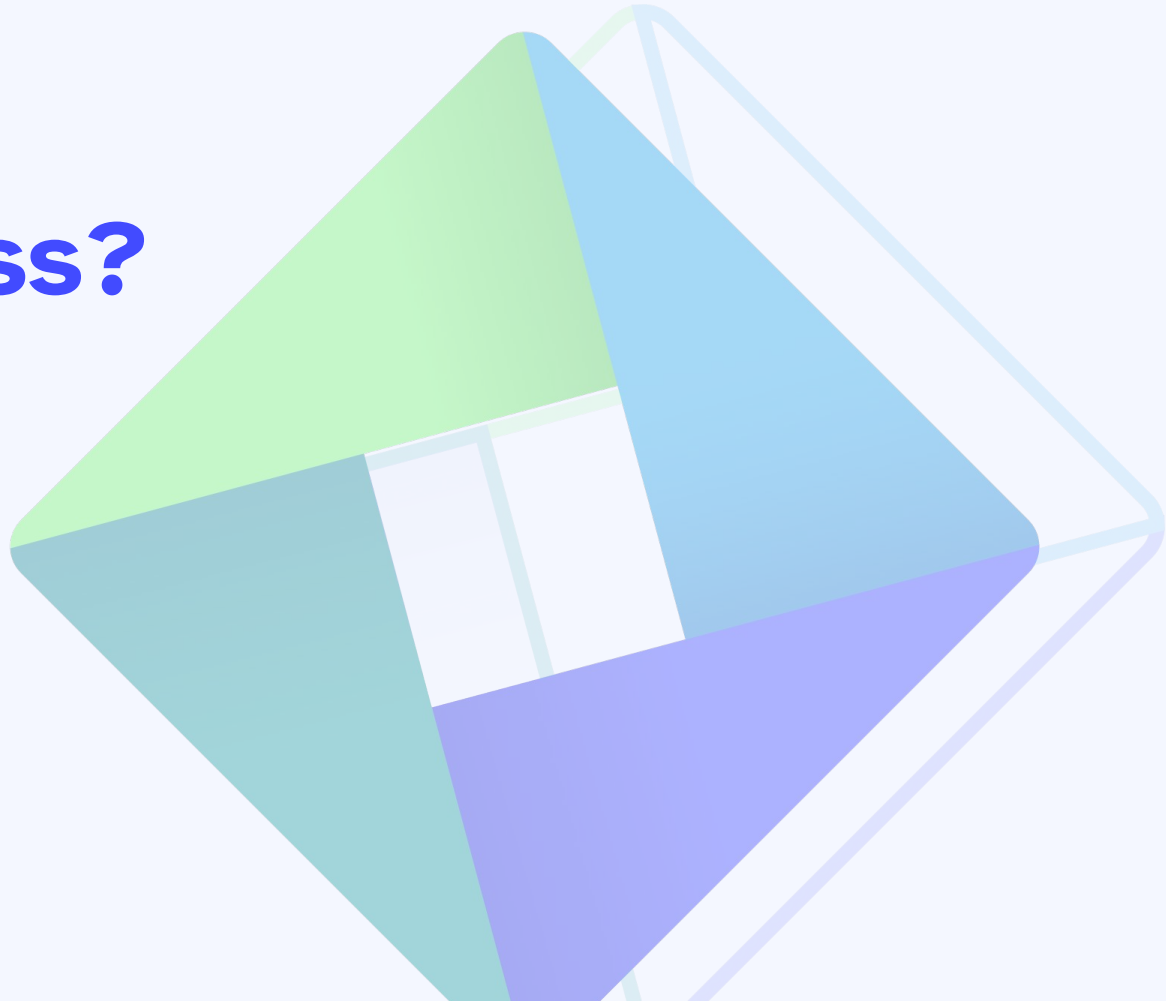
Quo vadis passwordless?

Die Zukunft der Authentifizierung



Clemens Hübner
inovex GmbH

German OWASP Day 2023

Clemens Hübner

Software Security Engineer @ inovex

Helps secure applications, still hacks them

Located in Munich

@ClemensHuebner

clemens.huebner@inovex.de

@clemens@infosec.exchange

@inovexgmbh

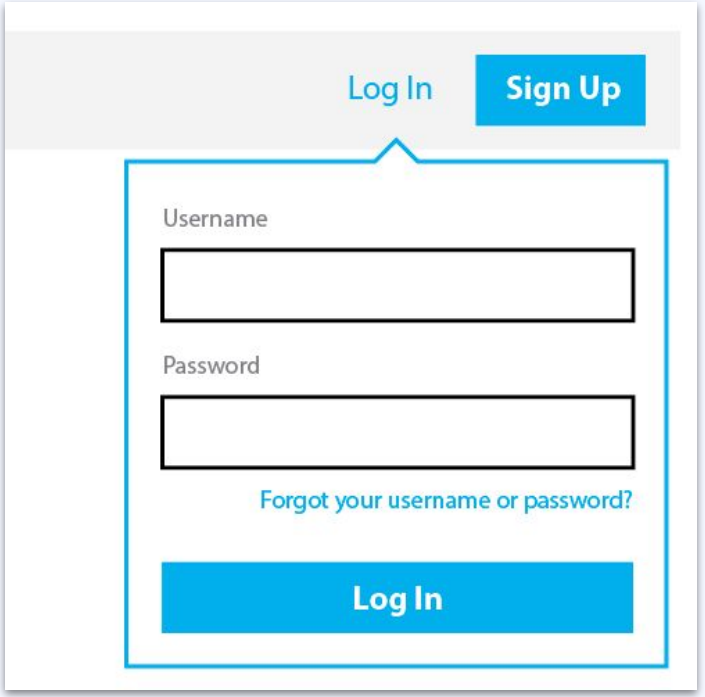
@inovexlife

inovex

Status quo of authentication

- Authentication with username & password

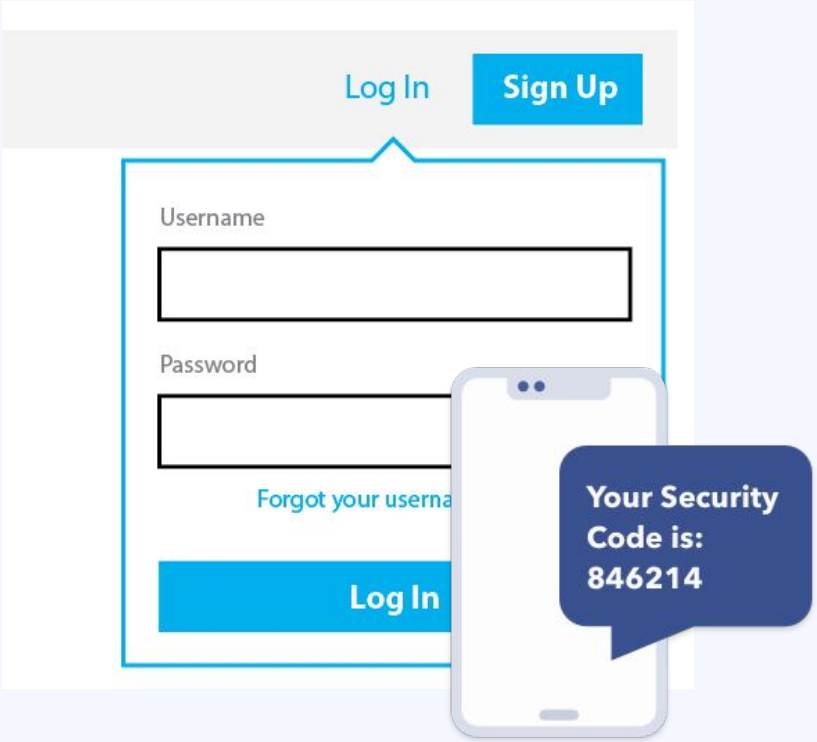
- The human brain is not built for memorizing strong passwords
- Passwords get guessed or stolen



