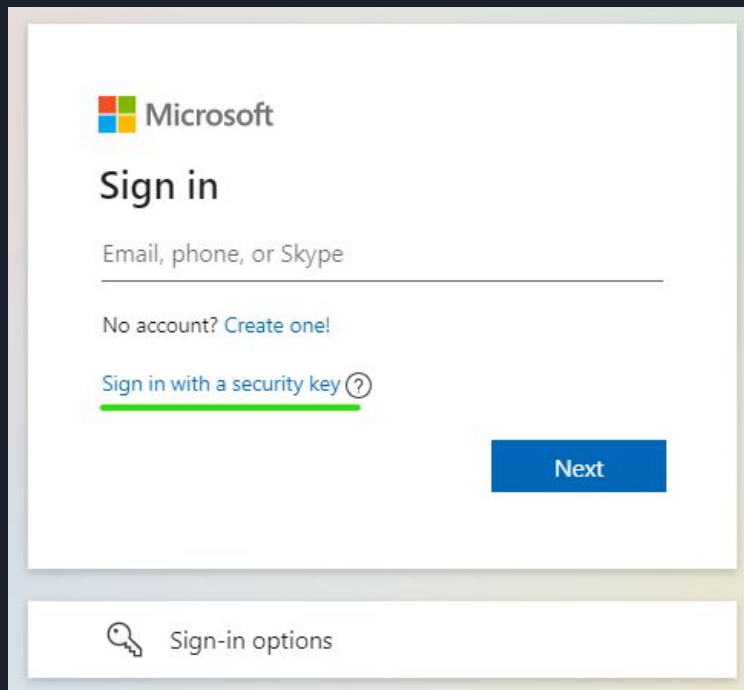
# Windows U2f / passwordless





# Windows passwordless - demo

<https://login.live.com/>



The screenshot shows the Microsoft sign-in interface. At the top is the Microsoft logo. Below it is the heading 'Sign in'. There is a text input field labeled 'Email, phone, or Skype'. Below the input field is a link 'No account? Create one!'. Below that is a link 'Sign in with a security key' which is underlined in green and followed by a question mark icon. To the right of this link is a blue 'Next' button. At the bottom of the page is a section titled 'Sign-in options' with a key icon.

Microsoft


## Sign in

Email, phone, or Skype

No account? [Create one!](#)

Sign in with a security key (?)

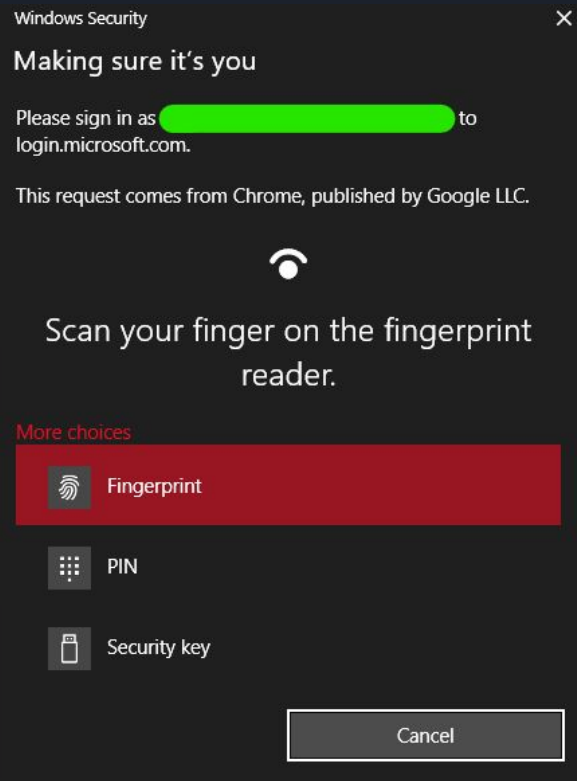
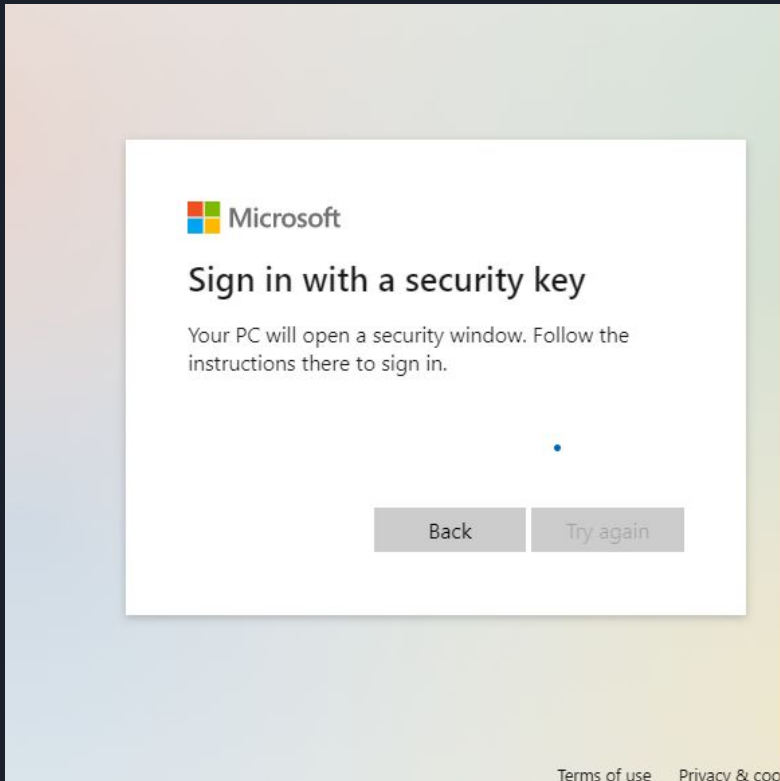
Next

 Sign-in options

# Windows passwordless - demo

<https://login.live.com/>

NO  
FF  
ONE  
2022



# Windows passwordless - demo

<https://login.live.com/>


Windows Security ✕

Making sure it's you

Please sign in to [login.microsoft.com](https://login.microsoft.com).

This request comes from Chrome, published by Google LLC.

Please enter your security key PIN.

