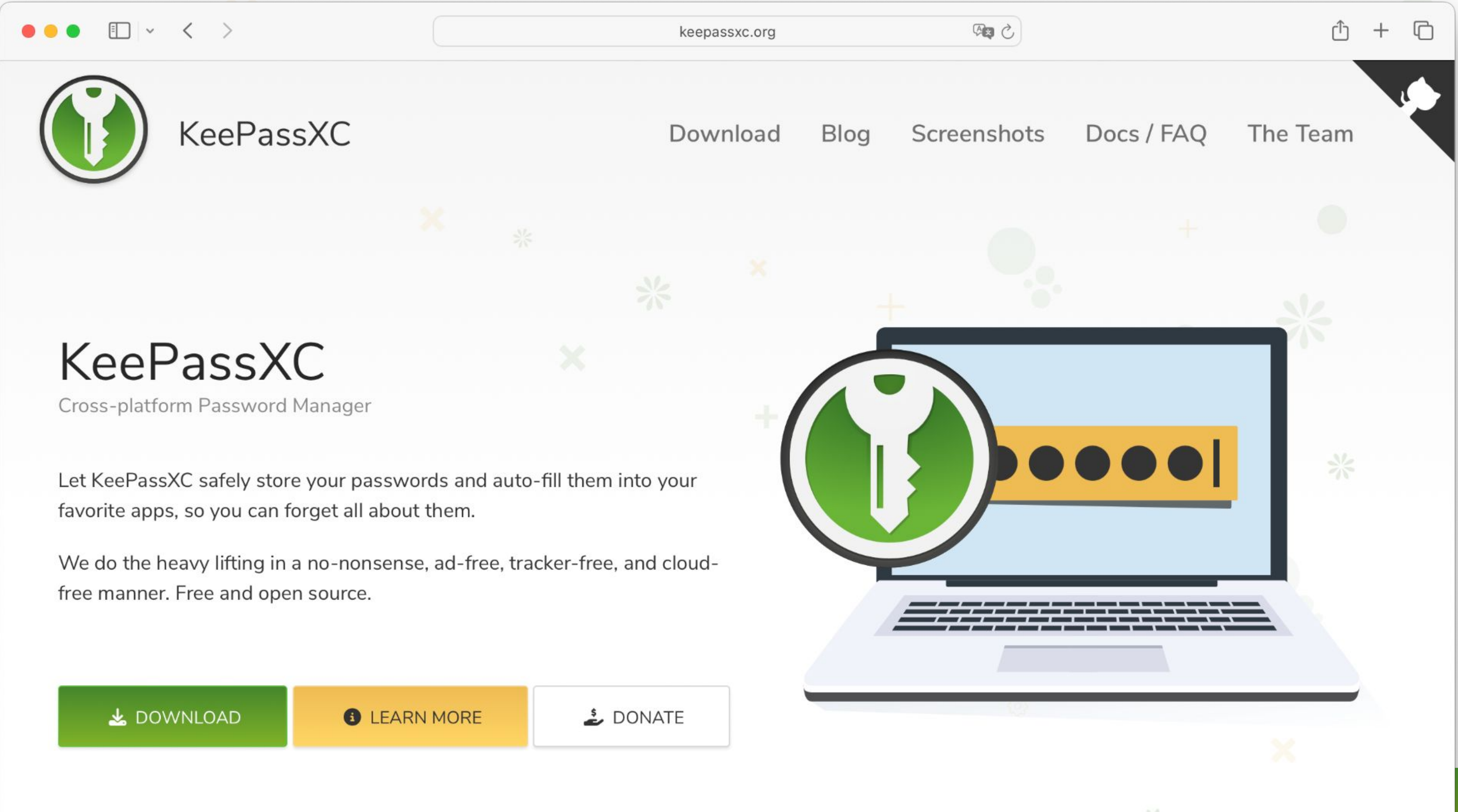
Passkeys With KeePassXC

An Introduction

Janek Bevendorff (KeePassXC Maintainer)
Freiburger Linux User Group, 17.09.2025

Outline

1. What is KeePassXC?
2. The problem with passwords.
3. What are passkeys and how do they work?
4. Using passkeys with KeePassXC.

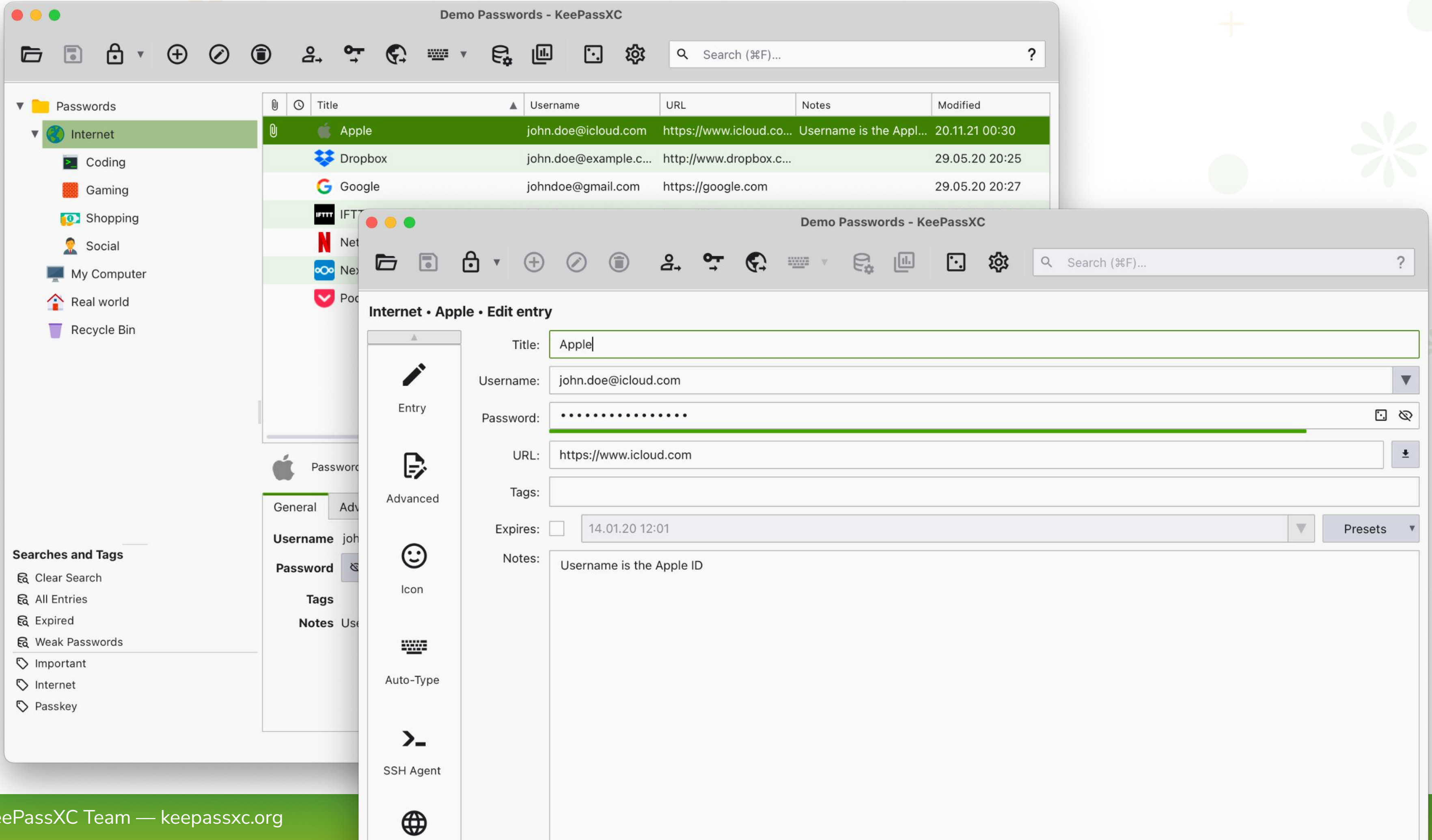


KeePassXC

Cross-platform Password Manager

Let KeePassXC safely store your passwords and auto-fill them into your favorite apps, so you can forget all about them.

We do the heavy lifting in a no-nonsense, ad-free, tracker-free, and cloud-free manner. Free and open source.



Demo Passwords - KeePassXC

Search (⌘F)...