Status quo of authentication

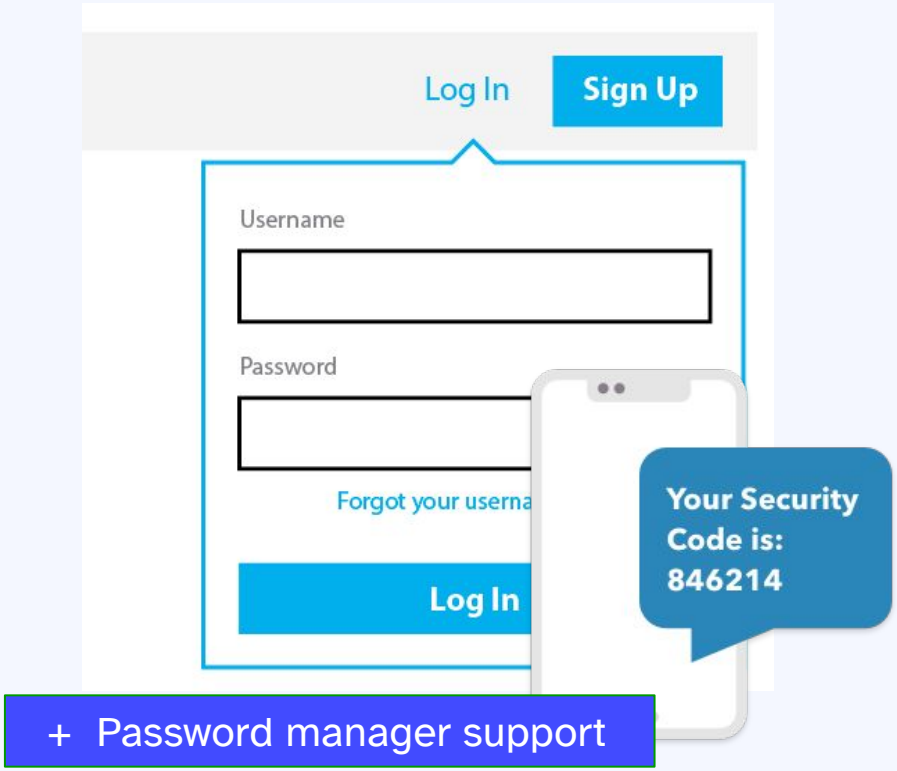
- Mitigate insecure passwords with second factor (2FA)

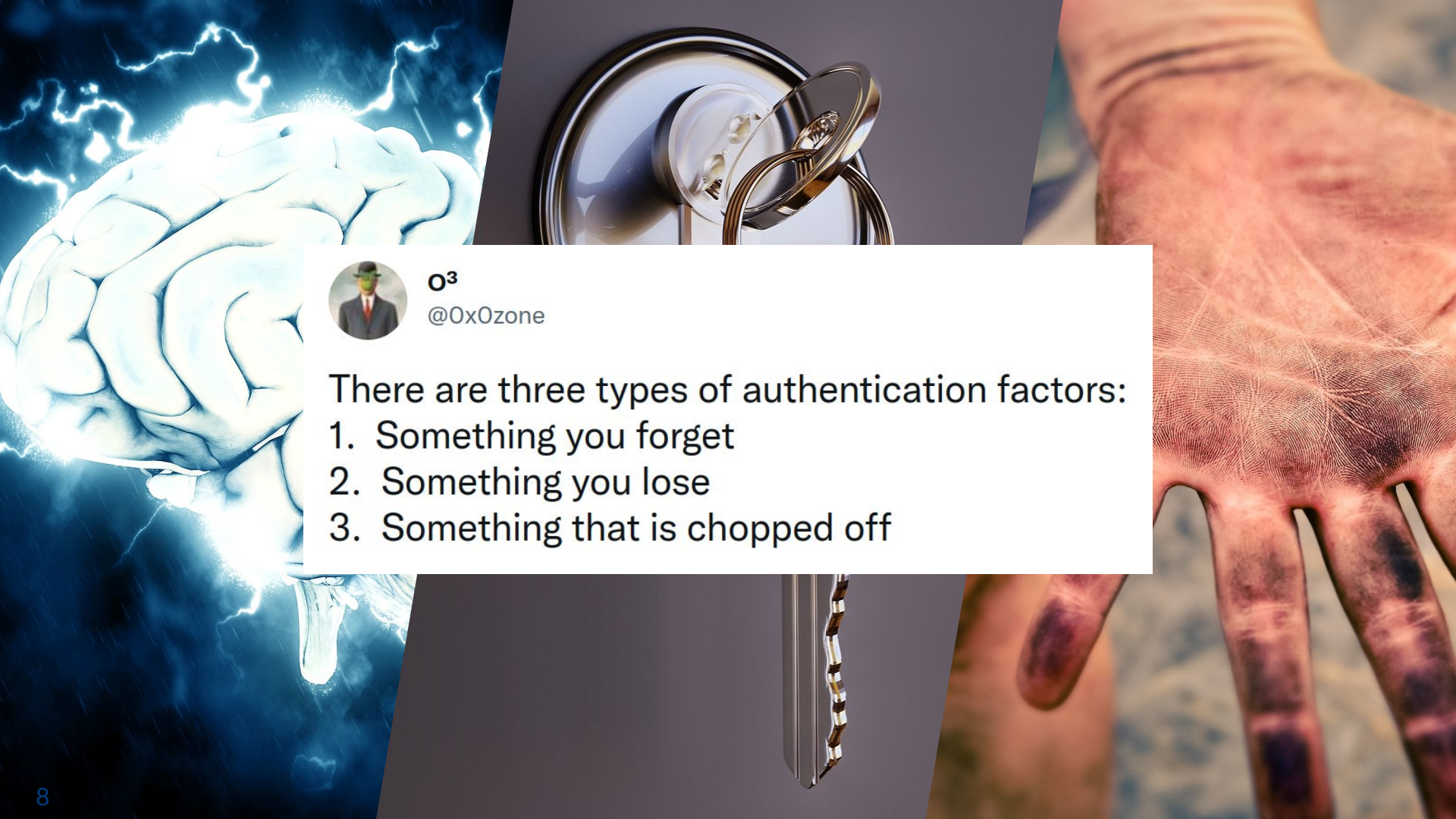
- Brain limits remain
- Problem of phishing



