passbolt

$ whoami

✉ remy@pasbolt.com

Connect with me on LinkedIn

$ hostname

www.passbolt.com

/passbolt

@passbolt@mastodon.social

passbolt

Open-source password manager for teams

AICPA SOC

MADE IN LUXEMBOURG

fido ALLIANCE MEMBER

CYBERSECURITY MADE IN EUROPE

Authentication?

Asserting a user identity using something they:

know (passphrase, password, pin)
have (token, certificate, key)
are (biometric) or do (typing pattern, gait)

Password based authentication

Security issues:

- Credential stuffing.
- Phishing.
- Password loss.
- Bruteforce (online)
- Bruteforce (offline, in case of leak).

~ Adversary in the middle (network)

~ Password logging.

~ User enumeration

Implementation considerations:

+ Checking against breaches & entropy

~ User training

+ Account recovery

+ Captcha (+GDPR) / WAF / Alerts

+ “Costly” hashing mechanism (bcrypt)

+ HTTPs pinned and well configured

+ Additional client side hashing?

+ Vague error messages & constant time?

“Magic link” authentication

Security issues:

~ Phishing (email provider)

- User enumeration

- Man in the middle

~ Replay attack

- Email logging / intercept

UX issues:

- Context switch, email delays, etc.

Implementation considerations:

~ User training

+ Vague error messages & constant time?

+ HTTPs required, no HTTP fallback

+ One-off use, expiry date

+ TLS for SMTP, relays, etc.

- Email client “preview” counts as a click?

SMS authentication

Security issues:

- Phishing
- Adversary in the middle
- Bruteforce
- SIM Card swap
- Phone theft (notif on lock screen?)
- SMS interception
- Delays in receiving SMS

Implementation considerations:

- ~ User training
- ~ HTTPs required
- ~ Max failed attempts / throttling / Alerts
- ~ Choose a good carrier?
- ~ Set safe phone settings?

MFA/TOTP authentication

Security issues:

- Adversary in the middle (phishing site)
- Adversary in the middle (network)
- Bruteforce
- Sync’ without encryption

UX issues:

- Lost TOTP

Implementation considerations:

~ User training

+ HTTPs required, no HTTP fallback

+ Max failed attempts / throttling / Alerts

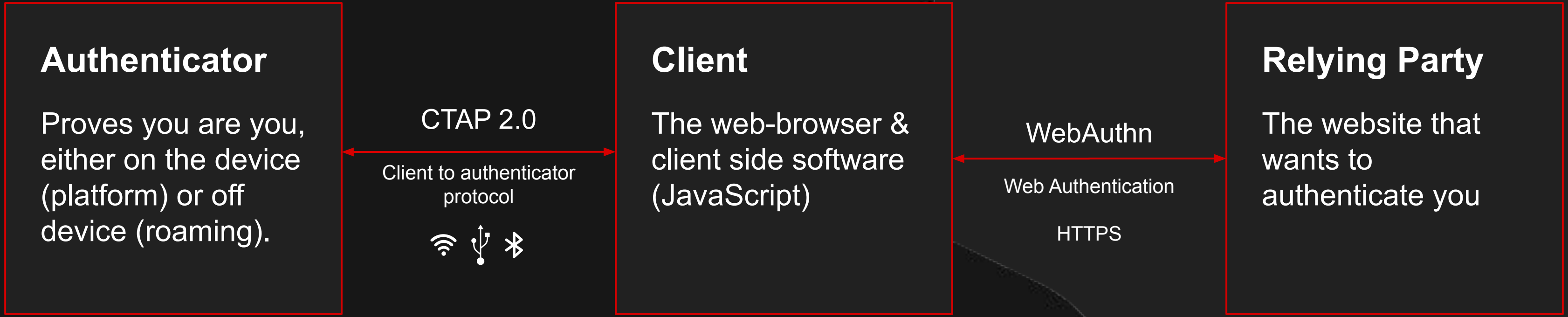
~ TOTP app preference?

+ Admin reset process? Another MFA?

FIDO2? Passkeys? Webauthn? U2F? CTAP?

FIDO2 Project

A joint effort between the FIDO Alliance and the W3C



Authenticator

Proves you are you, either on the device (platform) or off device (roaming).