- Passwords
  - Internet
    - Coding
    - Gaming
    - Shopping
    - Social
  - My Computer
  - Real world
  - Recycle Bin

Title	Username	URL	Notes	Modified
Apple	john.doe@icloud.com	https://www.icloud.co...	Username is the Appl...	20.11.21 00:30
Dropbox	john.doe@example.c...	http://www.dropbox.c...		29.05.20 20:25
Google	johndoe@gmail.com	https://google.com		29.05.20 20:27
IFTT				
Net				
Nex				
Poc				

Searches and Tags

- Clear Search
- All Entries
- Expired
- Weak Passwords
- Important
- Internet
- Passkey

Passwor

General | Adv

Username joh

Password

Tags

Notes Use

Demo Passwords - KeePassXC

Search (⌘F)...

Internet • Apple • Edit entry

Entry

Advanced

Icon

Auto-Type

SSH Agent

Title: Apple

Username: john.doe@icloud.com

Password: ••••••••••••••••

URL: https://www.icloud.com

Tags:

Expires: □ 14.01.20 12:01 Presets

Notes: Username is the Apple ID

KeePass? KeePassX? KeePassXC?

2003–today

keepass.info

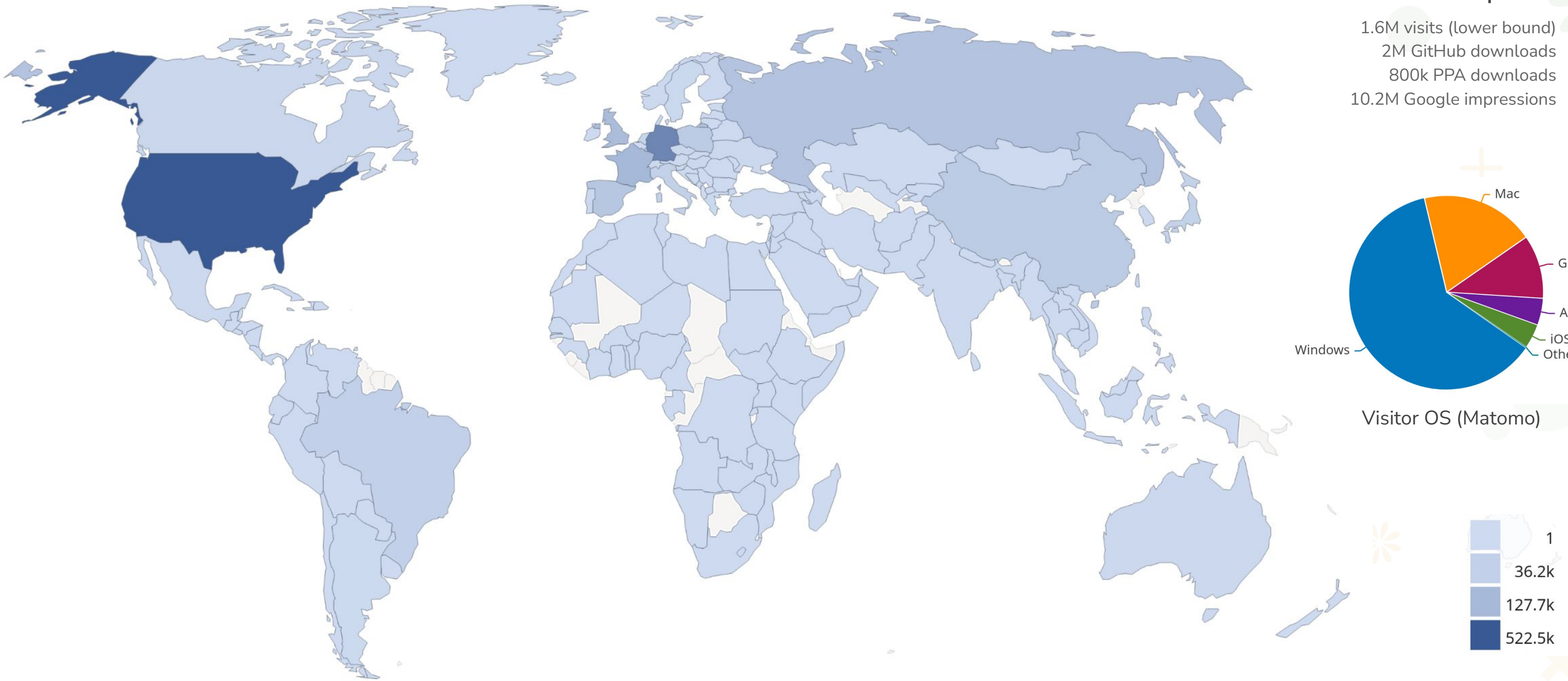
2005–2016

keepassx.org

2016–today

keepassxc.org

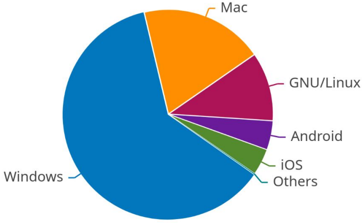
KeePassXC User World Map



Website Visits 2025 (Matomo)

Jan–Sep 2025:

1.6M visits (lower bound)
2M GitHub downloads
800k PPA downloads
10.2M Google impressions



Visitor OS (Matomo)

Password Security

Which password is best?

- `qwerty`
- `asdf!123`
- `H3110 w0r1d!11`
- `6F$j5CA#@,OS`
- `opiCqjfWMwgSxeIQ8kNFovfup8YfwN`
- `]÷O¯¤Ú®mKá¯û`
- `thaw unsmooth debate straggler syndrome tiara spotless poise`

Password Security

Which password is best?

- `qwerty` (~2 bit, ≪ 1 second to crack)
- `asdf!123` (~15 bit, 0.000001 seconds)
- `H3110 w0r1d!11` (~32 bit, 0.1 seconds)
- `6F$j5CA#@,OS` (~79 bit, 436.000 years)
- `opiCqjfWMwgSxeIQ8kNFovfup8YfwN` (~197 bit, 3.4x10^{23} times age of the universe)
- `]÷O¯¤Ú®mKá¯û` (~94 bit)
- `thaw unsmooth debate straggler syndrome tiara spotless poise` (~192 or 103 bit)

Cracking times: Single RTX 4090 with 22.000 MH/s (crude estimate)

Password Security

Which password is best?

- `qwerty` (~2 bit, « 1 second to crack)
- `asdf!123` (~15 bit, 0.000001 seconds)
- `H3110 w0r1d!11` (~32 bit, 0.2 seconds)
- `6F$j5CA#@,OS` (~70 bit, 41.000 years)
- `opiCqjfWMwgSxeIQ8kNFovfup8YfwN` (~162 bit, 4.7x10^{14} times age of the universe)
- `]÷O¯¤Ú®mKá¯û` (~150 bit)
- `thaw unsmooth debate straggler syndrome tiara spotless poise` (~192 or 103 bit)

(All bad — don't put passwords on slides!)

Cracking times: Single RTX 4090 with 22.000 MH/s (crude estimate)

Problems With Passwords

- Hard to remember (PMs solve this).
- Cumbersome to use (PMs *try* to solve this).
- Prone to phishing (PM browser extensions make phishing harder).
- Reuse makes users vulnerable (PMs discourage reuse).
- Must be changed when service compromised (PMs cannot solve this).

⇝ Passkeys are meant to solve all of the above.

Passkeys Aren’t Perfect

- Web service must support it.
- Cannot replace your banking PIN, locker combination, etc.
- Not meant for offline data encryption (but can be done).
- Hardware authenticators have limited storage capacity.
- Software authenticators vulnerable to malware.
- Import / export formats still work in progress.
- Standard allows enforcement of specific authenticators (vendor lock-in).

Passkeys: A Short History

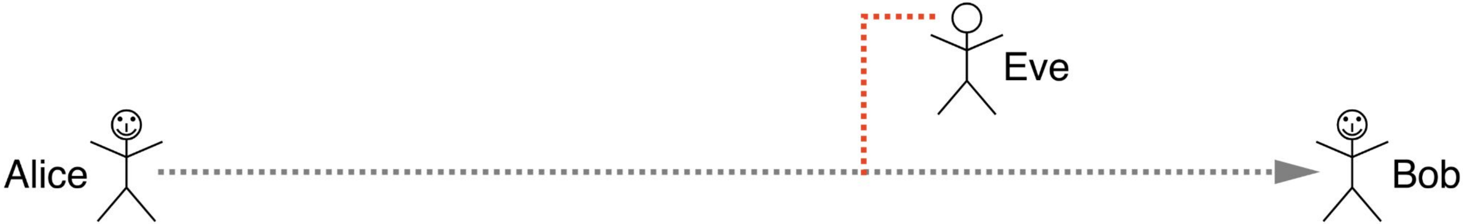
- 2013: FIDO Alliance founded
- 2014: Universal 2nd Factor (U2F) 1.0 standard released
- 2015: FIDO 2.0 proposal submitted to W3C
- 2017: U2F 1.2 standard released
- 2018: Client To Authenticator Protocol 2.0 (CTAP2) standard proposed
  - U2F renamed to CTAP1
- 2019: W3C WebAuthn Level 1 recommendation published
- 2020: Most major browsers support FIDO2
- 2022: Chrome and Safari ship native Passkey support
- 2024: Firefox supports native Passkeys as last major browser

Image credits: Yubico

FIDO? CTAP? WebAuthn? Passkey?