Problems with the status quo

- *Something you know* is hard to remember
- Phishing is possible
- Still need to trust the site to handle my password



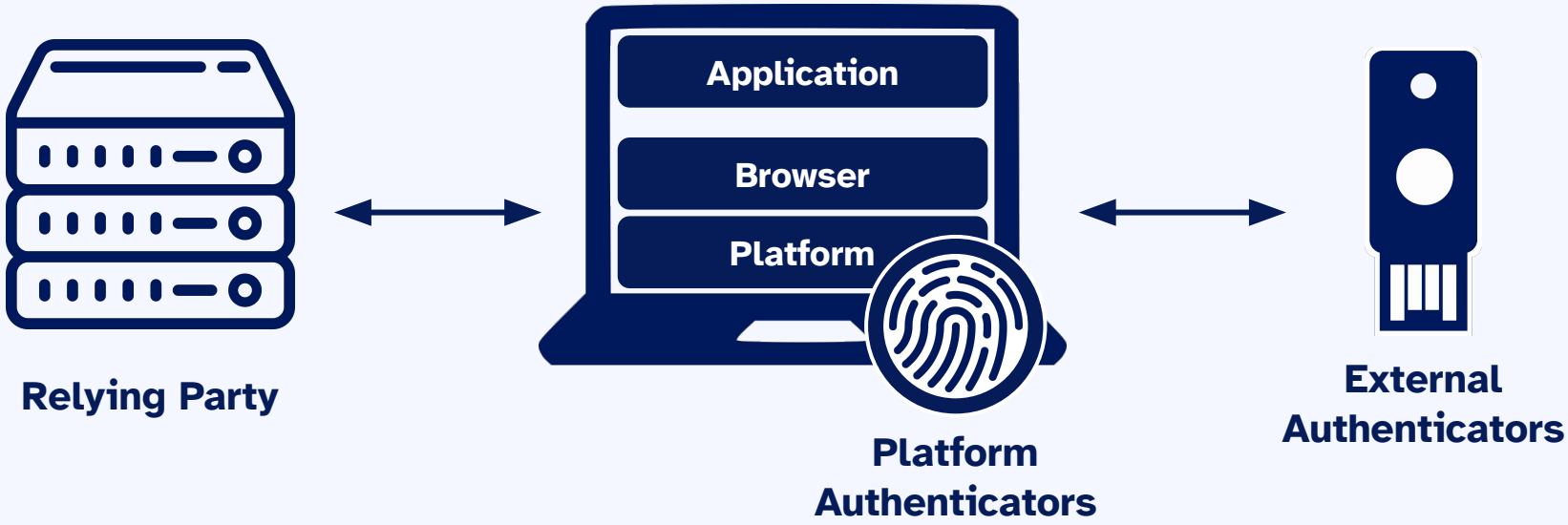

O³
@0x0zone
There are three types of authentication factors:
1. Something you forget
2. Something you lose
3. Something that is chopped off

Solution: Less knowledge-based authentication

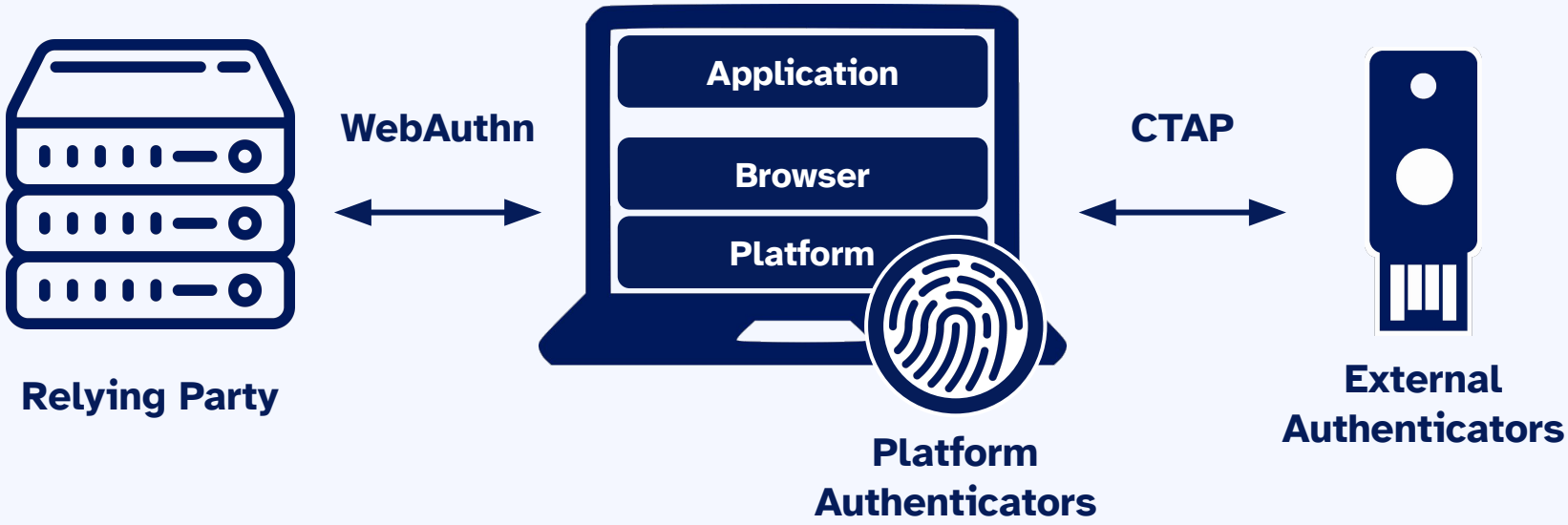
- use possessed or biometric factors
- use public-key based challenge-response (no leakage of any secret)
- strong scoping of credentials for phishing protection