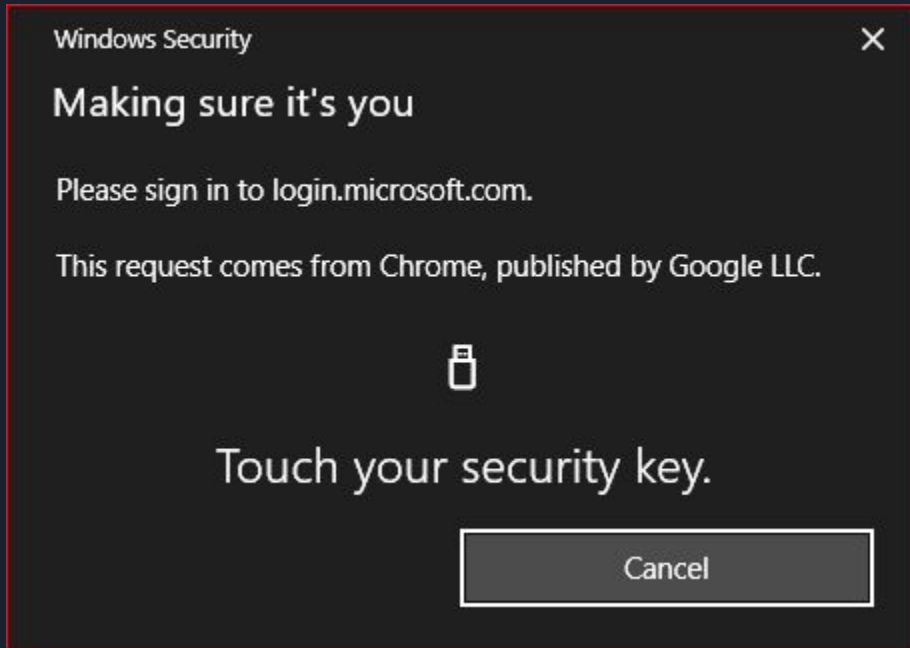


OK

Cancel

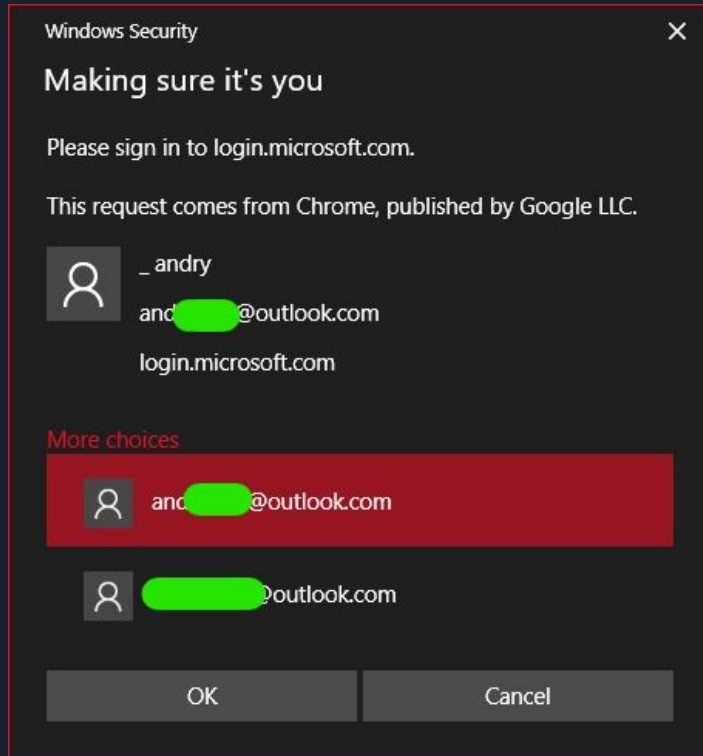
# Windows passwordless - demo

<https://login.live.com/>

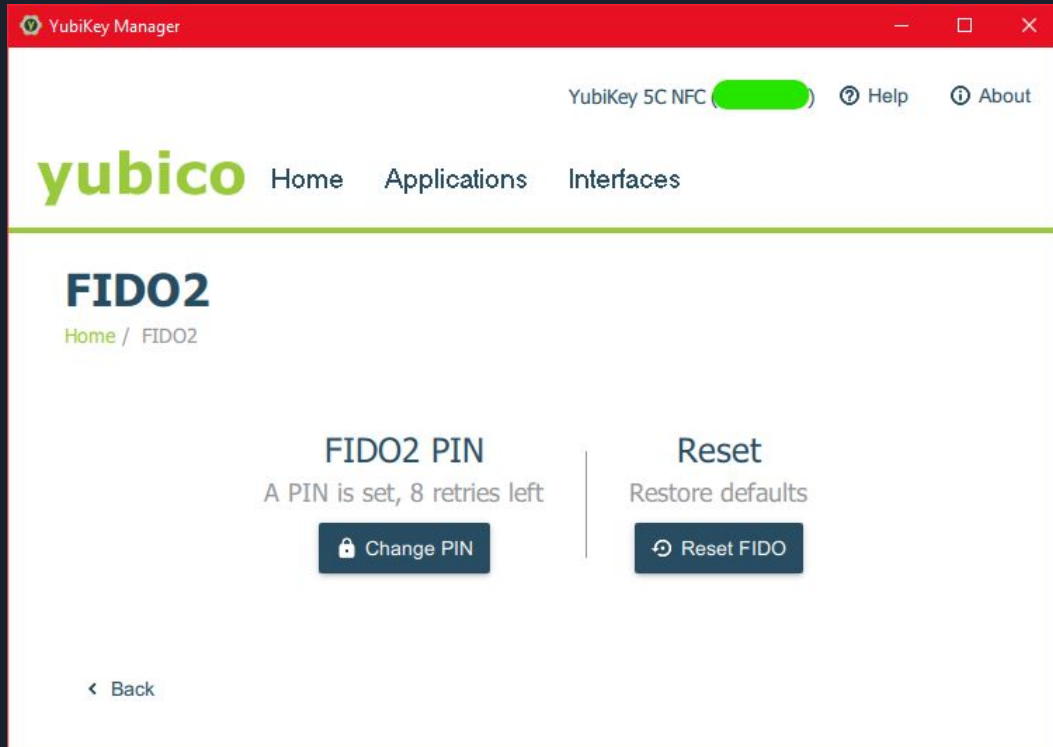


# Windows passwordless - demo

<https://login.live.com/>



# Manage FIDO2 passwordless



The screenshot shows the YubiKey Manager web application. The title bar is red and says "YubiKey Manager". The main header is white with the "yubico" logo in green and navigation links for "Home", "Applications", and "Interfaces". A status bar at the top right shows "YubiKey 5C NFC" with a green indicator, a help icon, and an "About" link. The main content area has a green horizontal line and the heading "FIDO2" with a breadcrumb "Home / FIDO2". Below this, there are two columns. The left column is titled "FIDO2 PIN" and contains the text "A PIN is set, 8 retries left" and a blue button with a lock icon labeled "Change PIN". The right column is titled "Reset" and contains the text "Restore defaults" and a blue button with a circular arrow icon labeled "Reset FIDO". At the bottom left, there is a link "< Back".

YubiKey Manager

YubiKey 5C NFC ( ) ? Help ? About

yubico Home Applications Interfaces

## FIDO2

Home / FIDO2

### FIDO2 PIN

A PIN is set, 8 retries left

Change PIN

### Reset

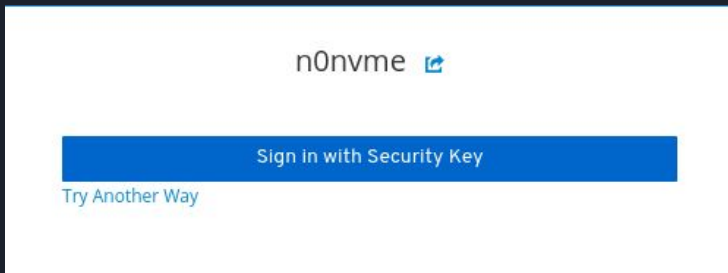
Restore defaults

Reset FIDO

< Back



# FIDO2 passwordless - SelfHosted - keycloak





# FIDO2 passwordless - SelfHosted - keycloak

## Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy CIBA Policy

Browser WebAuthn

New Copy Delete Edit Flow Add execution Add flow

| Auth Type   |   |  | Requirement                               |  |   |                                   |         |
|---|---|--|---|--|---|-----------------------------------|---------|
| <input type="checkbox"/> <input type="checkbox"/> | Cookie  |  | <input type="radio"/> REQUIRED            | <input checked="" type="radio"/> ALTERNATIVE | <input type="radio"/> DISABLED            |                                   | Actions |
| <input type="checkbox"/> <input type="checkbox"/> | Kerberos  |  | <input type="radio"/> REQUIRED            | <input type="radio"/> ALTERNATIVE            | <input checked="" type="radio"/> DISABLED |                                   | Actions |
| <input type="checkbox"/> <input type="checkbox"/> | Identity Provider Redirector  |  | <input type="radio"/> REQUIRED            | <input checked="" type="radio"/> ALTERNATIVE | <input type="radio"/> DISABLED            |                                   | Actions |
| <input type="checkbox"/> <input type="checkbox"/> | Browser WebAuthn Forms  |  | <input type="radio"/> REQUIRED            | <input checked="" type="radio"/> ALTERNATIVE | <input type="radio"/> DISABLED            | <input type="radio"/> CONDITIONAL | Actions |
|   | <input type="checkbox"/> <input type="checkbox"/> Username Form                       |  | <input checked="" type="radio"/> REQUIRED |  |   |                                   | Actions |
|   | <input type="checkbox"/> <input type="checkbox"/> Passwordless Or Password            |  | <input checked="" type="radio"/> REQUIRED | <input type="radio"/> ALTERNATIVE            | <input type="radio"/> DISABLED            | <input type="radio"/> CONDITIONAL | Actions |
|   | <input type="checkbox"/> <input type="checkbox"/> WebAuthn Passwordless Authenticator |  | <input type="radio"/> REQUIRED            | <input checked="" type="radio"/> ALTERNATIVE | <input type="radio"/> DISABLED            |                                   | Actions |
|   | <input type="checkbox"/> <input type="checkbox"/> Password Form                       |  | <input type="radio"/> REQUIRED            | <input checked="" type="radio"/> ALTERNATIVE | <input type="radio"/> DISABLED            |                                   | Actions |



# FIDO2 passwordless - SelfHosted - keycloak

## Authentication

- Flows
- Bindings
- Required Actions
- Password Policy
- OTP Policy
- WebAuthn Policy ?
- WebAuthn Passwordless Policy ?
- CIBA Policy

Register

| Required Action   | Enabled                             | Default Action ?         |
|---|-------------------------------------|--------------------------|
| <input type="checkbox"/> Webauthn Register Passwordless | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Configure OTP                  | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Terms and Conditions           | <input type="checkbox"/>            | <input type="checkbox"/> |

# FIDO2 passwordless - SelfHosted - keycloak



## Signing In

Configure ways to sign in.