CTAP 2.0

Client to authenticator protocol

Client

The web-browser & client side software (JavaScript)

WebAuthn

Web Authentication

HTTPS

Relying Party

The website that wants to authenticate you

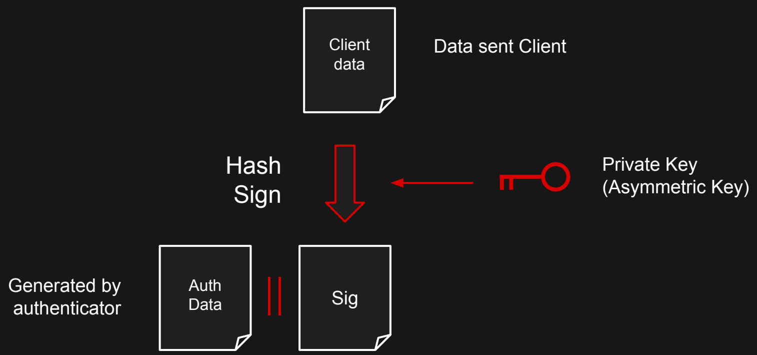
Examples:
iOS Keychain
Microsoft Hello
Yubikey
Dashlane

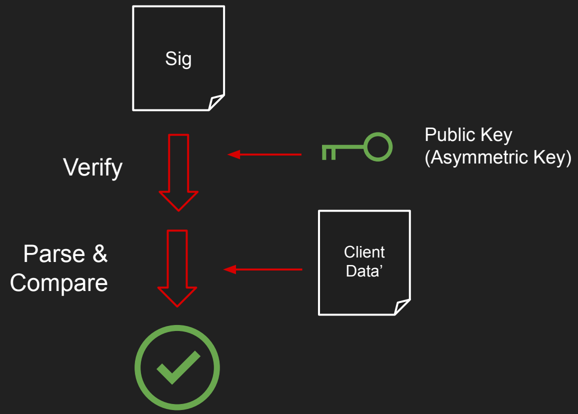
Examples:
Chrome
Firefox
Safari

Examples:
Google
etc.

Passkeys

A private-public keypair (credential) that can be used to authenticate
and that can be synced across multiple devices (as opposed to hardware bound).