→ WebAuthn to the rescue

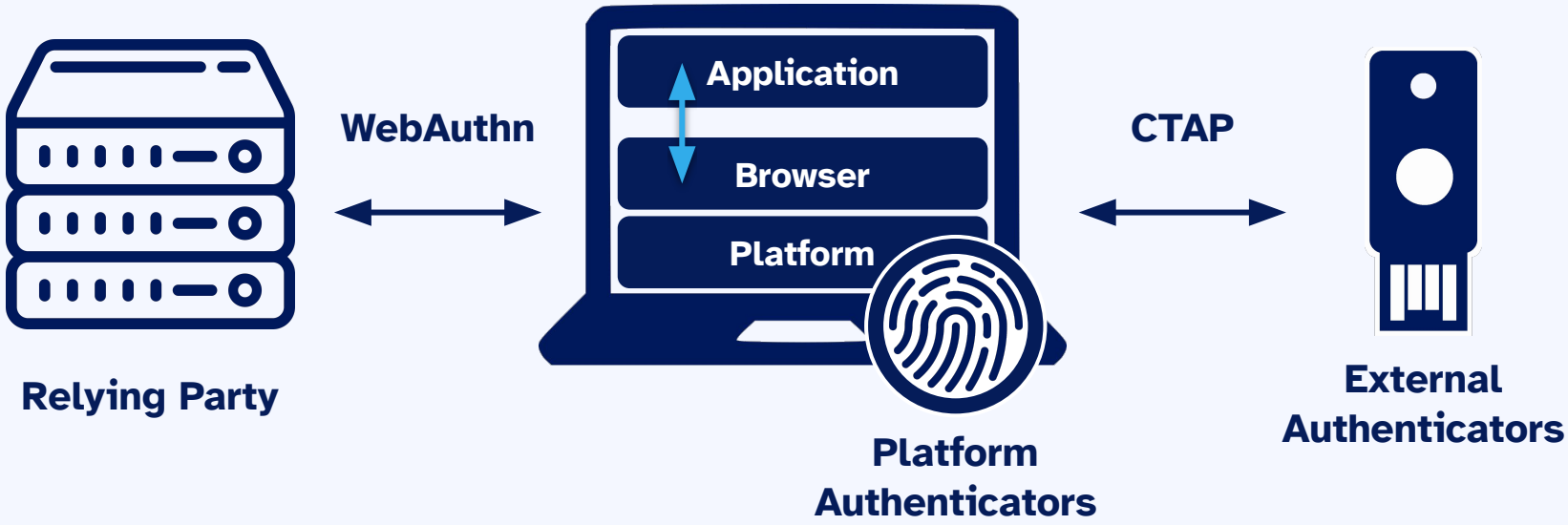
Architecture



Architecture



Architecture



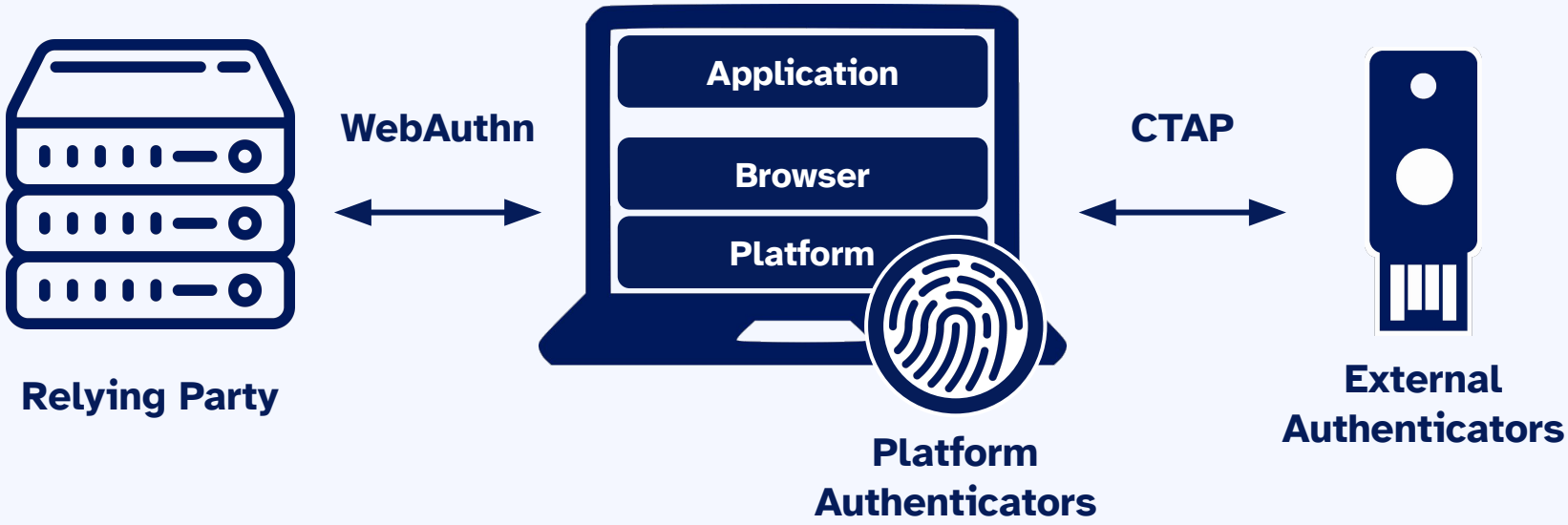
The two WebAuthn Ceremonies

Registration Ceremony	Authentication Ceremony
Creating a public key credential, scoped to the Relying Party, based on a user's identifier	**Proving** the presence of the private key and the consent of the user that registered it

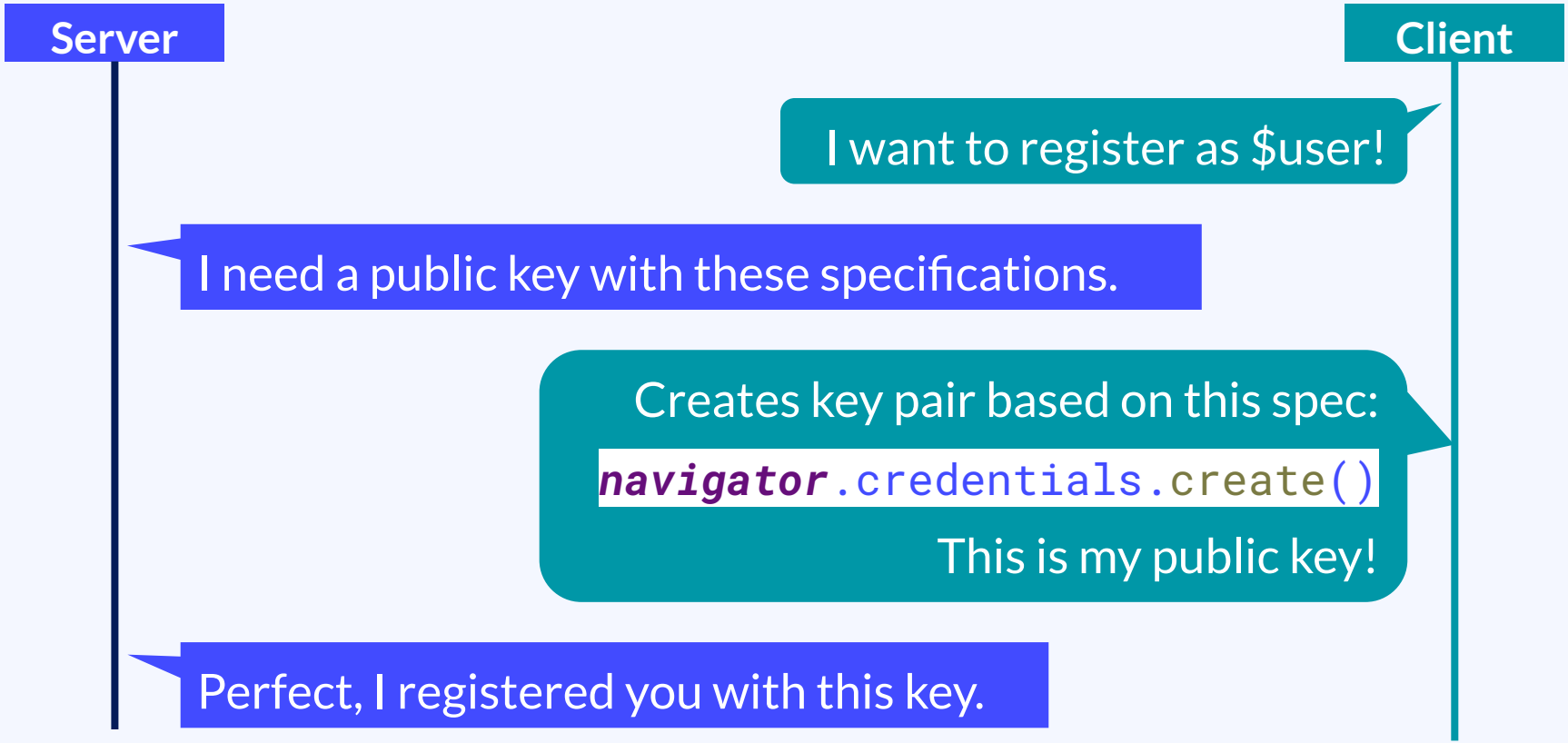
Attention: That's all!