- FIDO (Fast IDentity Online)
  - FIDO Alliance = The Consortium.
  - FIDO1 + FIDO2 = The parent specifications for everything below.
- CTAP
  - Protocol for talking to FIDO authenticators.
  - CTAP1 is the same as U2F.
  - CTAP2 is one of two parts of the FIDO2 specification.
- WebAuthn
  - W3C-standardised API for initiating passwordless user authentication (via CTAP).
  - WebAuthn is the second part of the FIDO2 specification.
- Passkeys
  - Marketing term by Apple without clear definition.
  - Usually refers to (discoverable) FIDO2 credential key pair.
  - Windows, macOS, iOS, Android have native passkey support (Linux in the works).

Excursion: Public Key Cryptography



Principles of secure information systems (there are two more):

- **Confidentiality:** The message must remain secret
- **Integrity:** The message must be unchanged
- **Authenticity:** The source must be trustworthy

Source: Stein, Bevendorff – webis.de (German)

Excursion: Public Key Cryptography

Let P be the set of all texts (*plain texts*), K the set of all keys, C the set of all encrypted texts (*cipher texts*), and e_k, d_k two functions:

$$\begin{array}{lcl} e_k : P \longrightarrow C & & \\ & \text{with} & d_k(e_k(x)) = x, \quad x \in P, \ k \in K \\ d_k : C \longrightarrow P & & \end{array}$$

Problem: Transmission of the (secret) key k.

Source: Stein, Bevendorff – webis.de (German)

Excursion: Public Key Cryptography

Idea: Alice and Bob each have two keys k_{pub} (public) and k_{priv} (private) so that

$$d_{k_{\text{pub}}}(e_{k_{\text{priv}}}(x)) = e_{k_{\text{priv}}}(d_{k_{\text{pub}}}(x))$$

Steps of asymmetric encryption:

1. Alice and Bob choose keys k^A_{pub}, k^A_{priv} and k^B_{pub}, k^B_{priv}.
2. Both publish their public keys k^A_{pub}, k^B_{pub}.
3. Alice sends message x as $y = e_{k^B_{\text{pub}}}(x)$ to Bob.
4. Bob decrypts y and gets $x = d_{k^B_{\text{priv}}}(y)$.

Source: Stein, Bevendorff – webis.de (German)

Excursion: Public Key Cryptography

How does Alice know that Bob and not Eve is the sender of x?

Digital signatures:

Let $h : P \longrightarrow N$ be a *hash function*, which calculates for x a unique characterisation $h(x)$ of fixed length (“message digest”).

Source: Stein, Bevendorff – webis.de (German)

Excursion: Public Key Cryptography

How does Alice know that Bob and not Eve is the sender of x?

Digital signatures:

Let $h : P \longrightarrow N$ be a *hash function*, which calculates for x a unique characterisation $h(x)$ of fixed length ("message digest").

1. Alice calculates for x the hash value $h(x)$.
2. Alice encrypts $h(x)$ as $y_h = e_{k^A_{\text{priv}}}(h(x))$.
3. Alice sends $y = e_{k^B_{\text{pub}}}(x+y_h)$ to Bob.
4. Bob decrypts $x+y_h = d_{k^B_{\text{priv}}}(y)$.
5. Bob calculates $h(x)$ and $d_{k^A_{\text{pub}}}(y_h)$ and compares values.

Source: Stein, Bevendorff – webis.de (German)

Universal Second Factor (U2F)

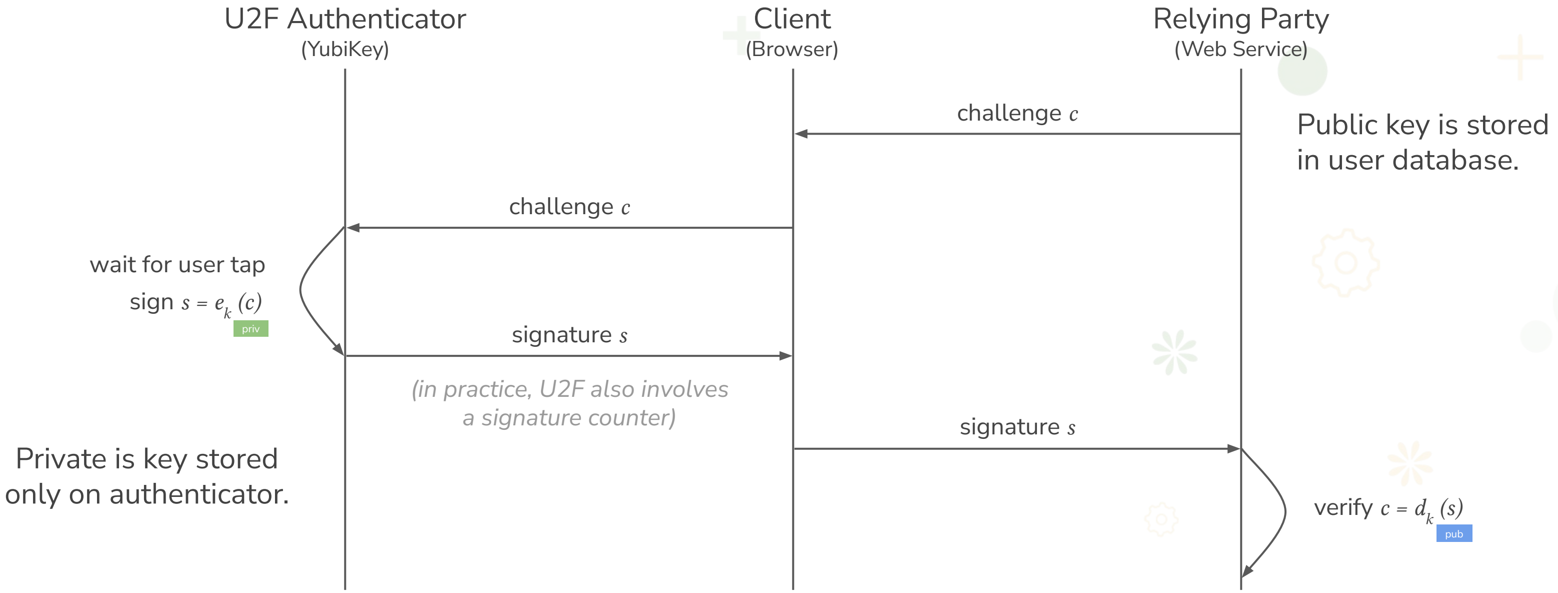
Traditionally, authentication factors are defined as:

- **Something you know** (password, PIN, …)
- **Something you have** (smart card, OTP generator, TAN list, …)
- **Something you are** (facial recognition, fingerprint, other biometrics, …)

⇝ Ideally, you have at least two.

Universal Second Factor (U2F)

U2F devices model **“something you have”** with public key crypto:



Public key is stored in user database.

