Passage

Goodbye Passwords, Hello Passkeys

What is passwordless
and why it is the future

Nick Hodges
Dev Advocate
Passage.id

Passage

Nick Hodges

- Developer Advocate at Passage
- Angular/Typescript
- Minnesota Sports Fan
- Lover of Pistachios
- https://passage.id/nick

https://passage.id/nick

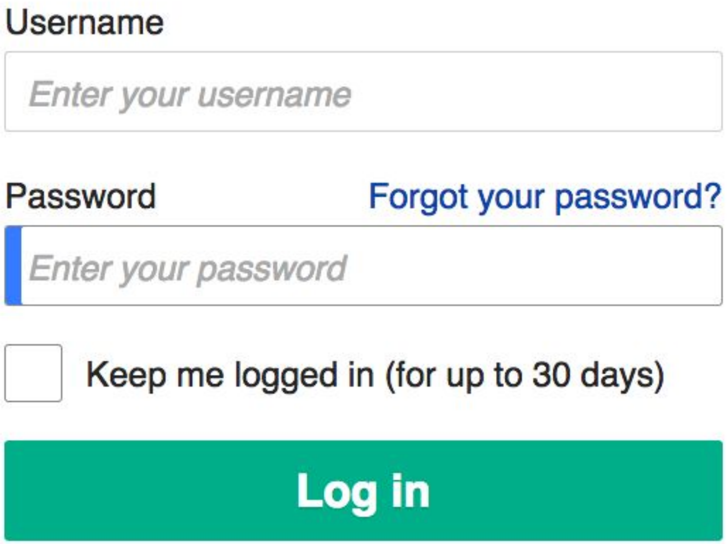
Passwords are...

...sub-optimal

Over 80% of all security breaches are the result of a compromised password

Why Are Passwords Suboptimal?

- They often aren’t complex enough
- They are frustrating for users
- They often get reused
- They often get shared
- The are phishable
- Password managers are no fun
- They don’t scale



Username

Enter your username

Password Forgot your password?

Enter your password

□ Keep me logged in (for up to 30 days)

So what is a developer to do?

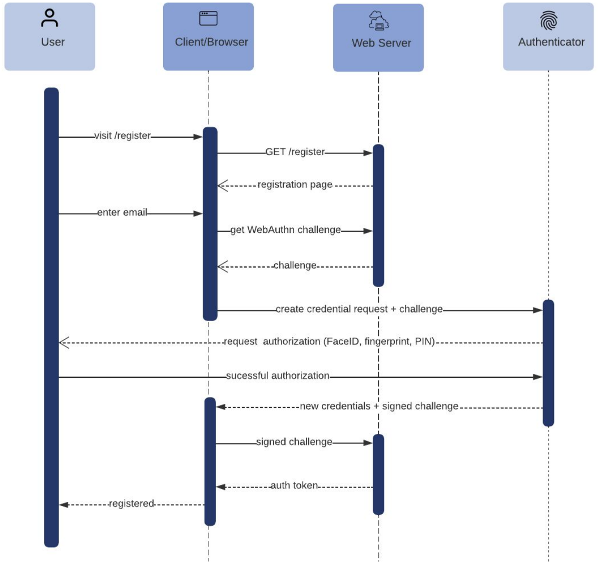
Biometrics for the Win!

- ✓ Nothing for users to remember (or forget)
- ✓ Two-factor authentication in a single quick step
- ✓ User don’t have to switch context to email for magic link