Demo time!

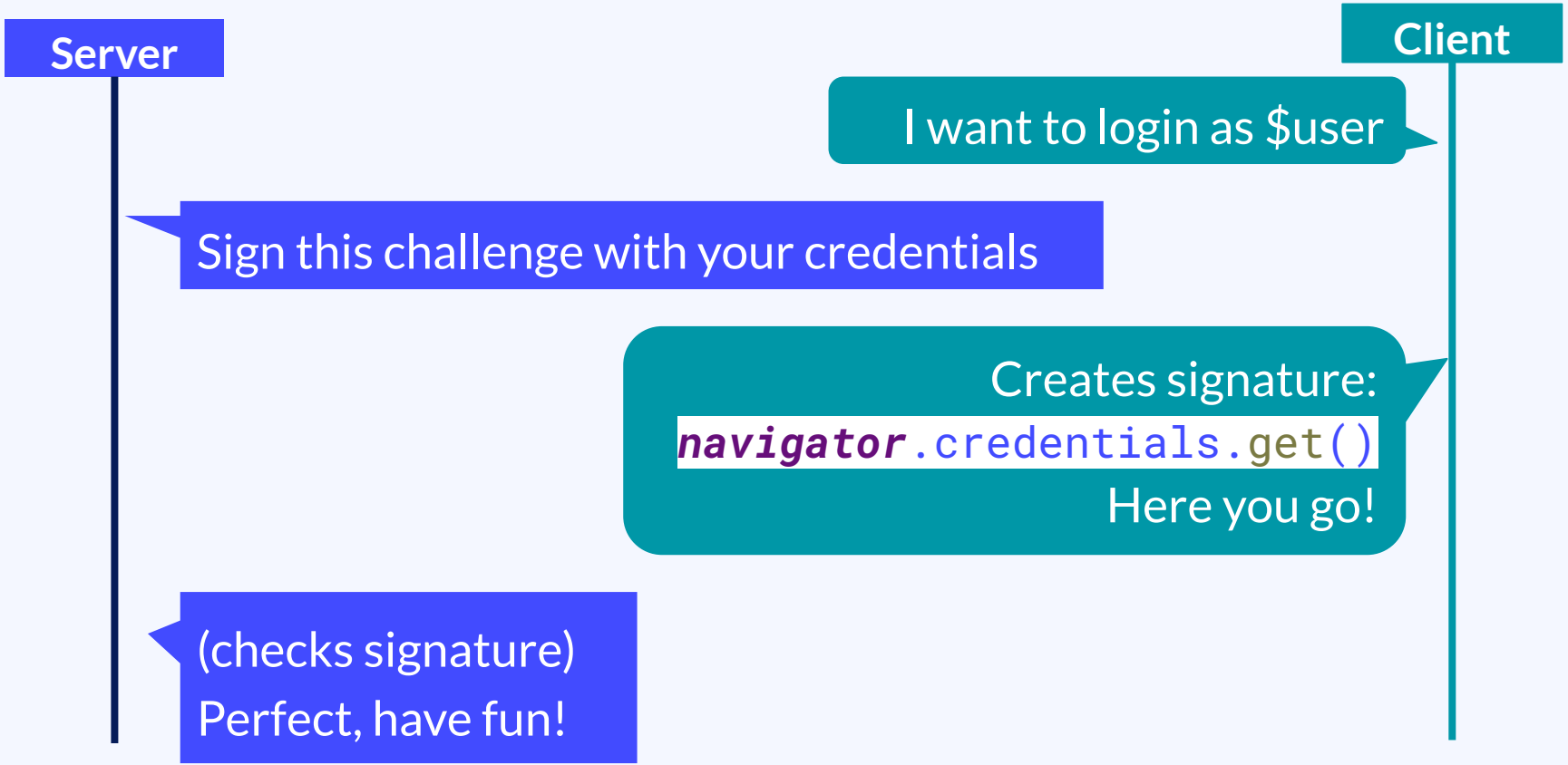
Architecture



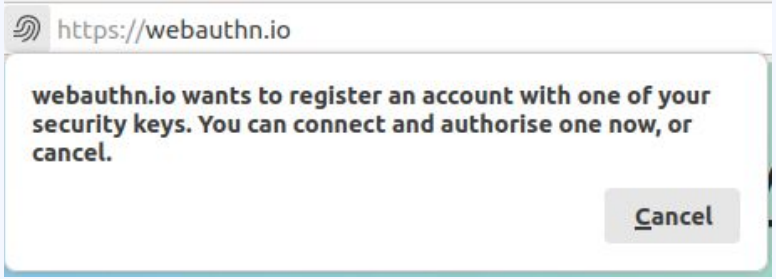
Registration ceremony



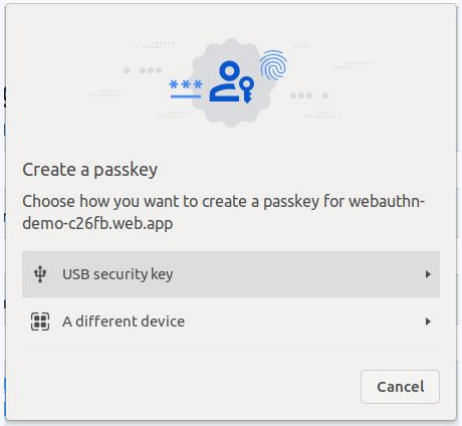
Authentication ceremony

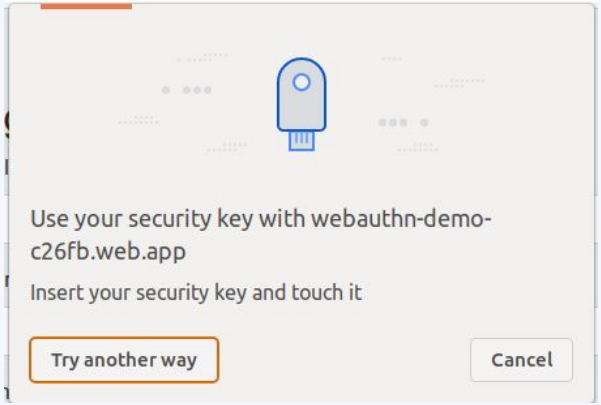


Different UI on different platforms

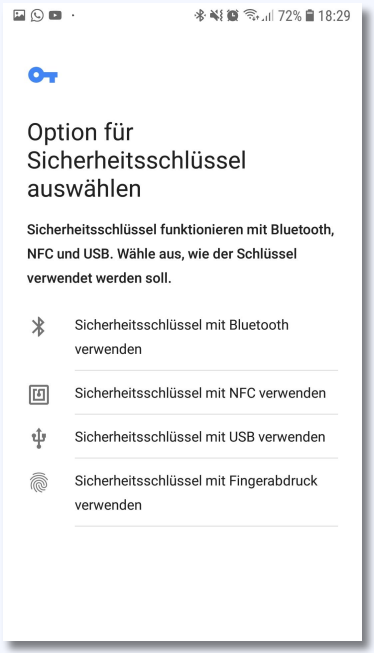


Firefox 109





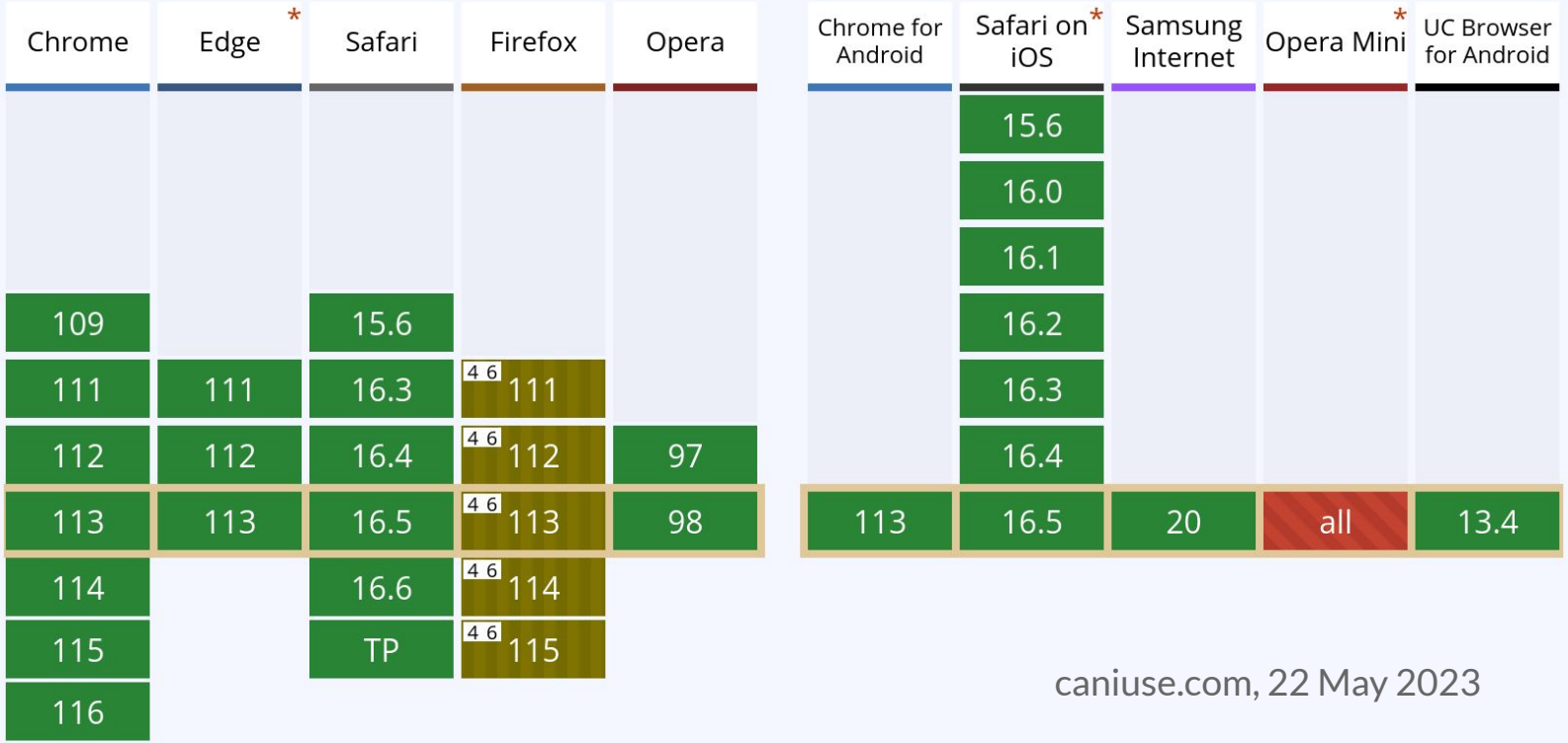
Chrome 110



Android 11 / 12

Can I use WebAuthn?

- today, >95% global usage possibility



caniuse.com, 22 May 2023

Timeline of WebAuthn

May 2016