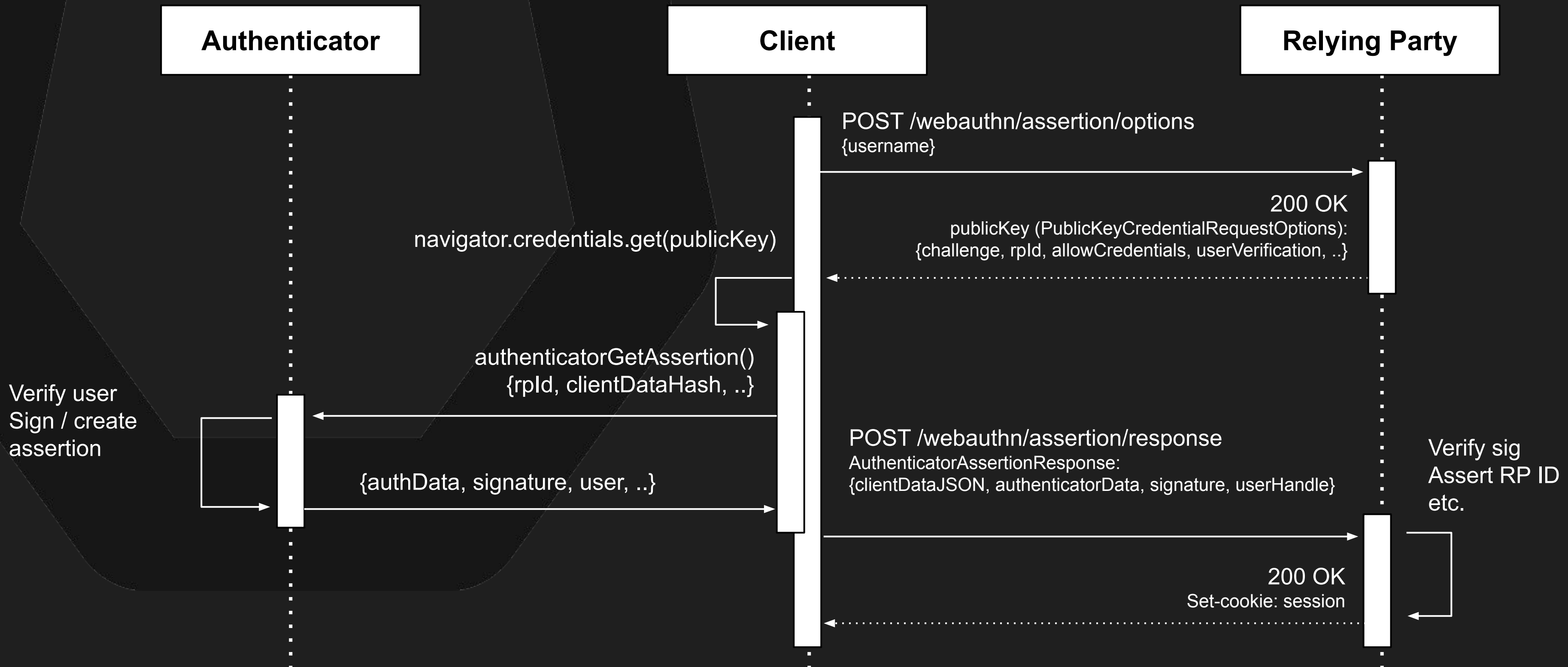




Sign | Verify

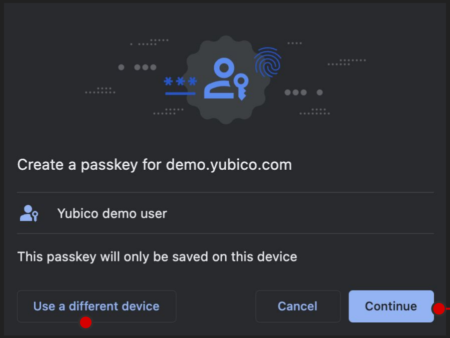
WebAuthn authentication

Assertion, e.g. authentication flow (login flow)


Authenticator
Client
Relying Party
POST /webauthn/assertion/options
{username}
200 OK
publicKey (PublicKeyCredentialRequestOptions):
{challenge, rpId, allowCredentials, userVerification, ..}
navigator.credentials.get(publicKey)
authenticatorGetAssertion()
{rpId, clientDataHash, ..}
Verify user
Sign / create
assertion
{authData, signature, user, ..}
POST /webauthn/assertion/response
AuthenticatorAssertionResponse:
{clientDataJSON, authenticatorData, signature, userHandle}
Verify sig
Assert RP ID
etc.
200 OK
Set-cookie: session

How does it look?

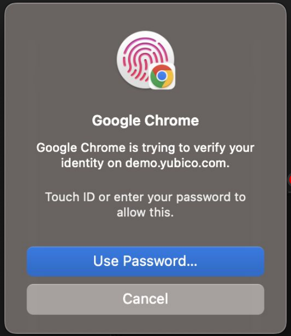
Registration on MacOS/Chrome



Create a passkey for demo.yubico.com

Yubico demo user

This passkey will only be saved on this device

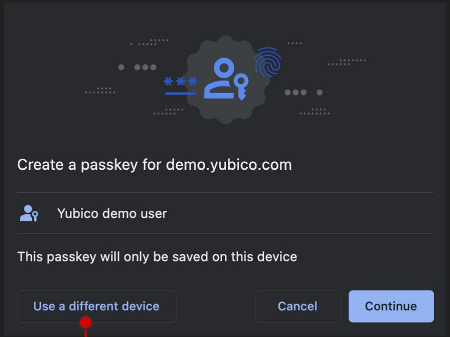


Google Chrome

Google Chrome is trying to verify your identity on demo.yubico.com.

Touch ID or enter your password to allow this.