(in practice, U2F also involves a signature counter)

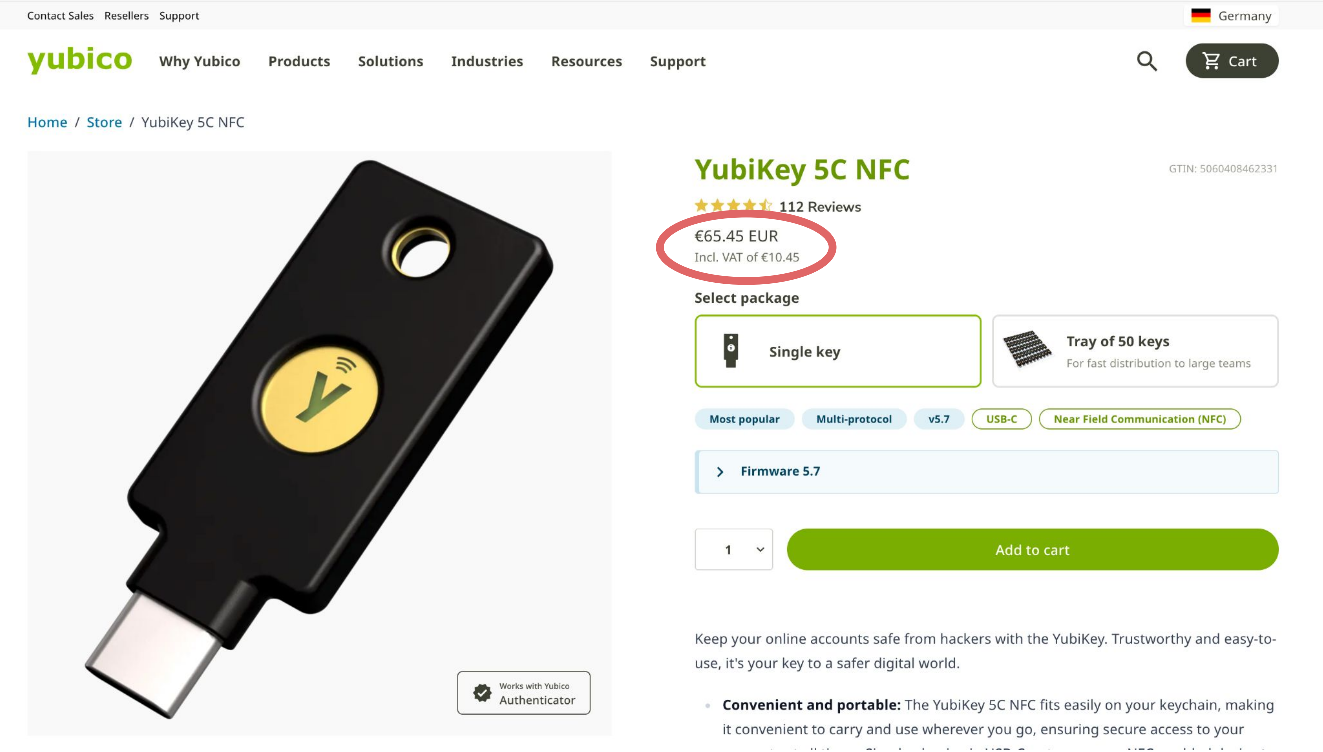
Private is key stored only on authenticator.

Going Passwordless With FIDO2

Main improvements over FIDO U2F:

- Proper API standardisation (WebAuthn)
- Individual (pass)keys per user and service
- Discoverable credentials (resident keys)
- Passwordless MFA via PIN or biometrics
- Platform authenticators ⇝ *KeePassXC*

Going Passwordless With FIDO2



Home / Store / YubiKey 5C NFC

YubiKey 5C NFC

GTIN: 5060408462331

112 Reviews

€65.45 EUR
Incl. VAT of €10.45

Select package

- Single key
- Tray of 50 keys — For fast distribution to large teams

Most popular · Multi-protocol · v5.7 · USB-C · Near Field Communication (NFC)

Firmware 5.7

1 — Add to cart

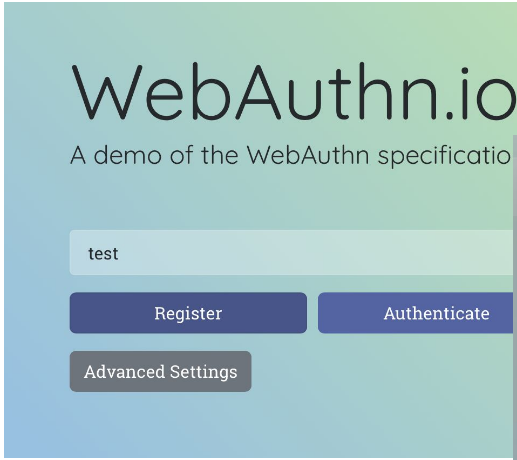
Keep your online accounts safe from hackers with the YubiKey. Trustworthy and easy-to-use, it's your key to a safer digital world.

- **Convenient and portable:** The YubiKey 5C NFC fits easily on your keychain, making it convenient to carry and use wherever you go, ensuring secure access to your

Screenshot: yubico.com

Passkey Authentication Workflow

1.



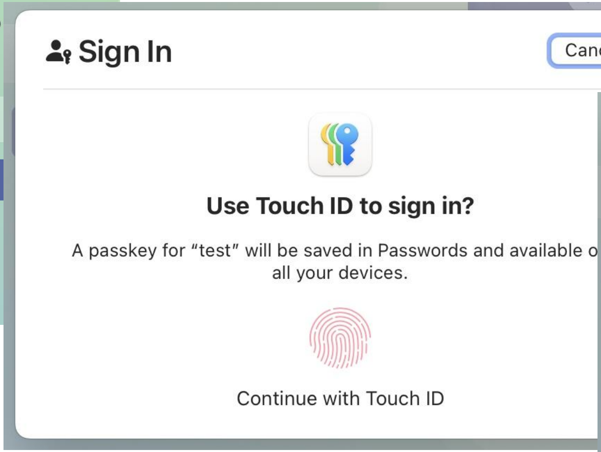
WebAuthn.io

A demo of the WebAuthn specificatio

test

Register

2.



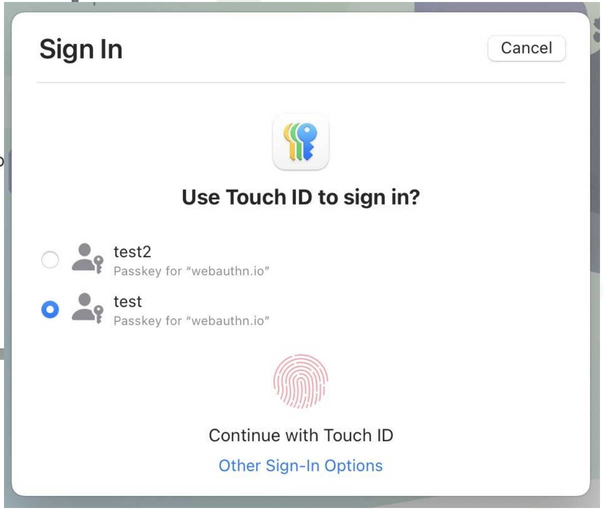
Sign In

Use Touch ID to sign in?

A passkey for “test” will be saved in Passwords and available o all your devices.

Store passkey

3.



Sign In

Use Touch ID to sign in?

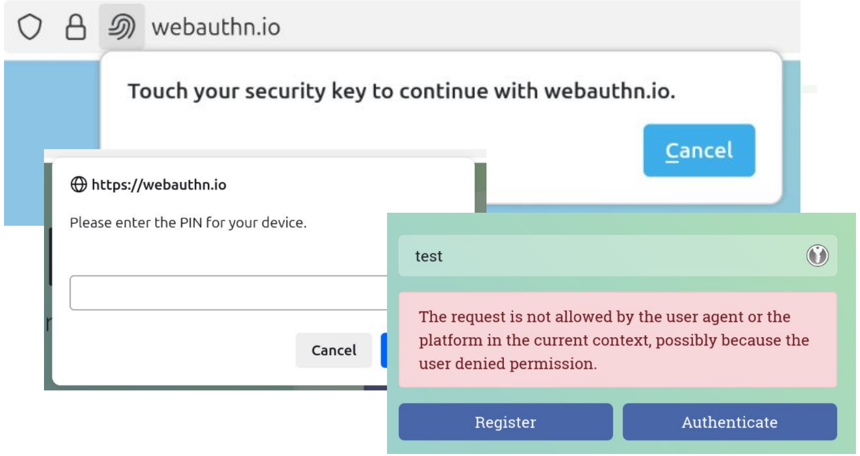
○ test2
Passkey for “webauthn.io”

● test
Passkey for “webauthn.io”

Authenticate

Linux: No Native Passkeys (Yet)

Firefox



Touch your security key to continue with webauthn.io.