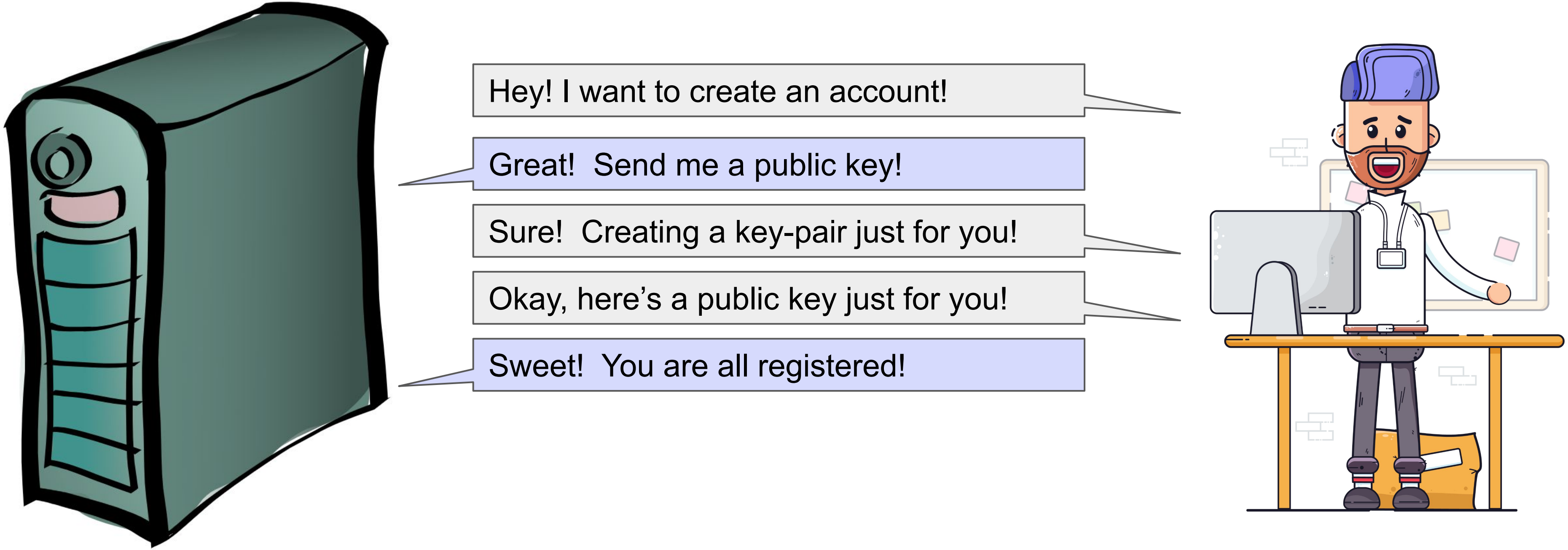
- ✓ No PII exposure or data breach due to weak passwords
- ✓ No sensitive data stored on the server
- ✓ Cannot be phished

What’s up with WebAuthn

- Approved by FIDO and W3.org
- Supported by most major browsers
- Uses Public Key cryptography
- Leverages biometrics



WebAuthn Registration Process



Hey! I want to create an account!

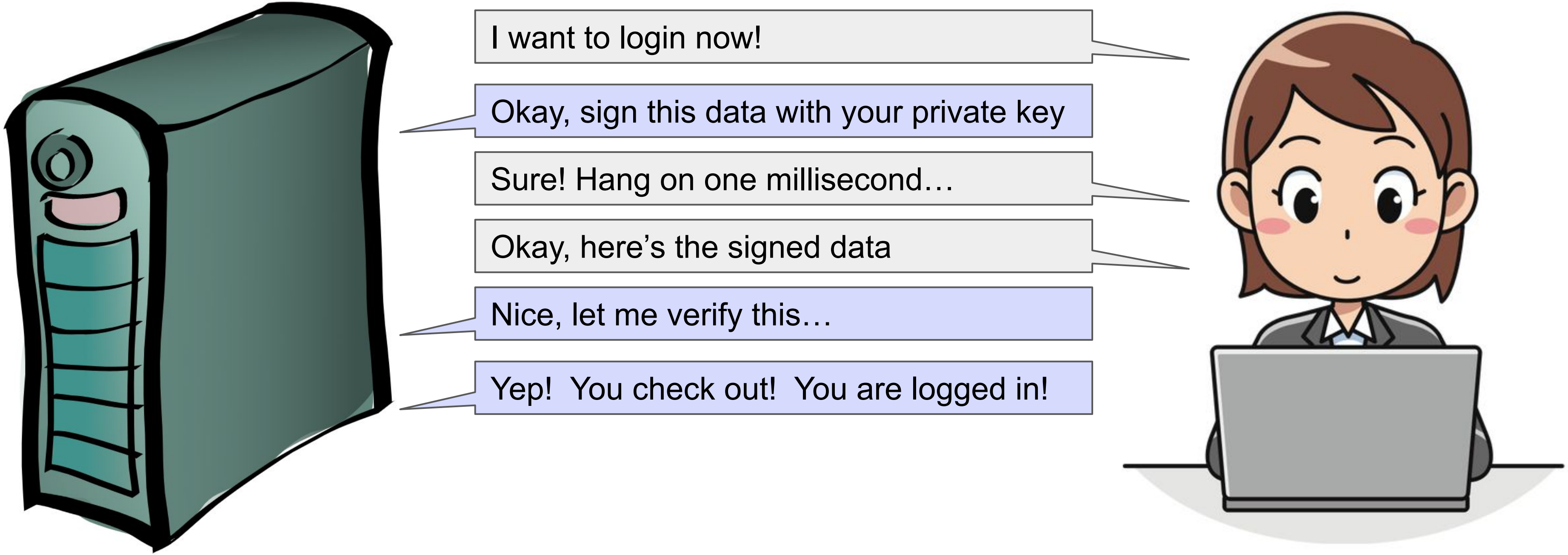
Great! Send me a public key!