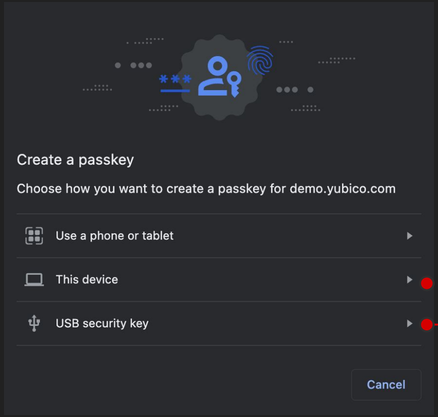
Registration on MacOS/Chrome



Create a passkey for demo.yubico.com

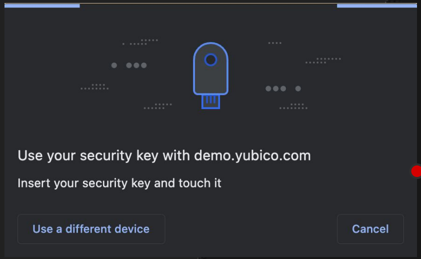
Yubico demo user

This passkey will only be saved on this device



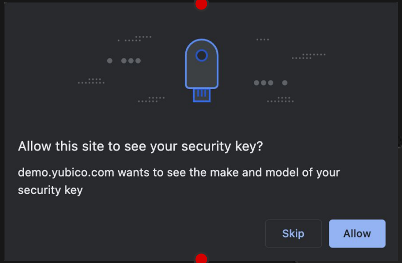
Create a passkey

Choose how you want to create a passkey for demo.yubico.com



Use your security key with demo.yubico.com

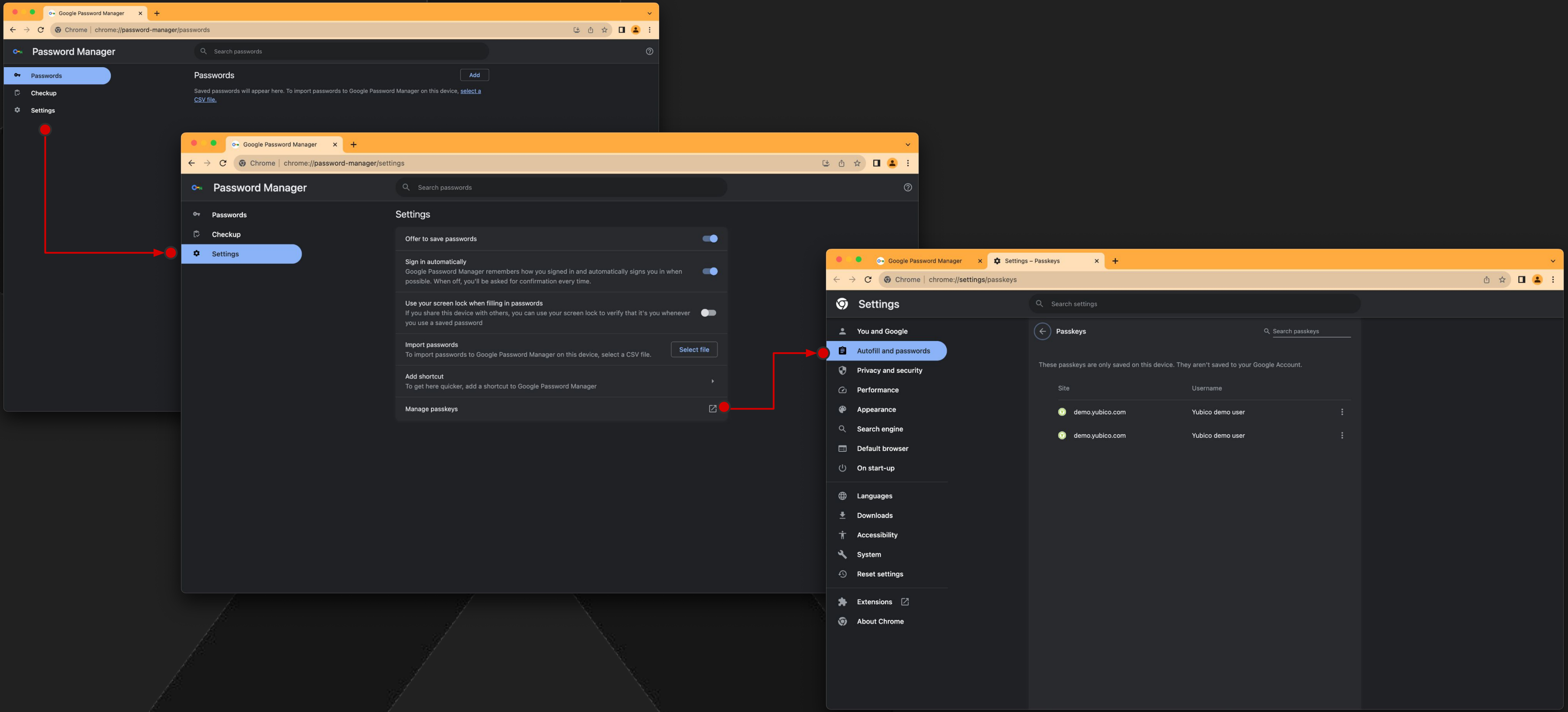
Insert your security key and touch it



Allow this site to see your security key?

demo.yubico.com wants to see the make and model of your security key

Managing passkeys on MacOS/Chrome



Passwords

Saved passwords will appear here. To import passwords to Google Password Manager on this device, select a CSV file.

Settings

Offer to save passwords

Sign in automatically
Google Password Manager remembers how you signed in and automatically signs you in when possible. When off, you'll be asked for confirmation every time.