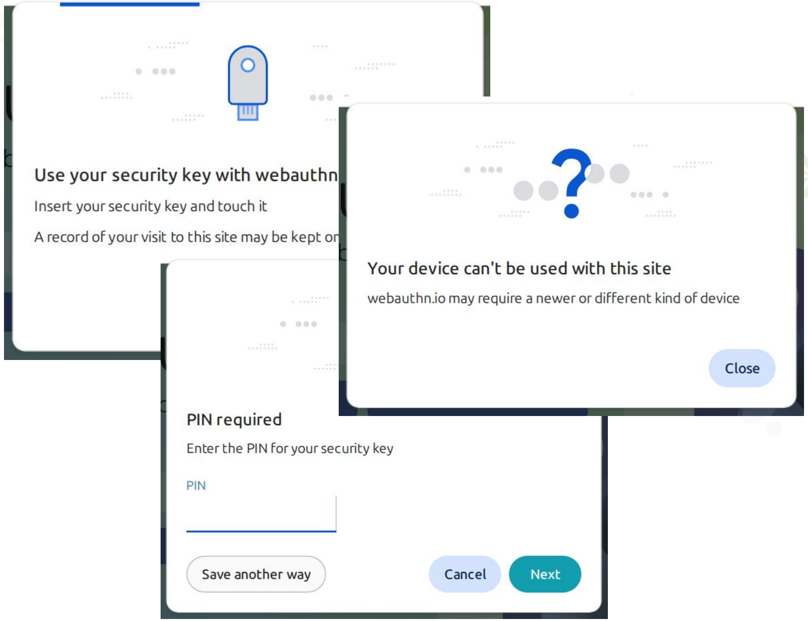
https://webauthn.io

Please enter the PIN for your device.

test

The request is not allowed by the user agent or the platform in the current context, possibly because the user denied permission.

Chrome



Use your security key with webauthn

Insert your security key and touch it

A record of your visit to this site may be kept or

Your device can't be used with this site

webauthn.io may require a newer or different kind of device

PIN required

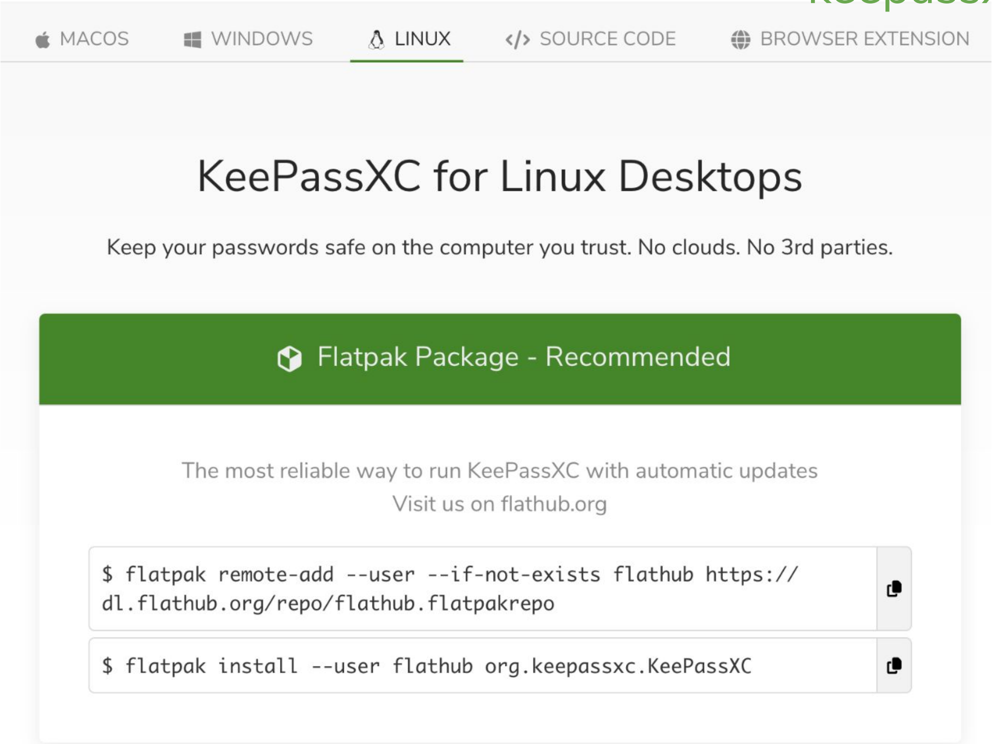
Enter the PIN for your security key

PIN:

YubiKey: ✅ Platform: ❌

Passkeys With KeePassXC

↝ keepassxc.org/download/



KeePassXC for Linux Desktops

Keep your passwords safe on the computer you trust. No clouds. No 3rd parties.

Flatpak Package - Recommended

The most reliable way to run KeePassXC with automatic updates

Visit us on flathub.org

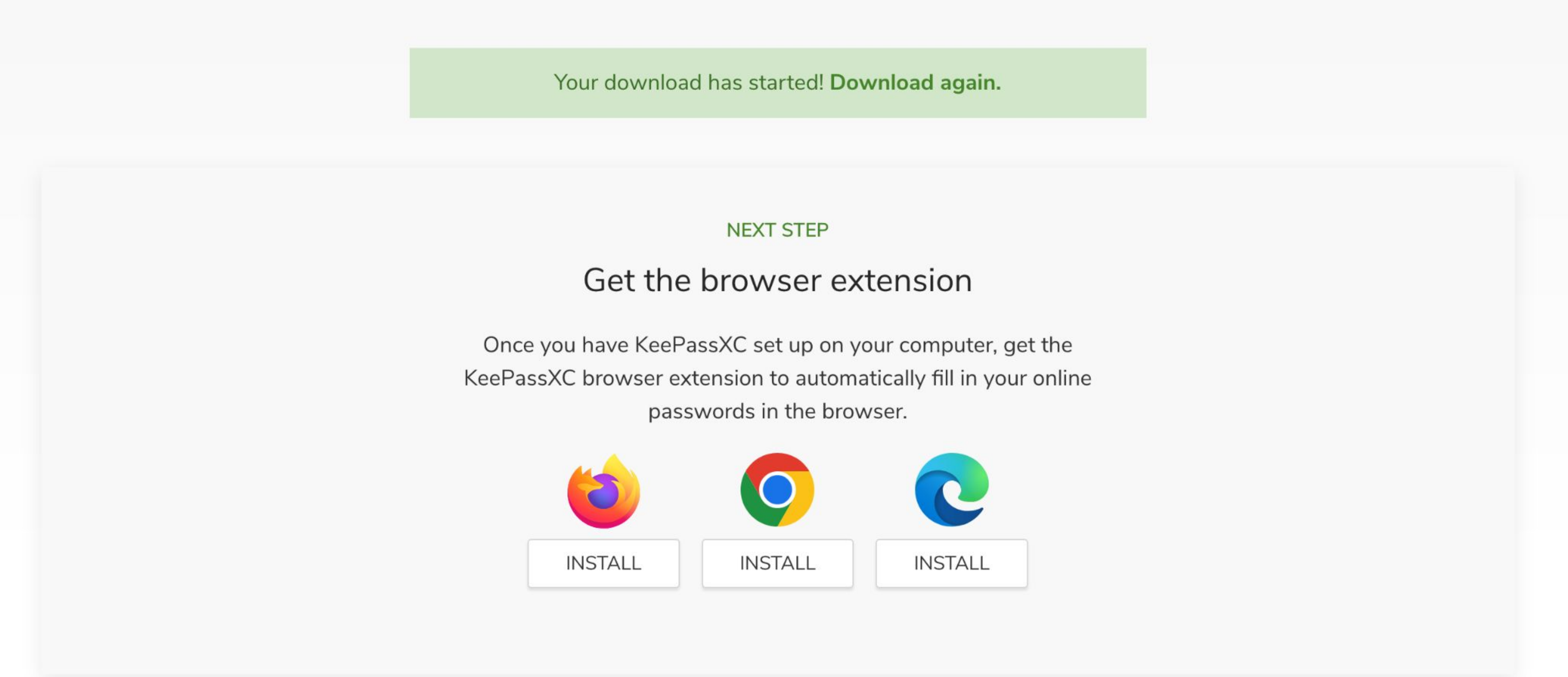
```
$ flatpak remote-add --user --if-not-exists flathub https://dl.flathub.org/repo/flathub.flatpakrepo
```

```
$ flatpak install --user flathub org.keepassxc.KeePassXC
```

Linux Tips:

- Flatpak or PPA are fine
- AppImage if you need to
- Distro package if not too old
- Avoid Snaps