### Basic Authentication

#### Password

Log in by entering your password.

My Password

Created: August 25, 2022 at 1:47 AM

[Update](#)

### Two-Factor Authentication

#### Authenticator Application

Enter a verification code from authenticator application.

[Set up Authenticator Application](#)

Authenticator Application is not set up.

### Passwordless

#### Security Key

Use your security key for passwordless sign in.

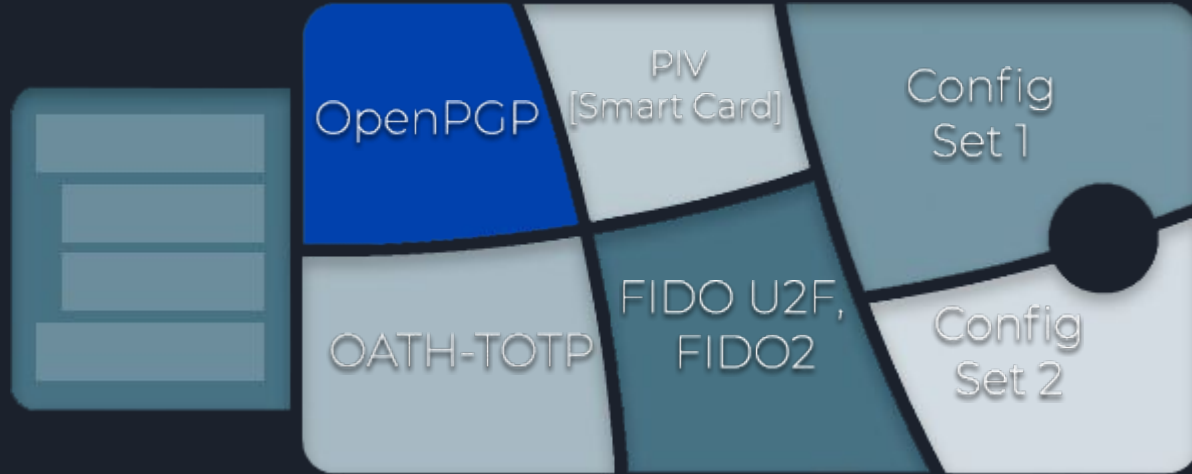
[Set up Security Key](#)

webAuthn keycloak test

Created: August 25, 2022 at 2:06 AM

[Remove](#)

# PGP



GPG or PGP or OpenPGP ?!

PGP

GPG

# PGP - Pretty Good Privacy

## GPG

PGP - Pretty Good Privacy - openpgp -  
proprietary

GPG



PGP - Pretty Good Privacy - openpgp -  
proprietary

GPG - GnuPG

PGP - Pretty Good Privacy - openpgp -  
proprietary

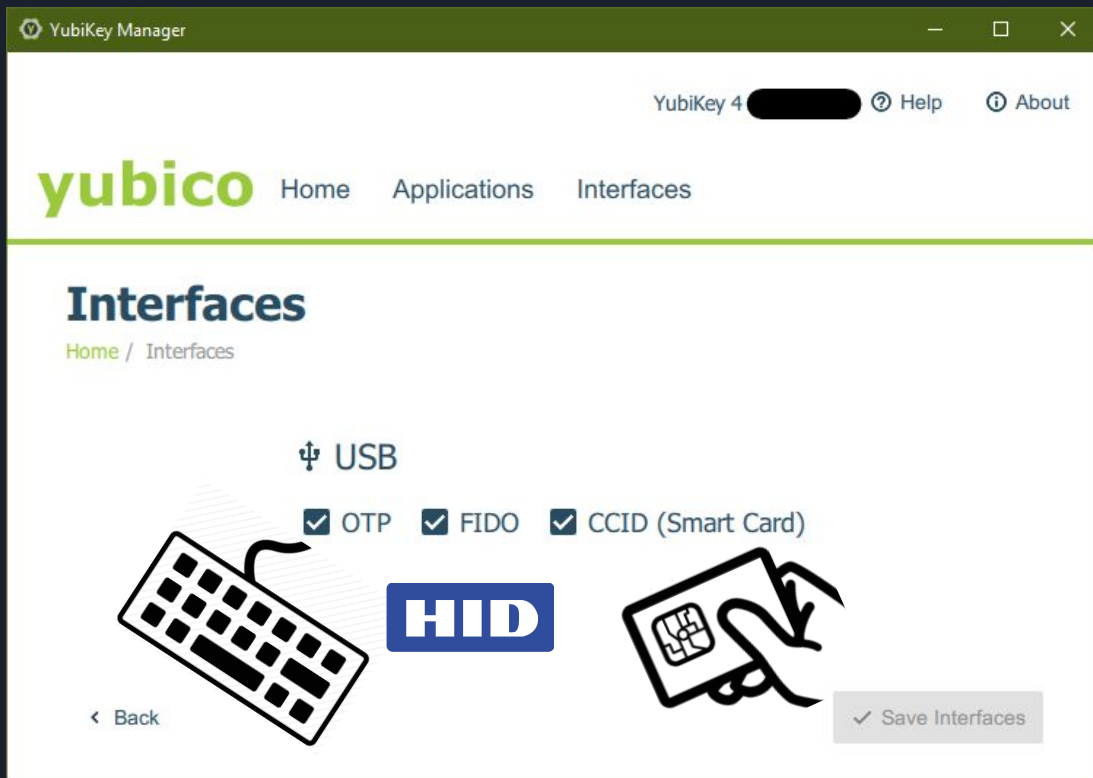
GPG - GnuPG - GNU Privacy Guard

PGP - Pretty Good Privacy - openpgp -  
proprietary

GPG - GnuPG - GNU Privacy Guard -  
open source

PGP ~ GPG

Что есть yubikey для  
компа?



<https://docs.yubico.com/hardware/yubikey/yk-5/tech-manual/index.html>

YubiKey Manager

YubiKey 5C NFC  ? Help i About

yubico

Home Applications Interfaces

# Interfaces

Home / Interfaces

USB

Disable all

☒ OTP

☒ FIDO2

☒ FIDO U2F

☒ OpenPGP

☒ PIV

☒ OATH

NFC

Disable all

☒ OTP

☒ FIDO2

☒ FIDO U2F

☒ OpenPGP

☒ PIV

☒ OATH

< Back

✓ Save Interfaces



# Yubikey/SmartCard backed TLS servers



Yubikey/SmartCard(GPG) backed TLS servers





# Yubikey/SmartCard(GPG) backed TLS servers

GPG и SSL(TLS)

в основе лежит RSA/ECC (Elliptic Curve Cryptography)

Та почему не использовать?)