Use your screen lock when filling in passwords
If you share this device with others, you can use your screen lock to verify that it's you whenever you use a saved password

Import passwords
To import passwords to Google Password Manager on this device, select a CSV file. Select file

Add shortcut
To get here quicker, add a shortcut to Google Password Manager

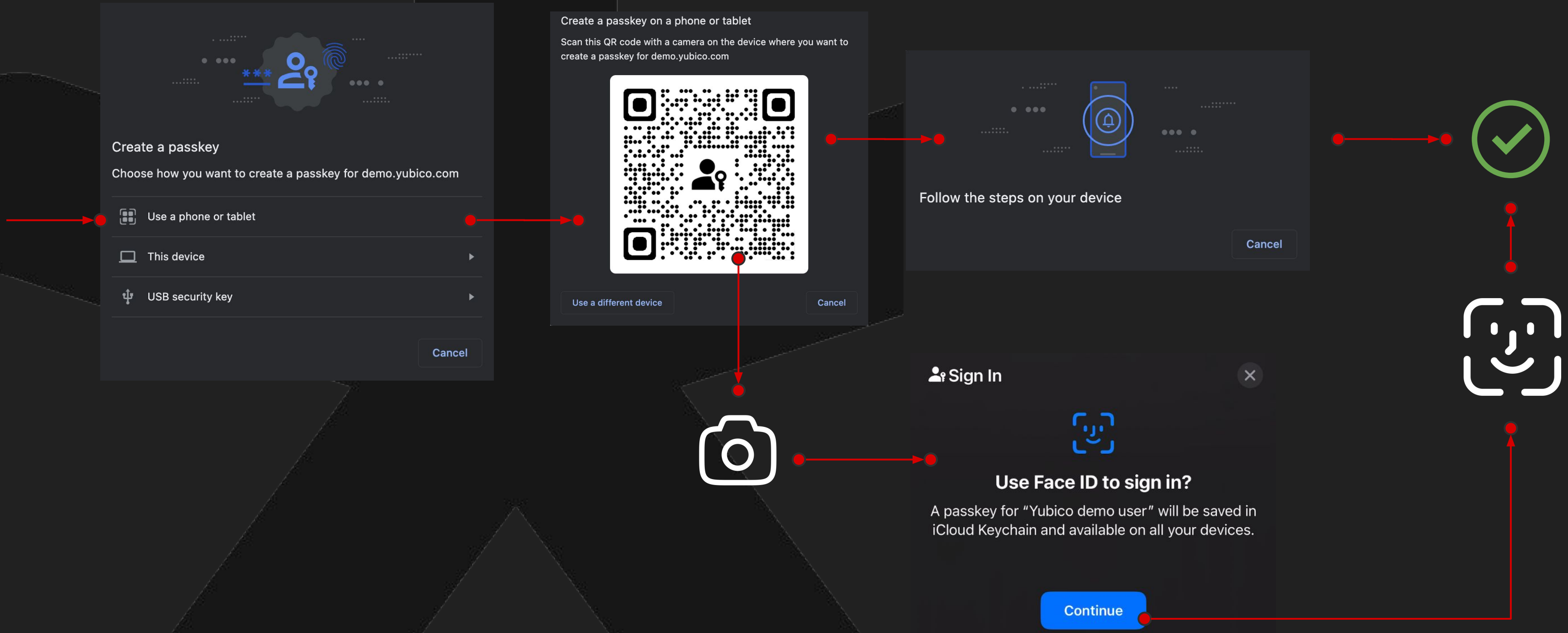
Manage passkeys

Passkeys

These passkeys are only saved on this device. They aren't saved to your Google Account.

Site	Username
demo.yubico.com	Yubico demo user
demo.yubico.com	Yubico demo user

Registration on MacOS/Chrome/iOS



Create a passkey

Choose how you want to create a passkey for demo.yubico.com

Create a passkey on a phone or tablet

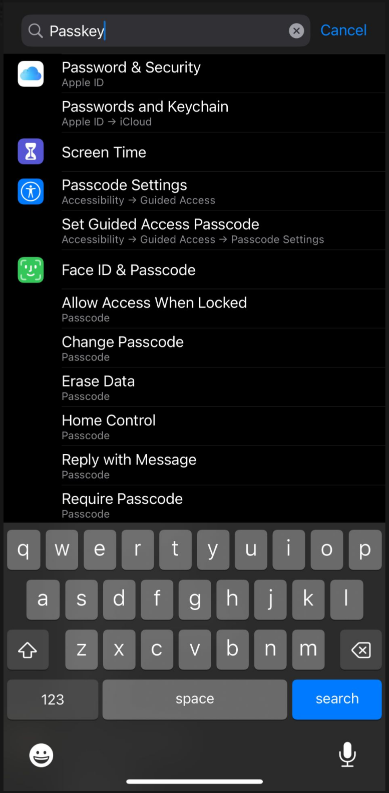
Scan this QR code with a camera on the device where you want to create a passkey for demo.yubico.com

Follow the steps on your device

Use Face ID to sign in?