Passkeys With KeePassXC



Your download has started! **Download again.**

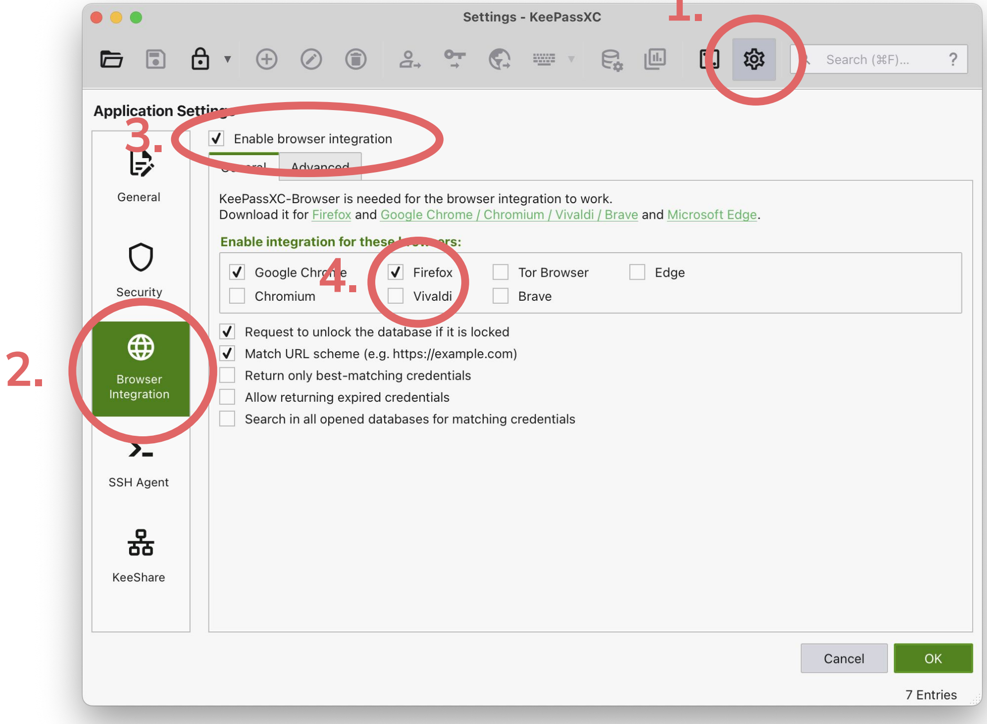
NEXT STEP

Get the browser extension

Once you have KeePassXC set up on your computer, get the KeePassXC browser extension to automatically fill in your online passwords in the browser.

Important: Snap / Flatpak browsers are not supported!

Enable Browser Integration



Application Settings

☑ Enable browser integration

General | Advanced

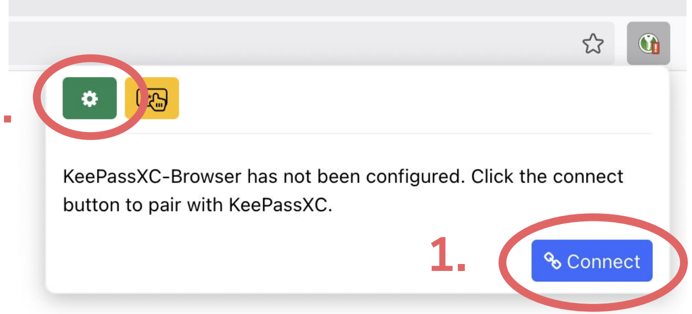
KeePassXC-Browser is needed for the browser integration to work.
Download it for Firefox and Google Chrome / Chromium / Vivaldi / Brave and Microsoft Edge.

Enable integration for these browsers:

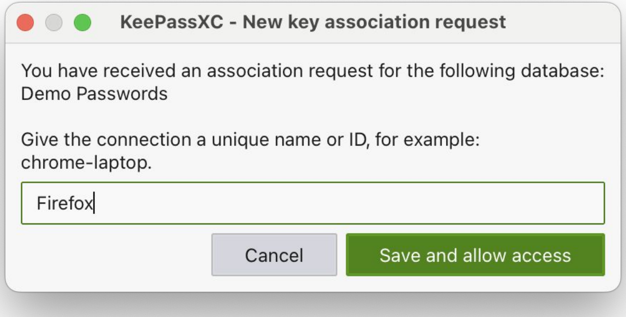
☑ Google Chrome ☑ Firefox □ Tor Browser □ Edge
□ Chromium □ Vivaldi □ Brave

☑ Request to unlock the database if it is locked
☑ Match URL scheme (e.g. https://example.com)
□ Return only best-matching credentials
□ Allow returning expired credentials
□ Search in all opened databases for matching credentials

Connect KeePassXC-Browser



KeePassXC-Browser has not been configured. Click the connect button to pair with KeePassXC.

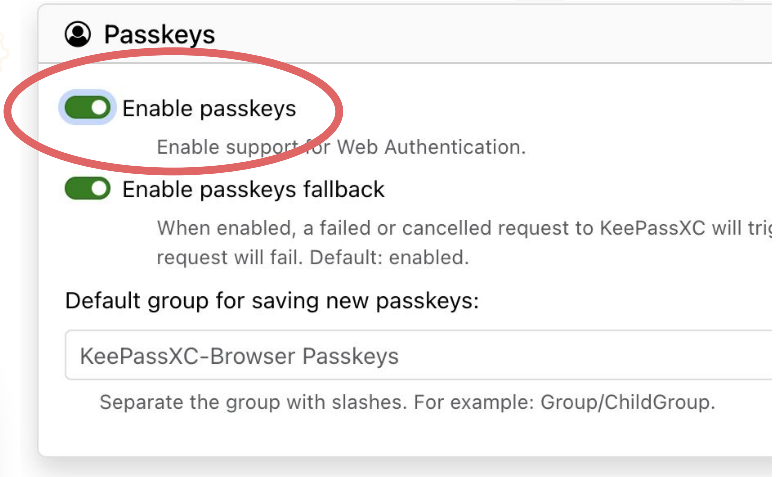


KeePassXC - New key association request

You have received an association request for the following database:
Demo Passwords

Give the connection a unique name or ID, for example:
chrome-laptop.

Firefox



Passkeys

● Enable passkeys
Enable support for Web Authentication.

● Enable passkeys fallback
When enabled, a failed or cancelled request to KeePassXC will trig
request will fail. Default: enabled.

Default group for saving new passkeys:

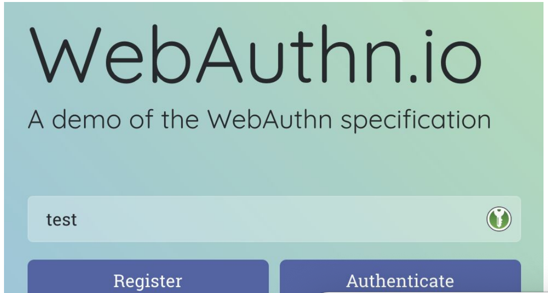
KeePassXC-Browser Passkeys

Separate the group with slashes. For example: Group/ChildGroup.

Register New Passkey

Register new passkey

1.

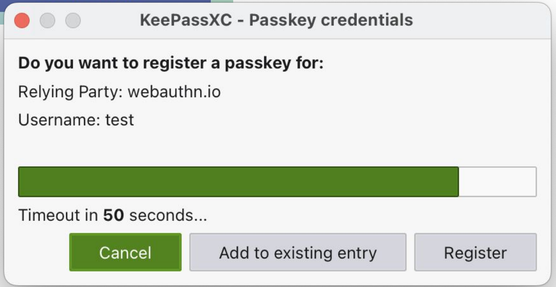


WebAuthn.io

A demo of the WebAuthn specification

test

2.



KeePassXC - Passkey credentials

Do you want to register a passkey for:

Relying Party: webauthn.io

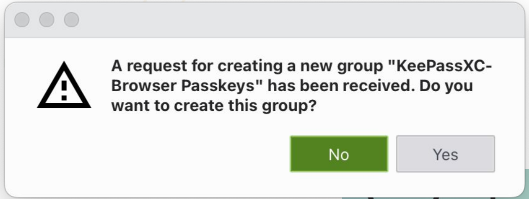
Username: test

Timeout in **50** seconds...

Confirm registration

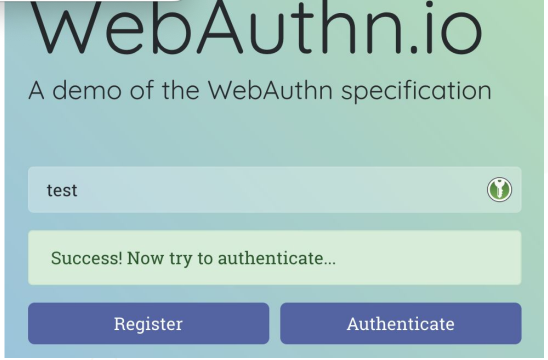
(3.)