[Yubikey/Smartcard backed TLS servers](#)

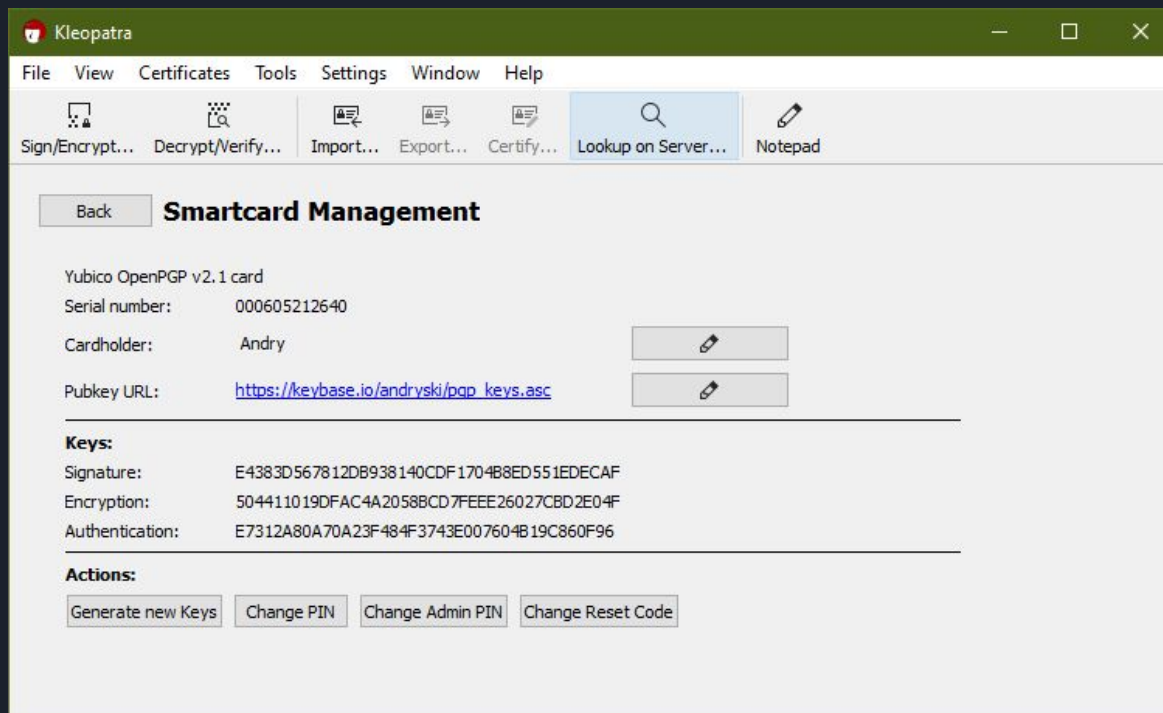
# YubiKey & ssh (?)

# YubiKey & ssh(certificate)

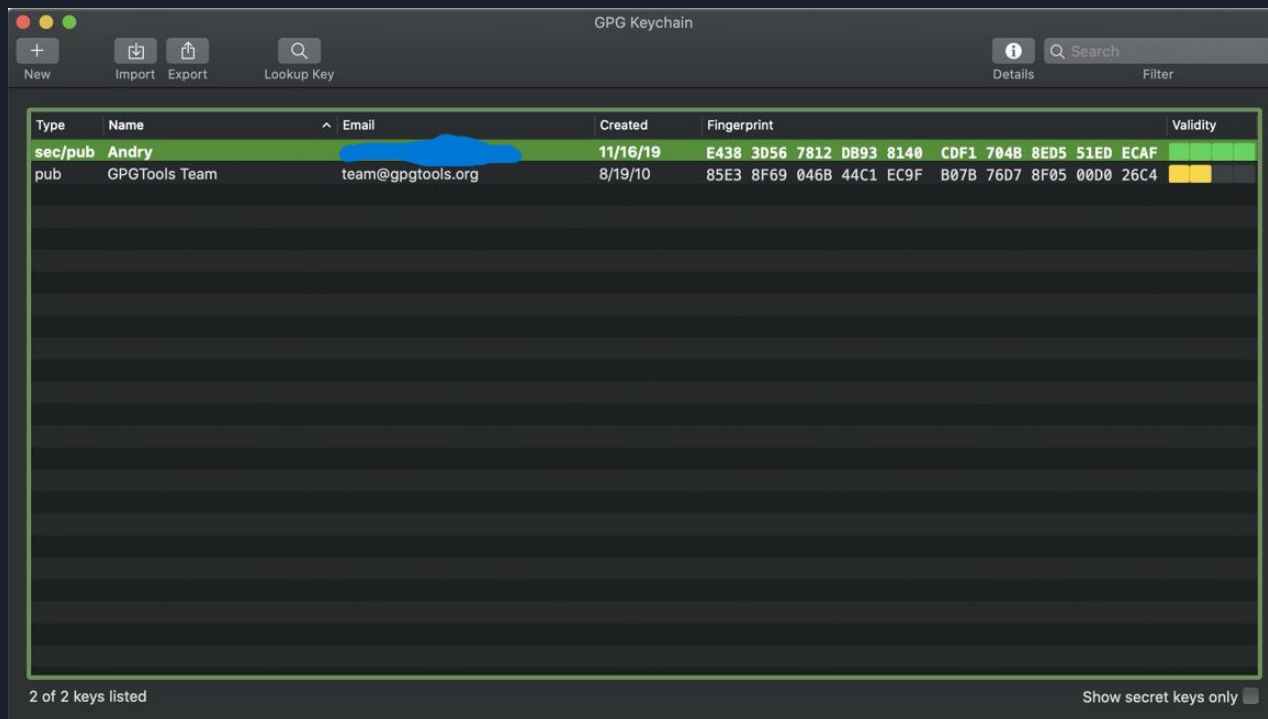
home work

# YubiKey & ssh (gpg)

# Common



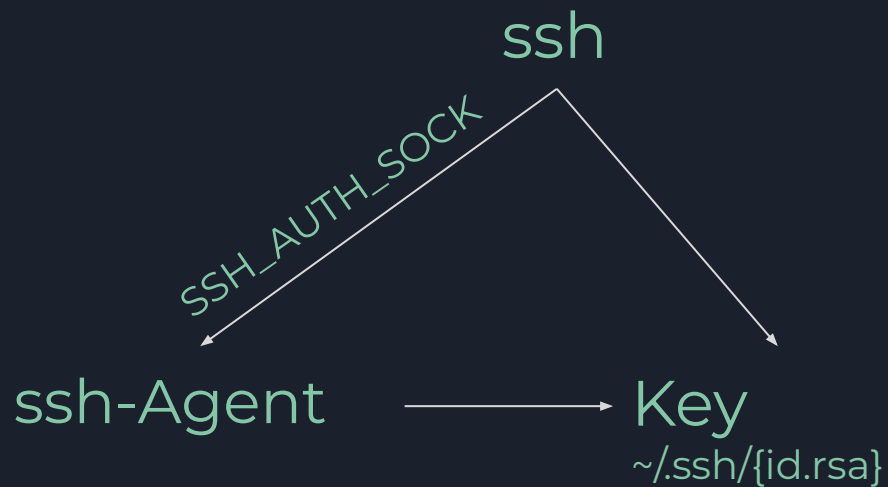
# Common





# ssh

environment variable - `SSH_AUTH_SOCK`







ssh





# ssh

```
export SSH_AUTH_SOCKET="${HOME}/.gnupg/S.gpg-agent.ssh"
```

```
$ ssh-add -L
```

```
ssh-rsa AAAA.....DmL cardno:000605212640
```

```
echo <KEY> > ~/.ssh/authorized_keys
```

```
ssh-copy-id
```

# ssh + GPG in Linux/Mac

~/.bashrc

~/.zshrc

ssg(){ ~/scripts/gssh.sh \$@; }

export -f ssg

# ssh + GPG in Linux/Mac

```
#!/bin/bash
```

```
if [ ! -S "${HOME}/gnupg/S.gpg-agent.ssh" ]; then  
    gpg-agent --daemon > /dev/null  
fi
```

```
gpg --card-status > /dev/null 2>/dev/null  
if [ $? -eq 0 ]  
then  
    echo "Success: gpg token fund"  
else  
    echo "Failure: gpg token NOT fund" >&2  
  
    exit 1  
fi
```