A passkey for "Yubico demo user" will be saved in iCloud Keychain and available on all your devices.

Managing Pass~~words~~keys on iOS



Passkey

Cancel

Password & Security
Apple ID

Passwords and Keychain
Apple ID → iCloud

Screen Time

Passcode Settings
Accessibility → Guided Access

Set Guided Access Passcode
Accessibility → Guided Access → Passcode Settings

Face ID & Passcode

Allow Access When Locked
Passcode

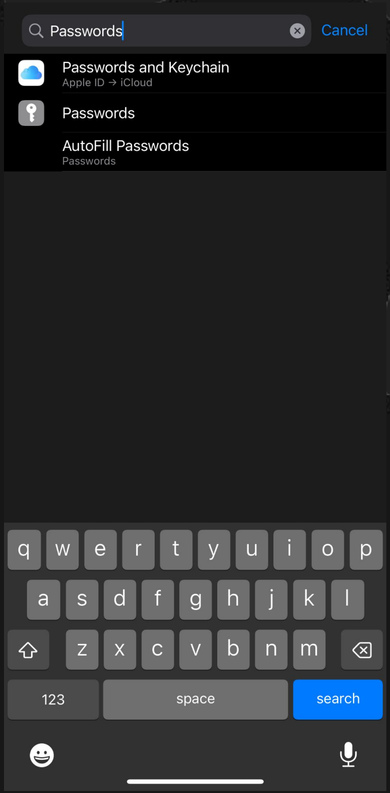
Change Passcode
Passcode

Erase Data
Passcode

Home Control
Passcode

Reply with Message
Passcode

Require Passcode
Passcode



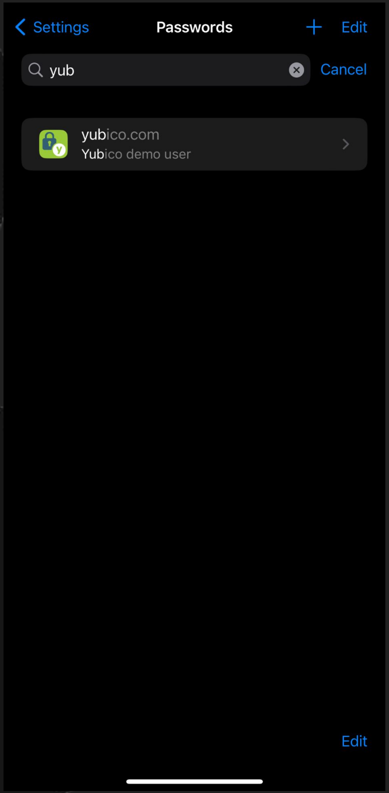
Passwords

Cancel

Passwords and Keychain
Apple ID → iCloud

Passwords

AutoFill Passwords
Passwords



Settings

Passwords

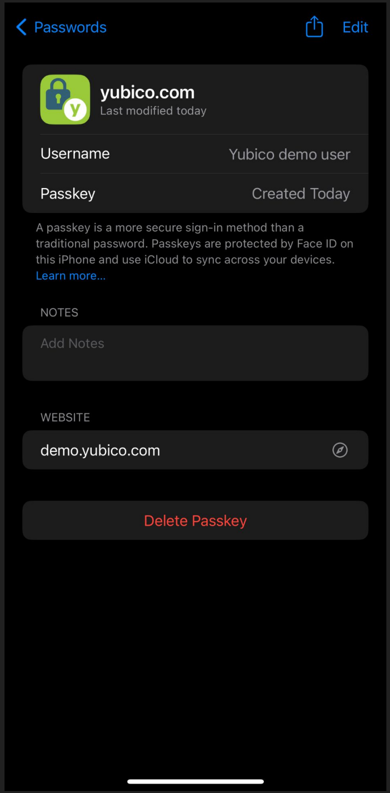
Edit

yub

Cancel

yubico.com
Yubico demo user

Edit



Passwords

Edit

yubico.com
Last modified today

Username: Yubico demo user

Passkey: Created Today

A passkey is a more secure sign-in method than a traditional password. Passkeys are protected by Face ID on this iPhone and use iCloud to sync across your devices. Learn more...