Confirm group creation (only once)



A request for creating a new group "KeePassXC-Browser Passkeys" has been received. Do you want to create this group?

4.



WebAuthn.io

A demo of the WebAuthn specification

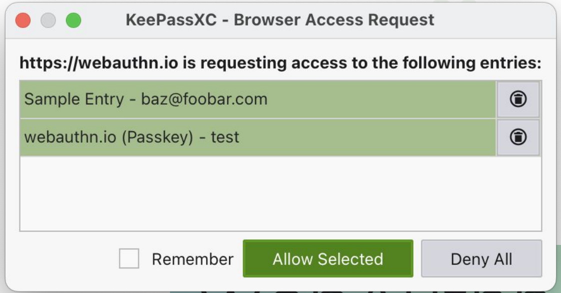
test

Success! Now try to authenticate...

Authenticate Via Passkey

Grant access to entry

1.



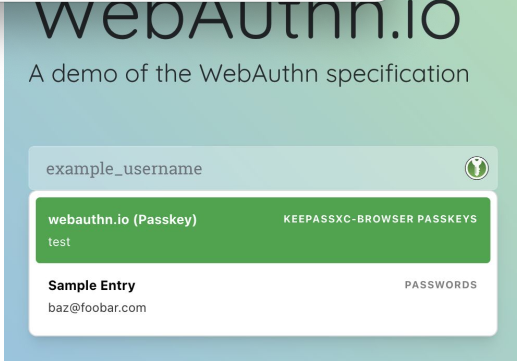
KeePassXC - Browser Access Request

https://webauthn.io is requesting access to the following entries:

Sample Entry - baz@foobar.com

webauthn.io (Passkey) - test

2.



webAuthn.io

A demo of the WebAuthn specification

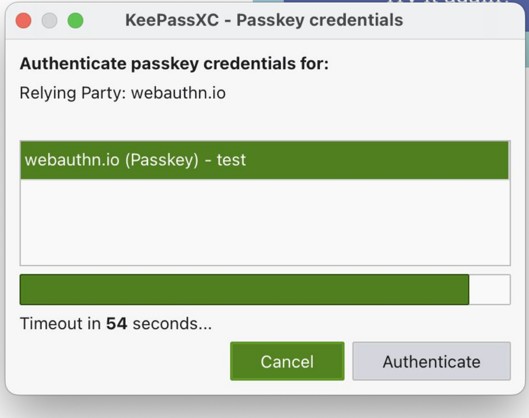
example_username

webauthn.io (Passkey) KEEPASSXC-BROWSER PASSKEYS
test

Sample Entry PASSWORDS
baz@foobar.com

Select passkey from menu

3.



KeePassXC - Passkey credentials

Authenticate passkey credentials for:

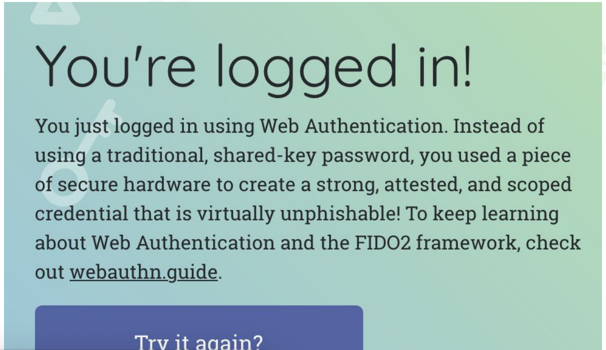
Relying Party: webauthn.io

webauthn.io (Passkey) - test

Timeout in **54** seconds...

Confirm authentication

4.

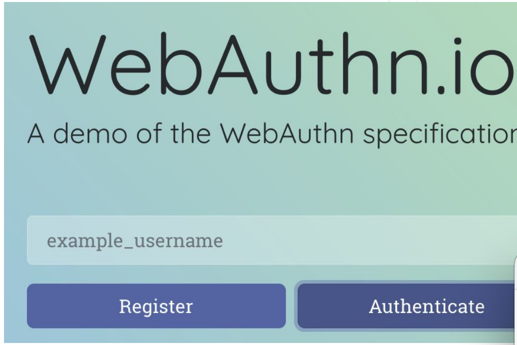


You’re logged in!

You just logged in using Web Authentication. Instead of using a traditional, shared-key password, you used a piece of secure hardware to create a strong, attested, and scoped credential that is virtually unphishable! To keep learning about Web Authentication and the FIDO2 framework, check out webauthn.guide.

Discoverable Credentials

1.



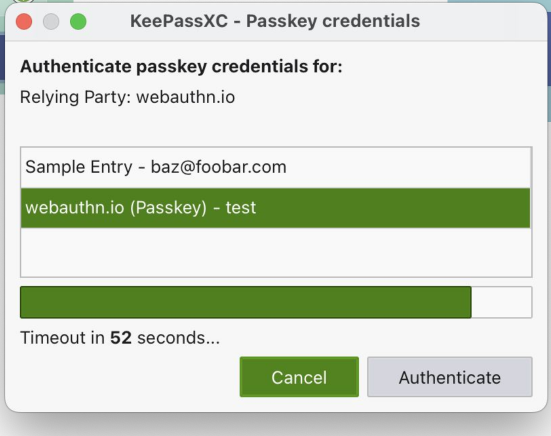
WebAuthn.io

A demo of the WebAuthn specification

example_username

Authenticate with empty username

2.



KeePassXC - Passkey credentials

Authenticate passkey credentials for:

Relying Party: webauthn.io

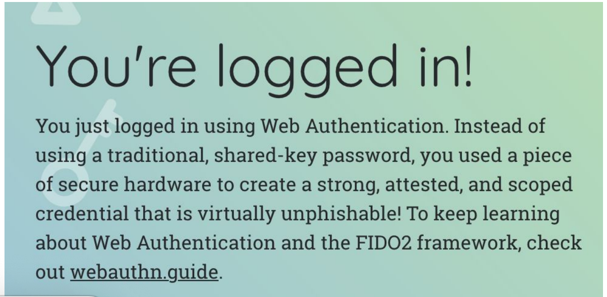
Sample Entry - baz@foobar.com

webauthn.io (Passkey) - test

Timeout in **52** seconds...

Confirm authentication and select passkey

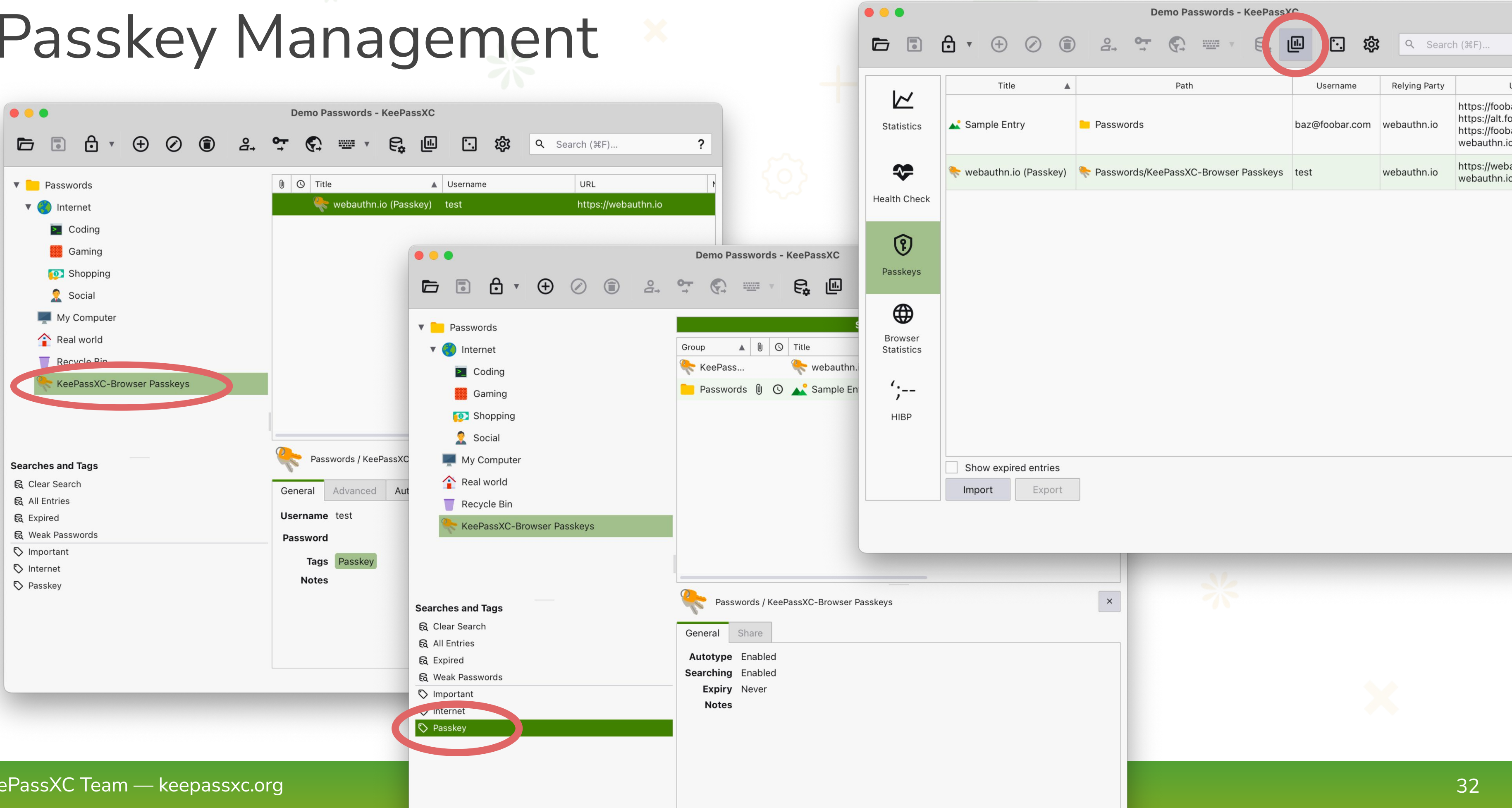
3.