# ssh + GPG in Linux/Mac

```
export SSH_AUTH_SOCKET_old=$SSH_AUTH_SOCKET
export SSH_AUTH_SOCKET="${HOME}/.gnupg/S.gpg-agent.ssh"
ssh $@
export SSH_AUTH_SOCKET=$SSH_AUTH_SOCKET_old
unset SSH_AUTH_SOCKET_old
```

## ssh + GPG in Mac

```
#!/bin/bash
```

```
if [ ! -S "${HOME}/gnupg/S.gpg-agent.ssh" ]; then  
    gpg-agent --daemon > /dev/null  
fi
```

```
gpg --card-status > /dev/null 2>/dev/null
```

```
if [ $? -eq 0 ]
```

```
then
```

```
    echo "Success: gpg token fund"
```

```
else
```

```
    echo "Failure: gpg token NOT fund" >&2
```

```
    gpgconf --kill gpg-agent
```

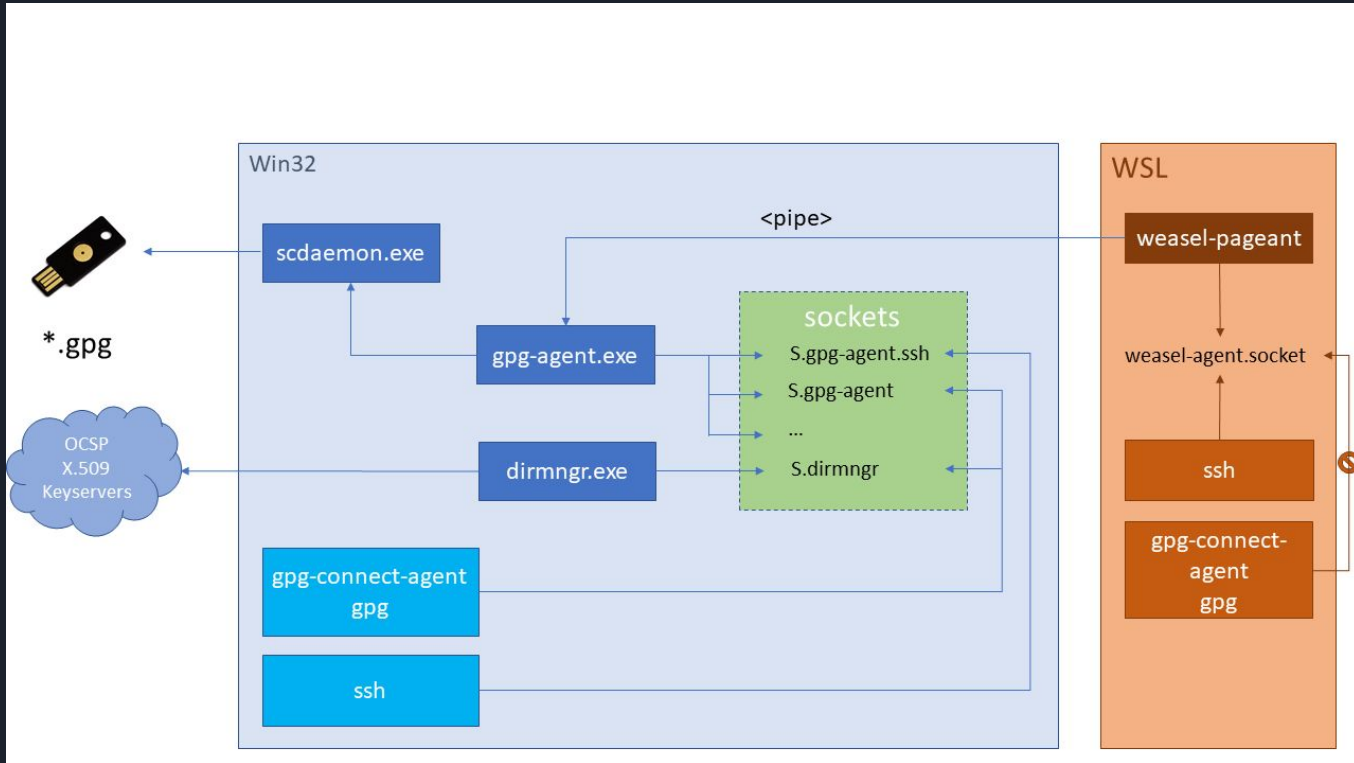
```
export GPG_TTY=$(tty)
```

```
    exit 1
```

```
fi
```

[https://www.gnupg.org/\(it\)/documentation/manuals/gnupg/Common-Problems.html](https://www.gnupg.org/(it)/documentation/manuals/gnupg/Common-Problems.html)

# ssh + GPG in Windows (WSL SSH bridge)

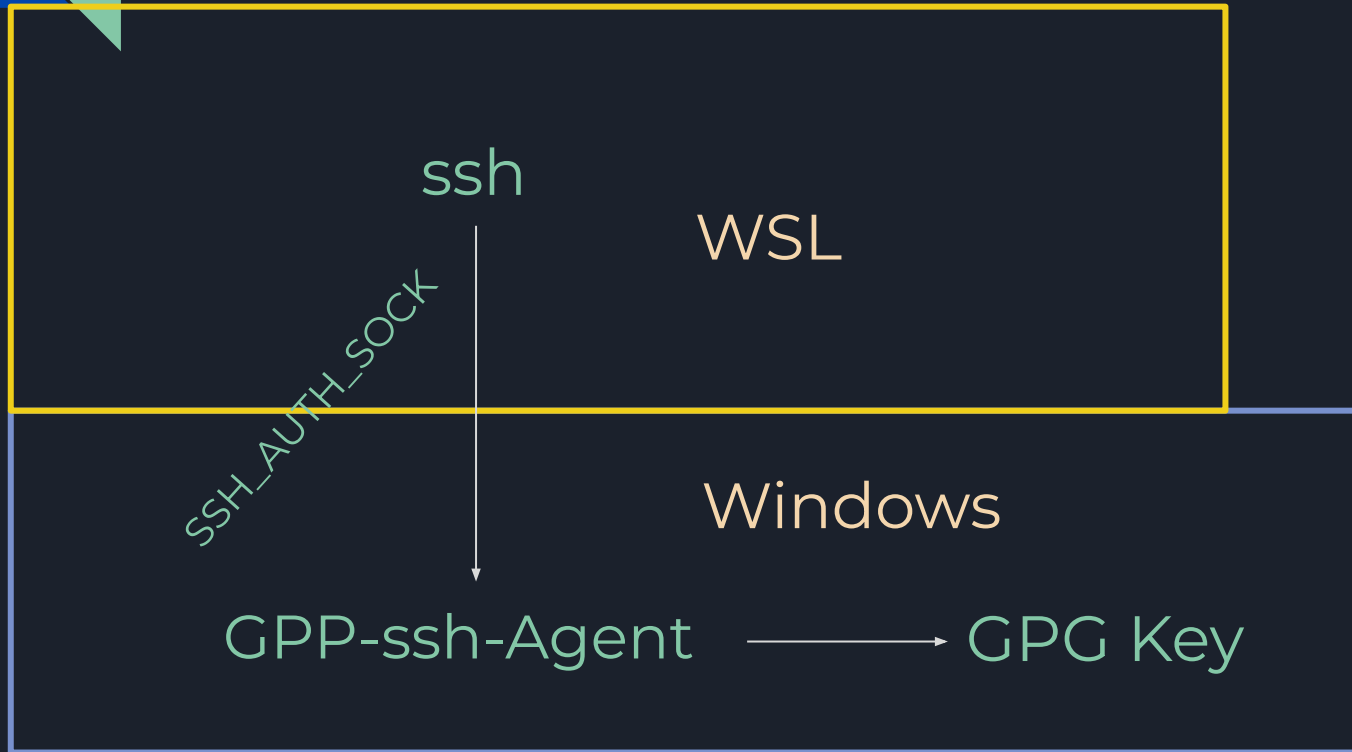


# ssh + GPG in Windows (WSL SSH bridge)





# ssh + GPG in Windows (WSL SSH bridge)



# ssh + GPG in Windows (WSL SSH bridge)

%APPDATA%\gnupg\gpg-agent.conf -> enable-putty-support

shell:startup

"C:\Program Files (x86)\GNU\GnuPG\gpg-connect-agent.exe" /bye

WSL

<https://github.com/benpye/wsl-ssh-pageant/releases>

# ssh + GPG in Windows (WSL SSH bridge)

```
C:\wsl-ssh\sbg.sh
#!/bin/bash
export SSH_AUTH_SOCKET_old=$SSH_AUTH_SOCKET
eval $(/mnt/c/wsl-ssh/weasel-pageant -r -a /tmp/S.weasel-pageant)
ssh $@
export SSH_AUTH_SOCKET=$SSH_AUTH_SOCKET_old
unset SSH_AUTH_SOCKET_old
```