NOTES

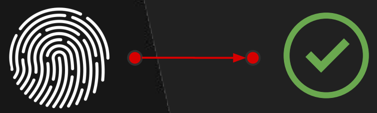
Add Notes

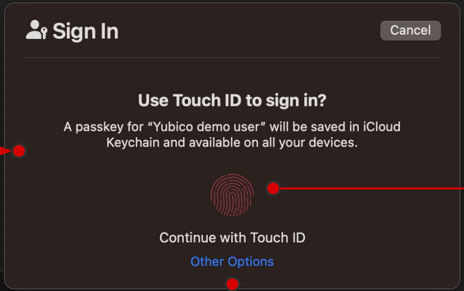
WEBSITE

demo.yubico.com

Delete Passkey

Registration on MacOS/Safari





Sign In

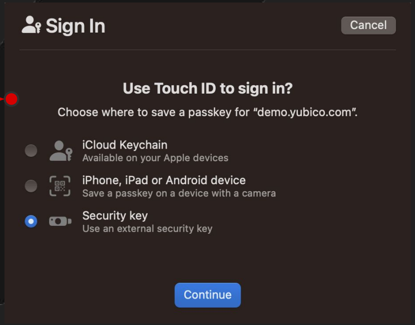
Cancel

Use Touch ID to sign in?

A passkey for “Yubico demo user” will be saved in iCloud Keychain and available on all your devices.

Continue with Touch ID

Other Options



Sign In

Cancel

Use Touch ID to sign in?

Choose where to save a passkey for “demo.yubico.com”.

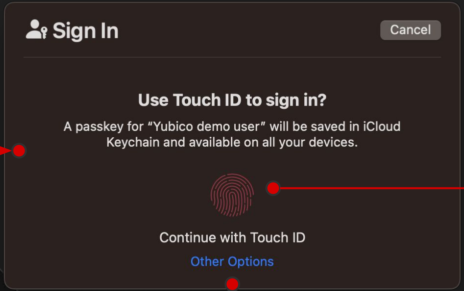
○ iCloud Keychain
Available on your Apple devices

○ iPhone, iPad or Android device
Save a passkey on a device with a camera

● Security key
Use an external security key

Continue

Registration on MacOS/Safari



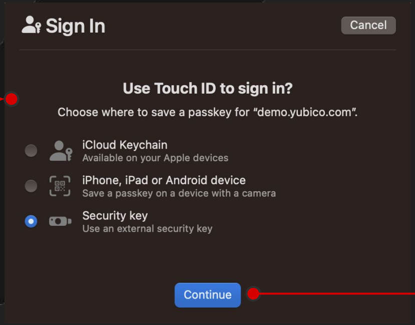
Sign In

Use Touch ID to sign in?

A passkey for "Yubico demo user" will be saved in iCloud Keychain and available on all your devices.

Continue with Touch ID

Other Options



Sign In

Use Touch ID to sign in?

Choose where to save a passkey for "demo.yubico.com".

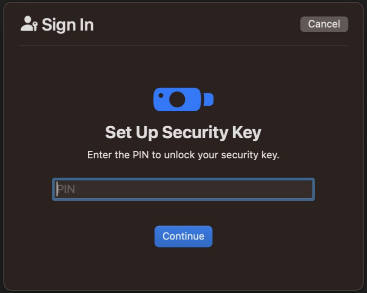
○ iCloud Keychain
Available on your Apple devices

○ iPhone, iPad or Android device
Save a passkey on a device with a camera

● Security key
Use an external security key

"Currently, YubiKeys can store a maximum of 25 passkeys." (if you've never entered a PIN when you registered your Yubikey you are not using resident keys).