You're logged in!

You just logged in using Web Authentication. Instead of using a traditional, shared-key password, you used a piece of secure hardware to create a strong, attested, and scoped credential that is virtually unphishable! To keep learning about Web Authentication and the FIDO2 framework, check out webauthn.guide.

Passkey Management



Demo Passwords - KeePassXC

Search (⌘F)...

- Passwords
  - Internet
    - Coding
    - Gaming
    - Shopping
    - Social
  - My Computer
  - Real world
  - Recycle Bin
  - KeePassXC-Browser Passkeys

Title	Username	URL
webauthn.io (Passkey)	test	https://webauthn.io

Searches and Tags

- Clear Search
- All Entries
- Expired
- Weak Passwords
- Important
- Internet
- Passkey

Passwords / KeePassXC

General | Advanced | Aut

Username test

Password

Tags Passkey

Notes

Demo Passwords - KeePassXC

- Passwords
  - Internet
    - Coding
    - Gaming
    - Shopping
    - Social
  - My Computer
  - Real world
  - Recycle Bin
  - KeePassXC-Browser Passkeys

Group	Title
KeePass...	webauthn.
Passwords	Sample En

Searches and Tags

- Clear Search
- All Entries
- Expired
- Weak Passwords
- Important
- Internet
- Passkey

Passwords / KeePassXC-Browser Passkeys

General | Share

Autotype Enabled

Searching Enabled

Expiry Never

Notes

Demo Passwords - KeePassXC

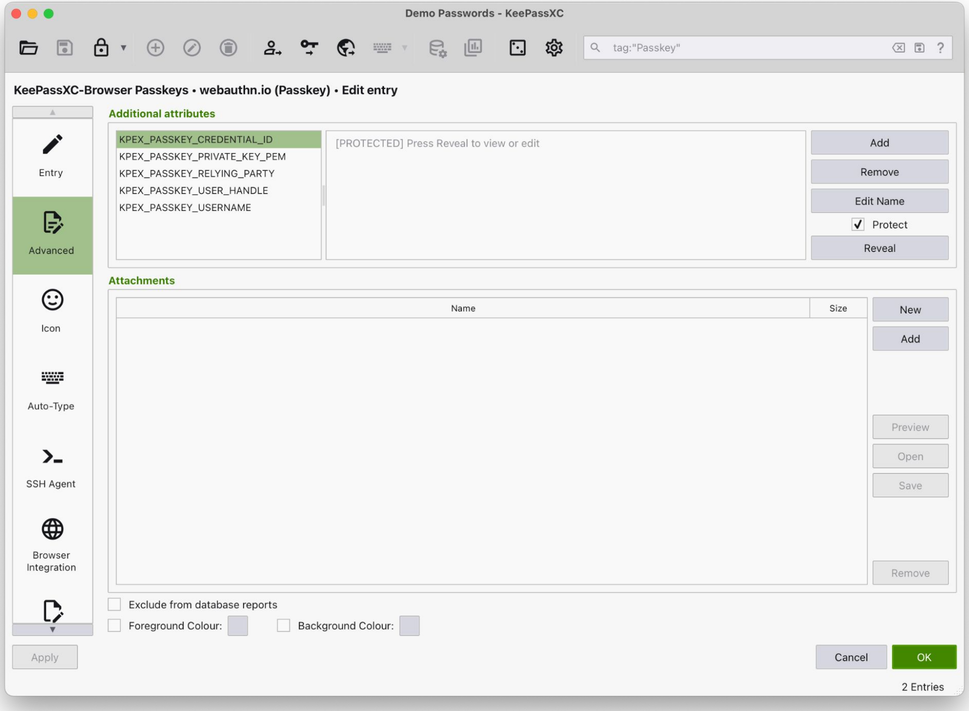
Search (⌘F)...

Title	Path	Username	Relying Party	U
Sample Entry	Passwords	baz@foobar.com	webauthn.io	https://fooba https://alt.fo https://fooba webauthn.io
webauthn.io (Passkey)	Passwords/KeePassXC-Browser Passkeys	test	webauthn.io	https://weba webauthn.io

□ Show expired entries

Import | Export

Passkey Management



Demo Passwords - KeePassXC

tag:"Passkey"

KeePassXC-Browser Passkeys • webauthn.io (Passkey) • Edit entry

Additional attributes

- KPEX_PASSKEY_CREDENTIAL_ID
- KPEX_PASSKEY_PRIVATE_KEY_PEM
- KPEX_PASSKEY_RELYING_PARTY
- KPEX_PASSKEY_USER_HANDLE
- KPEX_PASSKEY_USERNAME

[PROTECTED] Press Reveal to view or edit

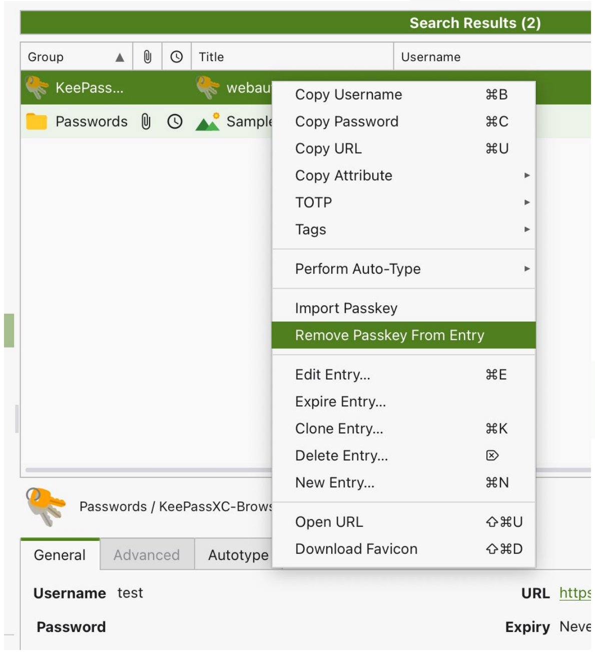
Attachments

Name	Size

□ Exclude from database reports

□ Foreground Colour: □ Background Colour:

2 Entries



Search Results (2)

Group			Title	Username
KeePass...			webau	
Passwords			Sample	

Passwords / KeePassXC-Brows

Username test

URL https

Password

Expiry Neve

Summary

Passkeys with KeePassXC…

- … allow passwordless login (except for the master password 😉).
- … prevent credential phishing.
- … prevent password leakage.
- … are portable and easy to back up.

Thanks!

Follow us:

- Web: keepassxc.org
- Bluesky: bsky.app/profile/keepassxc.org
- Mastodon: fosstodon.org/@keepassxc
- GitHub: github.com/keepassxreboot/

Documentation: keepassxc.org/docs/

Donate: keepassxc.org/donate/