# ssh + GPG in Windows (WSL SSH bridge)

```
export SSH_AUTH_SOCKET_old=$SSH_AUTH_SOCKET  
export SSH_AUTH_SOCKET="${HOME}/.gnupg/S.gpg-agent.ssh"
```

```
wsl
```

```
export SSH_AUTH_SOCKET_old=$SSH_AUTH_SOCKET  
eval $(/mnt/c/wsl-ssh/weasel-pageant -r -a /tmp/S.weasel-pageant)
```

# ssh + GPG in Windows (SSH)

win-gpg-agent

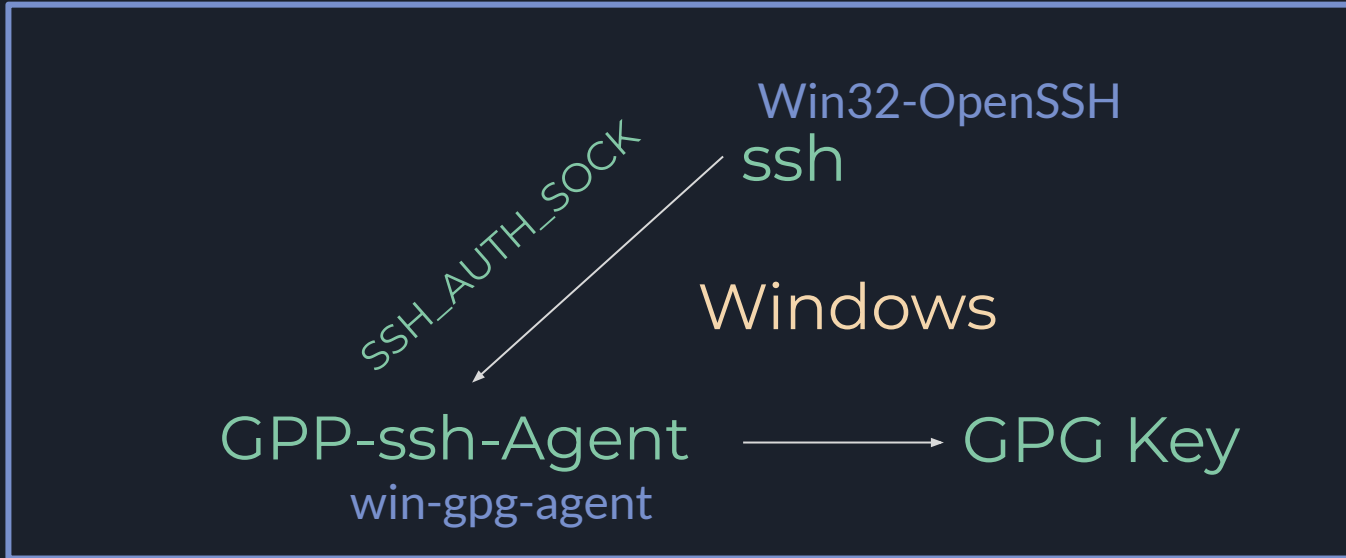
ssh

<https://github.com/rupor-github/win-gpg-agent>

<https://github.com/PowerShell/Win32-OpenSSH>



# ssh + GPG in Windows (SSH)



ssh Deeper



# ssh Deeper

Релиз OpenSSH 8.2 с поддержкой токенов двухфакторной аутентификации FIDO/U2F



<https://www.openssh.com/txt/release-8.2>

<https://www.opennet.ru/opennews/art.shtml?num=52369>

<https://about.gitlab.com/blog/2022/03/03/how-to-protect-gitlab-connected-ssh-key-with-yubikey/>

<https://cryptsus.com/blog/how-to-configure-openssh-with-yubikey-security-keys-u2f-otp-authentication-ed25519-sk-ecdsa-sk-on-ubuntu-18.04.html>



# FIDO2 SSH

## FIDO 2

```
ssh-keygen -t ed25519-sk -O resident -O application=ssh:n0nvme -C  
n0nvme@yubikey2
```

ssh-add -K - add resident key to agent

ssh-keygen -K - restore resident key to File system

windows bug - <https://github.com/PowerShell/Win32-OpenSSH/issues/1915>

## U2F

нужно выполнять без "-O resident", и сгенеренные файлы не потерять.

GIT





# GIT

SSH and GPG keys

SSH Keys

GPG Keys





# GIT

(Signature key)

```
git config --global user.signingkey 51EDECAF
```

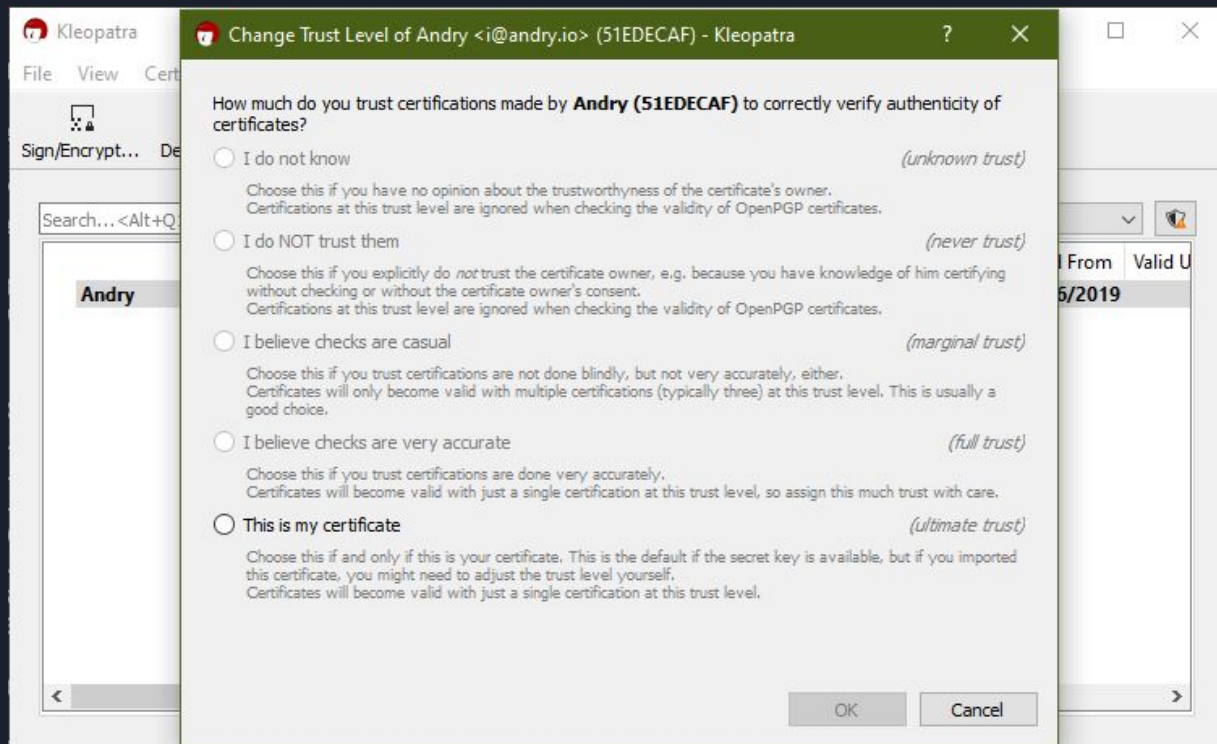
```
git config --global commit.gpgsign true
```

windows

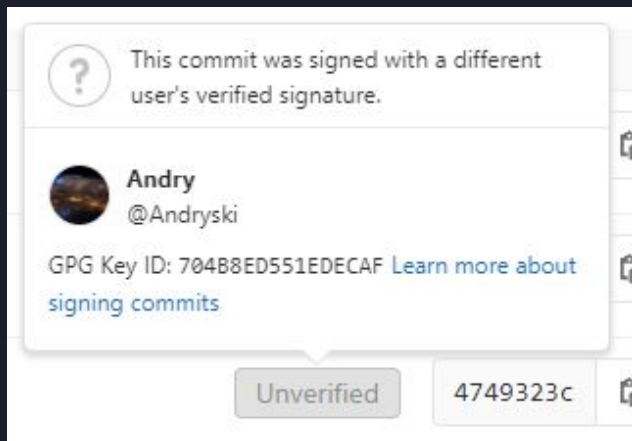
```
git config --global gpg.program "C:\Program Files (x86)\GnuPG\bin\gpg.exe"
```