🤔



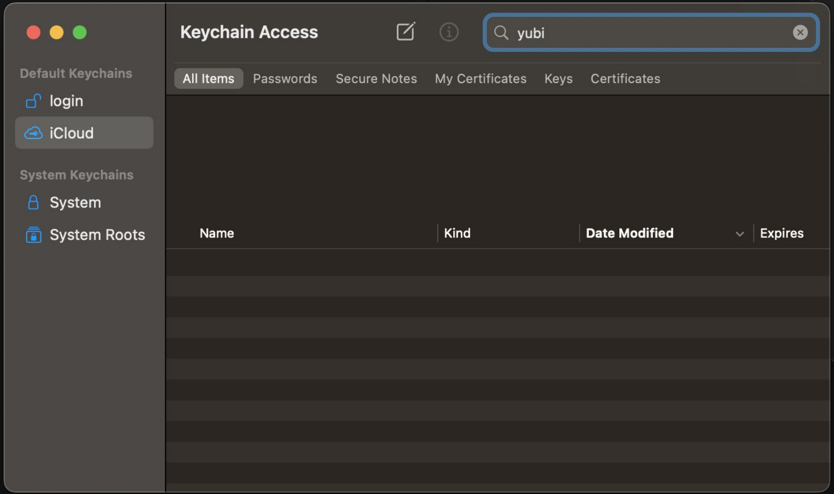
Sign In

Set Up Security Key

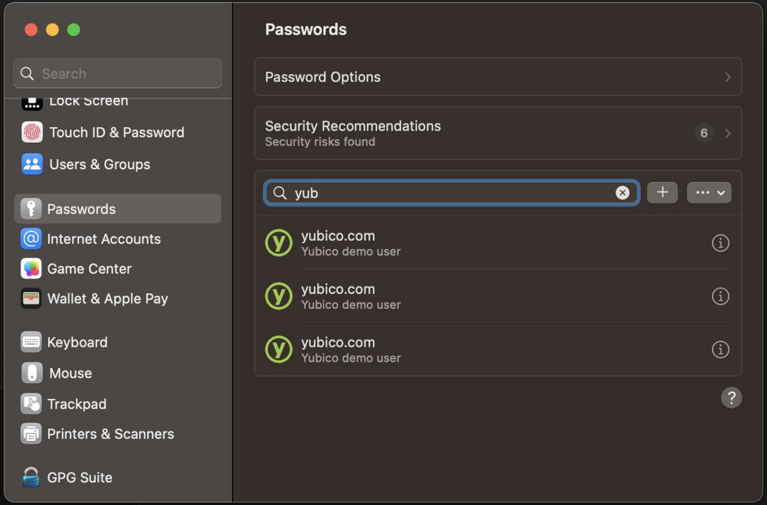
Enter the PIN to unlock your security key.

PIN

Managing Pass~~words~~keys on MacOS



yubi



yub

yubico.com
Yubico demo user

yubico.com
Yubico demo user

yubico.com
Yubico demo user

Will be saved in iCloud Keychain?

Will be stored in settings > passwords!

Recovery of passkeys (iCloud)

“Passkeys can be recovered through iCloud keychain escrow, which is also protected against brute-force attacks, even by Apple. [...]

To recover a keychain, a user must authenticate with their iCloud account and password and respond to an SMS sent to their registered phone number. After they authenticate and respond, the user must enter their device passcode. iOS, iPadOS, and macOS allow only 10 attempts to authenticate. After several failed attempts, the record is locked and the user must call Apple Support to be granted more attempts. After the tenth failed attempt, the escrow record is destroyed.

Optionally, a user can set up an account recovery contact [...].”

Ref. https://support.apple.com/en-gb/guide/security/sec3e341e75d/web

Passwords security issues

Security issues:

- ~~Credential stuffing.~~
- ~~Adversary in the middle (phishing).~~
- Pass~~word~~keys loss.
- ~~Bruteforce (online)~~
- ~~Bruteforce (offline, in case of leak).~~
- ~~Adversary in the middle (network)~~
- ~~Password logging.~~

~ User enumeration

Implementation considerations:

+ ~~Checking against breaches & entropy~~

~ User training

~ Account recovery

+ ~~Captcha (+GDPR) / WAF / Alerts~~
+ ~~“Costly” hashing mechanism (bcrypt)~~
+ ~~HTTPs pinned and well configured~~
+ ~~Additional client side hashing?~~
+ See small prints

Passkeys security issues

Security issues:

- Passkeys loss (device loss)

~ Physical Proximity (BLE, NFC)

- Passkey management & review

~ Passkeys availability to admins?

- User enumeration

~ Root CA leak / rotation

~ Quantum computers?

~ more, see Security considerations

Implementation considerations:

~ Account recovery? More passkeys?

~ Accept risk?

~ User training? Better UX? Alerts?

~ Better signalization of sharing props

~ Username-less design

~ Passkey rotations

~ PQC, crypto agility

Passkeys issues

Other issues:

- End user experience

~ Specs stabilization?

- Authenticator gatekeeping?
- Pay to play / Diversity?
- Open-source ecosystem support

Other considerations:

~ UX Working group

~ Traction?

~ Monkey patching? Fines?

~ Get involved?

~ Get involved!

Thank you!

Any questions?