Sure! Creating a key-pair just for you!

Okay, here’s a public key just for you!

Sweet! You are all registered!

WebAuthn Login Process



I want to login now!

Okay, sign this data with your private key

Sure! Hang on one millisecond…

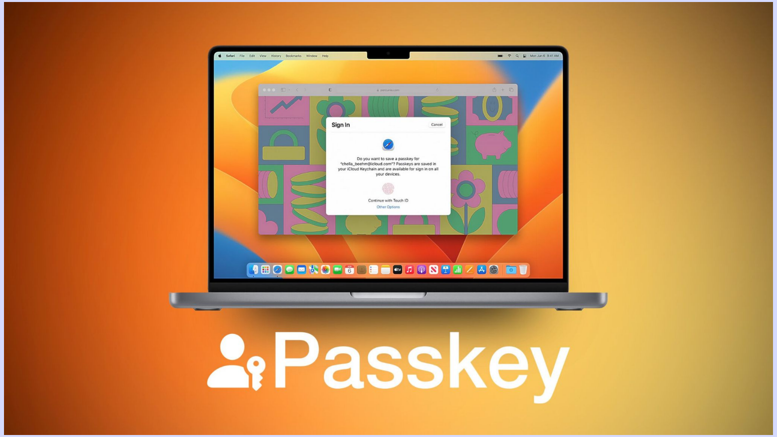
Okay, here’s the signed data

Nice, let me verify this…

Yep! You check out! You are logged in!

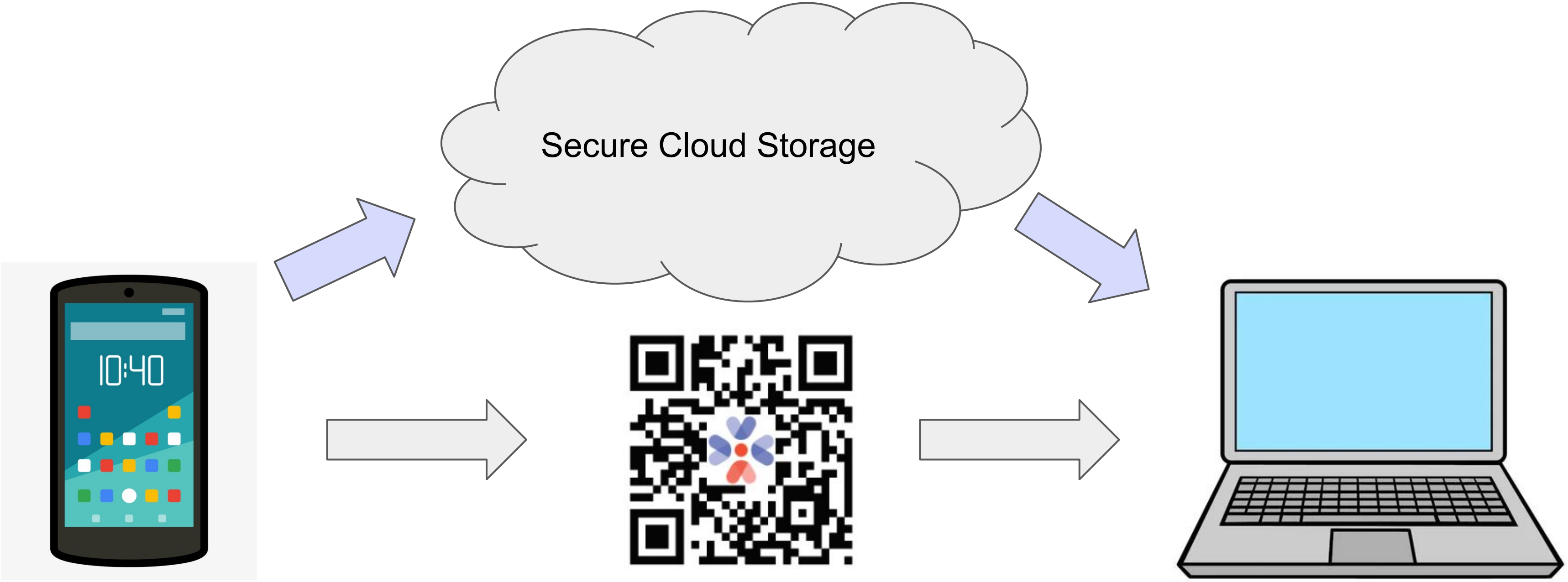
Where do Passkeys fit in all of this?