# GIT

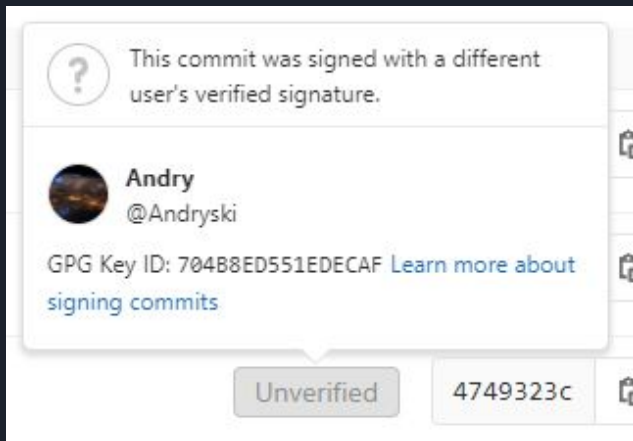
NOFF  
ONE  
2022



# GIT

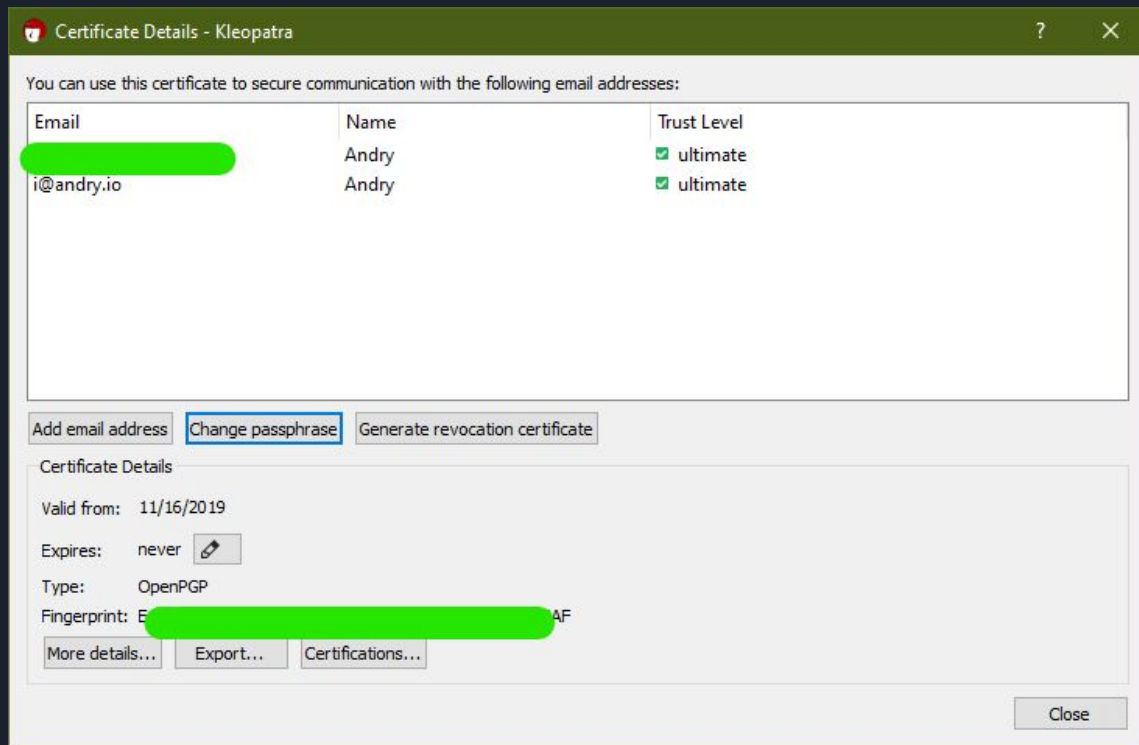


# GIT



```
created ....: 2019-11-16 14:41:33
Authentication key: E731 2A80 A70A 23F4 84F3 743E 0076 04B1 9C86 0F96
General key info.: pub rsa2048/704B8ED551EDECAF 2019-11-16 Andry <i@andry.io>
sec> rsa2048/704B8ED551EDECAF created: 2019-11-16 expires: never
card-no: 0006 05212640
pub rsa2048/007604B19C860F96 created: 2019-11-16 expires: never
```

# GIT





# GIT

**Certificate Details - Kleopatra**

You can use this certificate to secure communication with the following email addresses:

| Email      | Name  | Trust Level                                  |
|------------|-------|--|
| [REDACTED] | Andry | <input checked="" type="checkbox"/> ultimate |
| i@andry.io | Andry | <input checked="" type="checkbox"/> ultimate |

**Certificate Details**

Valid from: 11/16/2019

Expires: never

Type: OpenPGP

Fingerprint: E [REDACTED]

[More details...](#) [Export...](#) [Certifications...](#)

[Add email address](#) [Change passphrase](#) [Generate revocation certificate](#)

**Add New User-ID - Kleopatra**

Name:  (optional)

Email:  (optional)


Comment:  (optional)

This is how the new User-ID will be stored in the certificate:


**Andry**

[OK](#) [Cancel](#)

# GIT



This commit was signed with a **verified** signature and the committer email is verified to belong to the same user.




**Andry**  
@Andryski

GPG Key ID: 704B8ED551EDECAF [Learn more about signing commits](#)


Verified

dc08051b

# GIT



This commit was signed with a **verified** signature and the committer email is verified to belong to the same user.




**Andry**  
@Andryski



GPG Key ID: 704B8ED551EDECAF [Learn more about signing commits](#)

Verified

dc08051b

Your GPG keys (1)



|   |          |            |            |
|---|----------|------------|------------|
|       | Verified | i@andry.io | Unverified |
| E4  |          |            |            |

GIT + SSH ?!

GIT + SSH ?!



А почему бы



и нет?

# GIT + SSH + GPG

## Your SSH keys (2)

 cardno:000605212640 4b:13:34:3a:86:12:3b:ce:8a:6d:31:b0:b3:c4:a6:12  
Last used: 3 weeks ago Expires: Never Created 3 weeks ago 