W3C First Public Working Draft

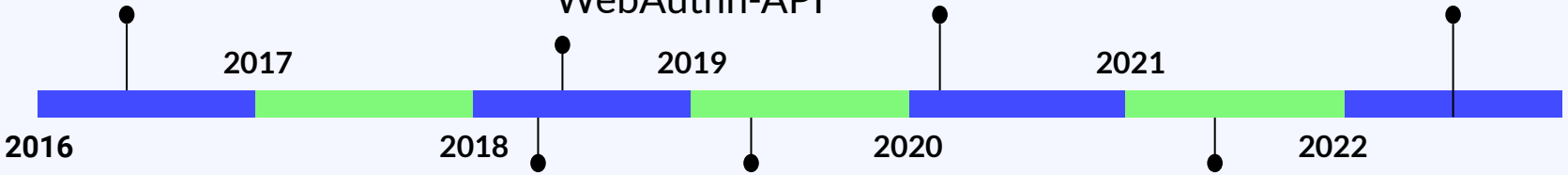
May 2018

Firefox 60 and Chrome 67 support WebAuthn-API

February 2020

Apple joins the FIDO Alliance

Summer 2022…



March 2018

W3C Candidate Recommendation

March 2019

Level 1 W3C Recommendation

April 2021

Level 2 W3C Recommendation

Three flavours of WebAuthn

WebAuthn as 2FA	Passwordless WebAuthn	ID-less WebAuthn
Username + Password + WebAuthn	Username + WebAuthn	WebAuthn
• alternative factors possible (e.g. OTP)	• “default” usage of WebAuthn	• requires use of resident keys