Microsoft, Apple, and Google all committed to supporting this system.



Do you want to save a passkey for "chella_boehm@icloud.com"? Passkeys are saved in your iCloud Keychain and are available for sign in on all your devices.

Passkeys are Sharable

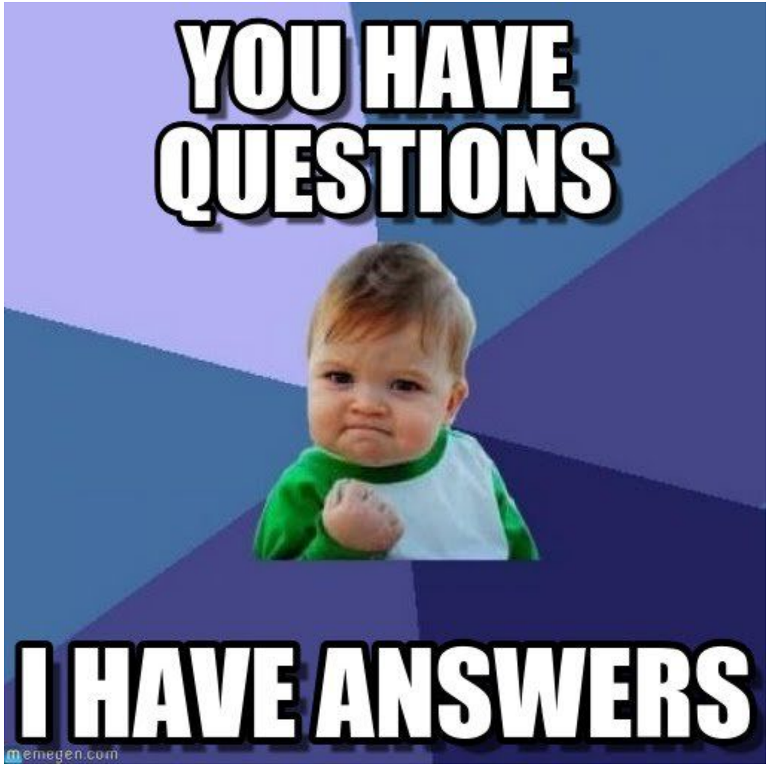


Why is all this is better

- No biometric information ever leaves the user’s device
- The Trusted Platform Model (TPM) chip does all the work
- Can’t be phished (or at least no one can conceive how…)
- Vastly better user experience
  - More conversions

Misconceptions

- “There is still a password backup”
- “It requires Bluetooth to login”
- “Lose your phone, lose your info”
- “The TPM can be cracked”
- “If you don’t have your phone, you can’t login”



Let me head off some questions…

- “What if I lose my phone?”
- “What if my biometric information is compromised?”
- “What if my physical biometrics change?”
- What else?

Give it a try this very minute!

https://passage.id/demo

Code

https://github.com/passageidentity

About Passage

- Startup based out of Austin
- https://passage.id
- Support almost any web framework with a web component
- Just released a beta of our iOS SDK
  - https://github.com/passageidentity/passage-ios
  - More SDKs in work

Passage

Thanks!

Nick Hodges

Developer Advocate

https://passage.id/nick

@passagenick

Slides: https://noti.st/nickhodges

Passage

Passage