# GIT + SSH + GPG

## Your SSH keys (2)

cardno:000605212640 4b:13:34:3a:86:12:3b:ce:8a:6d:31:b0:b3:c4:a6:12



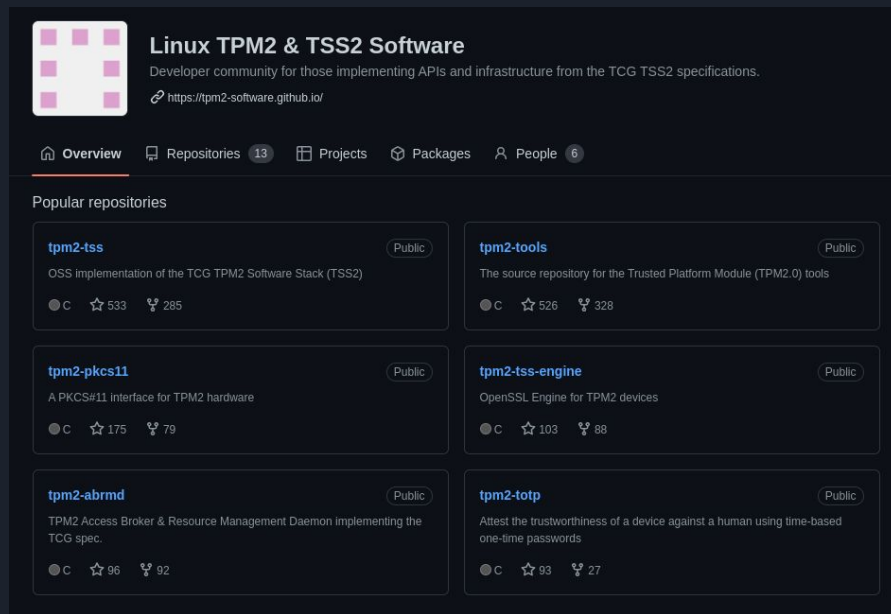
Last used: 3 weeks ago

Expires: Never

Created 3 weeks ago



# SSH + TPM + Linux (Dependencies)



The screenshot shows the GitHub repository page for "Linux TPM2 & TSS2 Software". The repository is described as a "Developer community for those implementing APIs and infrastructure from the TCG TSS2 specifications." and has a link to <https://tpm2-software.github.io/>. The page features a navigation bar with tabs for Overview, Repositories (13), Projects, Packages, and People (6). Below the navigation bar, there is a section titled "Popular repositories" which displays six repository cards. Each card includes the repository name, a brief description, and statistics for commits, stars, and watchers.

| Repository Name | Description  | Commits | Stars | Watchers |
|-----------------|--|---------|-------|----------|
| tpm2-tss        | OSS implementation of the TCG TPM2 Software Stack (TSS2)                                   | 533     | 285   |          |
| tpm2-tools      | The source repository for the Trusted Platform Module (TPM2.0) tools                       | 526     | 328   |          |
| tpm2-pkcs11     | A PKCS#11 interface for TPM2 hardware  | 175     | 79    |          |
| tpm2-tss-engine | OpenSSL Engine for TPM2 devices  | 103     | 88    |          |
| tpm2-abrmd      | TPM2 Access Broker & Resource Management Daemon implementing the TCG spec.                 | 96      | 92    |          |
| tpm2-totp       | Attest the trustworthiness of a device against a human using time-based one-time passwords | 93      | 27    |          |

# <https://github.com/tpm2-software>

\$ `sudo pacman -S tpm2-tss tpm2-abrmd tpm2-pkcs11 tpm2-tools`



# SSH + TPM + Linux

# Создаем новый слот в tpm

```
tpm2_ptool init
```

# Генерируем ключ

```
tpm2_ptool addtoken --pid=1 --label=ssh-key --sopin=XXXX --userpin=YYYY
```

```
tpm2_ptool addkey --label=ssh-key --userpin=YYYY --algorithm=ecc256
```

```
ssh-keygen -D /usr/lib/pkcs11/libtpm2_pkcs11.so
```

# Проверка что все ок

```
ssh -I /usr/lib/pkcs11/libtpm2_pkcs11.so user@example.com
```

# Добавляем в ssh-agent

```
ssh-add -s /usr/lib/pkcs11/libtpm2_pkcs11.so
```

# PROFIT

```
ssh user@example.com
```

Аналоги?



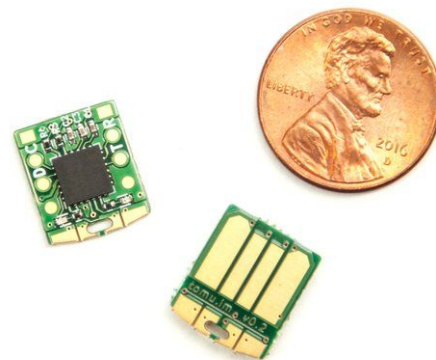
Miss the Kickstarter campaign?

Preorder  
Solo V2  
At  
**INDIEGOGO**

Click picture to go to the  
campaign



NO  
**FF  
ONE**  
2022



# аналоги



opensource

2022

| name         | FIDO | FIDO2 | OTP | GPG |  |  |
|--------------|------|-------|-----|-----|--|--|
| Nitrokey     |      |       |     |     |  |  |
| Thetis Fido  |      |       |     |     |  |  |
| Trezor       |      |       |     |     |  |  |
| Tomu         |      |       |     |     |  |  |
| OnlyKey      |      |       |     |     |  |  |
| Librem Key   |      |       |     |     |  |  |
| U2F Zero     |      |       |     |     |  |  |
| GOOGLE TITAN |      |       |     |     |  |  |
| HyperFIDO    |      |       |     |     |  |  |
| OpenSK       |      |       |     |     |  |  |
| solokey      |      |       |     |     |  |  |

## Yubikey-Analogues

| name         | FIDO | FIDO2 | OTP | GPG | static password | static password manager | PIV | Challenge-response | version with nfc | can use self FW      | opensource |
|--------------|------|-------|-----|-----|-----------------|-------------------------|-----|--------------------|------------------|----------------------|------------|
| Yubikey 5    | +    | +     | +   | +   | +               | -                       | +   | +                  | +                | -                    | -          |
| Nitrokey     | +    | +     | +   | +   | +               | +?                      | +   | -                  | -                | -                    | +          |
| Thetis Fido  | +    | -     | -   | -   | -               | -                       | -   | -                  | -                | -                    | -          |
| Trezor       | +    | +     | -   | -   | -               | -                       | -   | -                  | -                | -                    | -          |
| ledger       | +    | -     | -   | -   | -               | -                       | -   | -                  | -                | -                    | -          |
| Tomu         | +    | +     | ?   | -   | -               | -                       | -   | -                  | -                | +                    | +          |
| OnlyKey      | +    | +     | +   | -   | -               | -                       | -   | -                  | -                | -                    | -          |
| Librem Key   | -    | -     | +   | -   | -               | -                       | -   | -                  | -                | -                    | +?         |
| U2F Zero     | +    | -     | -   | -   | -               | -                       | -   | -                  | -                | +                    | +          |
| GOOGLE TITAN | +    | -     | -   | -   | -               | -                       | -   | -                  | -                | -                    | -          |
| HyperFIDO    | +    | +     | -   | -   | -               | -                       | -   | -                  | -                | -                    | -          |
| OpenSK       | +    | +     | -   | -   | -               | -                       | -   | -                  | -                | +                    | +          |
| solokey      | +    | +     | -   | -   | -               | -                       | -   | -                  | +                | +(on unlock version) | +          |
| solokey 2    | +    | +     | +   | +?  | ?               | ?                       | +   | ?                  | +                | +(on unlock version) | +          |





<https://habr.com/ru/post/329648/>

<https://tomu.im/womu.html>

<https://habr.com/ru/company/globalsign/blog/500356/>

<https://www.yubico.com/products/compare-products-series/>

<https://www.yubico.com/solutions/passwordless/>

<https://www.nitrokey.com/>

<https://github.com/danstiner/rust-u2f>

<https://romannurik.github.io/SlidesCodeHighlighter/>

<https://developers.yubico.com/WebAuthn/>

<https://www.yubico.com/>

[https://raymii.org/s/tutorials/Three New Nitrokeys Pro 2 Storage 2 and Fido u2f.html#toc\\_11](https://raymii.org/s/tutorials/Three+New+Nitrokeys+Pro+2+Storage+2+and+Fido+u2f.html#toc_11)

<https://github.com/drduh/YubiKey-Guide#verify-yubikey>

<https://codingnest.com/how-to-use-gpg-with-yubikey-wsl/>

<https://habr.com/ru/post/354638/>

<https://habr.com/ru/post/305508/>

<https://webauthn.io/>

<https://codingnest.com/how-to-use-gpg-with-yubikey-wsl/>

<https://github.com/NZSmartie/npiperelay> (not work - analog wsl-ssh-pagean)

# Q&A

# Спасибо за внимание

Feel free to contact us:  
Tg: @Andryski @n0nvme



Telegram



Offtop &)