WebAuthn in the wild

April 2022

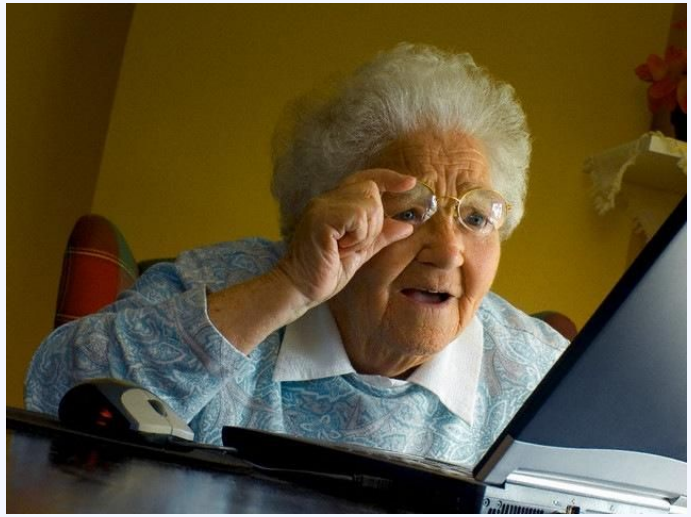
- still small number of real passwordless applications

- increased usage of WebAuthn as second factor

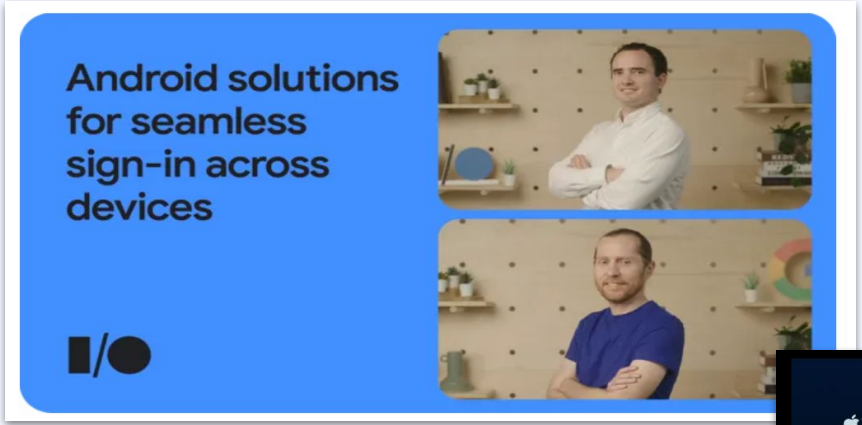
Usability problems with WebAuthn

- Passwords are known and widely understood
- Public key crypto is not

- Usage of external authenticators is new for most users
- Platform authenticators lack portability

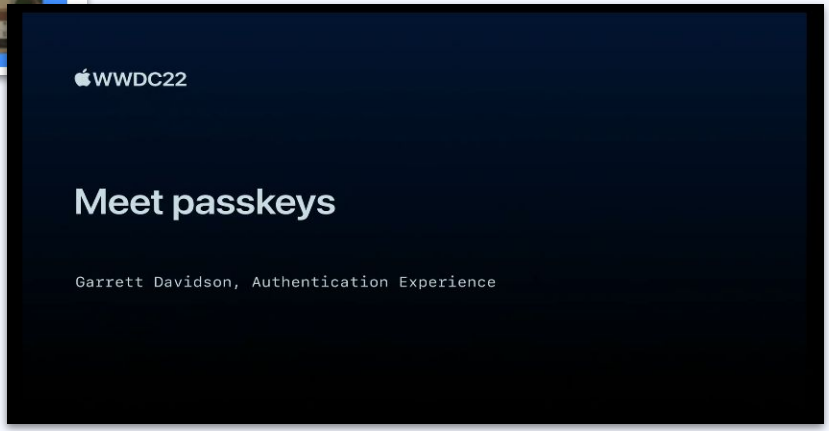


⇨ Strong security requirements hinder the spread of WebAuthn



Google I/O 2022

Apple WWDC22



Passkeys to the rescue

Passkeys vs WebAuthn

Passkeys are WebAuthn credentials + *usability*

Integrated

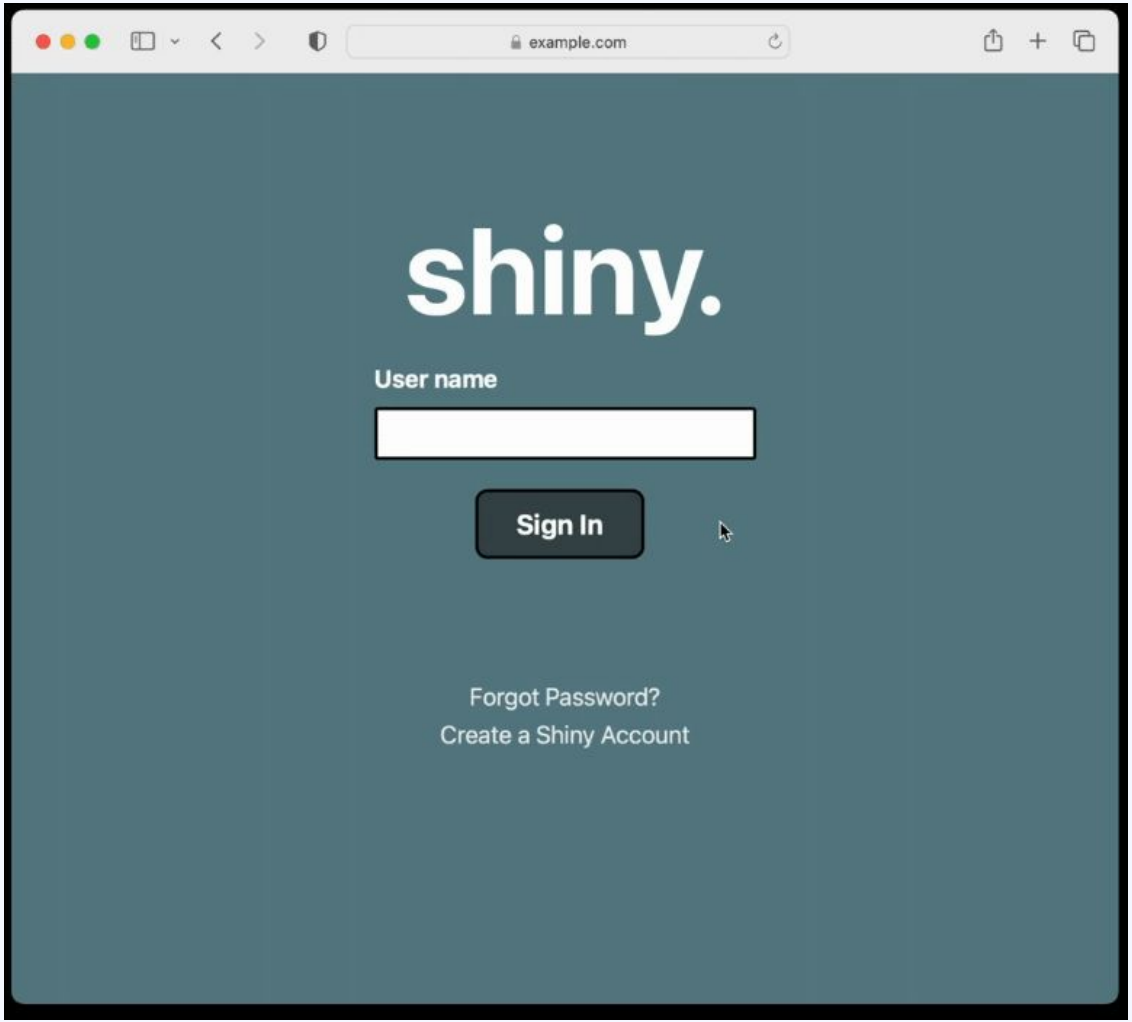
Synced

Portable

Improved integration into clients

- added to ecosystems and combined with user accounts

- using existent factors (Device lock / FaceID / TouchID)


example.com
shiny.
User name
Sign In
Forgot Password?
Create a Shiny Account


9:41
shiny
User name
Sign In
sign in with passkey for example.com
garrett
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
@
.
return

Improved usability in login process

Conditional mediation

aka Conditional UI

aka Autofill UI

```
<input
  type="text" name="username"
  autocomplete="username webauthn"
  …
>
```

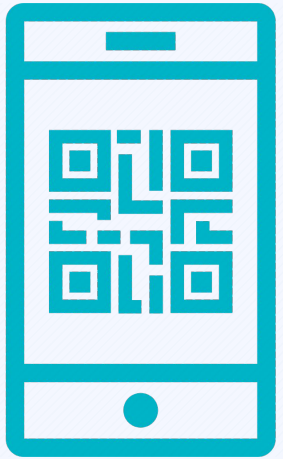
https://passkeys.dev/

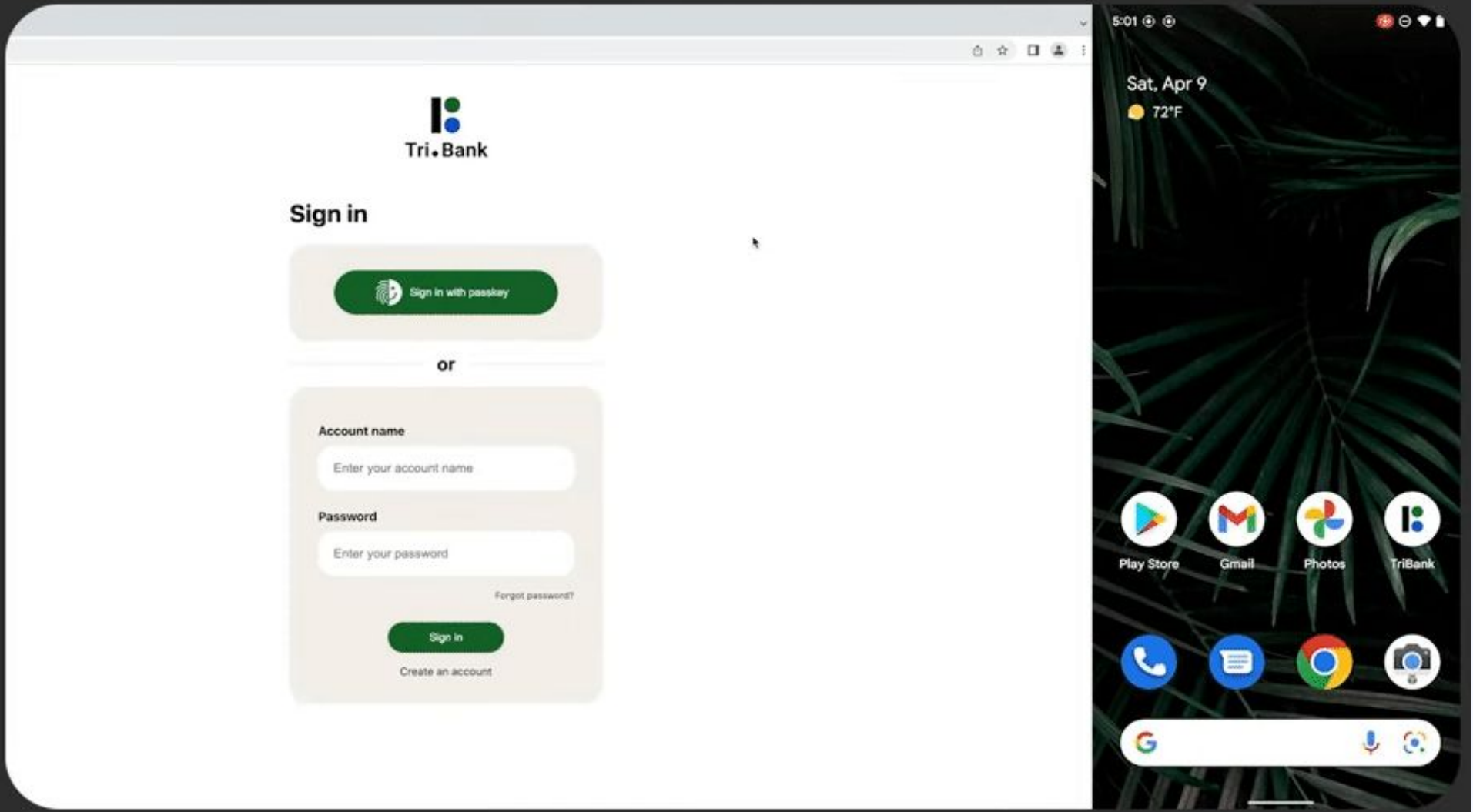
Synced

- Google:
  - Google Password Manager
  - e2e-encrypted
- Apple:
  - iCloud Keychain
  - e2e-encrypted
- Microsoft: not synced yet

Cross-device usage of passkeys

- own protocol for key exchange
  Cross-Device Authentication
  - often powered by QR code
  - using CTAP
- security features
  - proximity check
  - e2e encrypted




Tri.Bank
Sign in
Sign in with passkey
or
Account name
Enter your account name
Password
Enter your password
Forgot password?
Sign in
Create an account
5:01
Sat, Apr 9
72°F
Play Store
Gmail
Photos
TriBank

WebAuthn in the wild - 2023

May 2023

- increasing number of real passwordless applications

...

Quo vadis passwordless?

- Topic is back on the table
- Google, Microsoft & Apple push the enrollment
- Surrounding eco-system arises

- Concentration of authentication information
- W3C-Standard is weakened
- Passkeys are less widely supported than WebAuthn L2

Further resources

Web-Authn-Specifications:

- Level 1, Level 2, latest draft

Demos:

- Webauthn: Simple demo, extensive demo
- Passkeys: Simple demo

Tools and resources:

- Web debugger, Chromium dev tool
- Dev guide WebAuthn, Dev guide passkeys

Takeaways

Passkeys may give WebAuthn
a new momentum

WebAuthn could become usable
for a broader range of people

Platform oligopoly strikes again,
independency of WebAuthn is unclear

Vielen Dank!

@ClemensHuebner

clemens.huebner@inovex.de

@clemens@infosec.exchange

@inovexgmbh

@inovexlife