



U2 can U2F

Hello!

Rob N ★

Email: robn@fastmail.com

Twitter: [@robn](https://twitter.com/@robn)

Github: [@robn](https://github.com/@robn)

<https://robn.io/u2f-lca-2017>

Two-factor authentication

- Something you know
 - Password
- Something you have
 - SMS (phone)
 - TOTP (phone, standalone)
 - Proprietary/enterprise/corporate things (standalone)



Two-factor authentication

- Registration
 - Connect a second factor to an existing account
- Authentication
 - Verify that the user has the second factor





Not a
live demo

SMS registration

We will text you a single-use code to verify your phone number.

Australia (+61) ▾

41 [REDACTED] 40

Carrier SMS charges may apply.

[Send Verification Code](#)

SMS registration



8C2JNS is your FastMail
verification code

Now

SMS registration

Please enter the code sent to +61 41 [REDACTED] 40.

8C2JNS|

Verify

Texts may take up to 30 seconds to arrive.

Change Phone Number

Resend Code

SMS authentication

The image shows a login interface with a light gray background and a white rectangular input area. At the top left is a **Username** field containing the text "robn@fastmail.com". Below it is a **Password** field with a series of black dots representing the password. At the bottom left is a checkbox labeled "Keep me logged in". In the bottom right corner is a large green rectangular button with the text "Log In" in white.

Username

robn@fastmail.com

Password

.....

Keep me logged in

Log In

SMS authentication

Send a single use code to:

+61 4XX XXX X40 Sent

Enter the code we sent you:

BH2KP4

Don't require two-step verification again on this device

Verify

TOTP registration

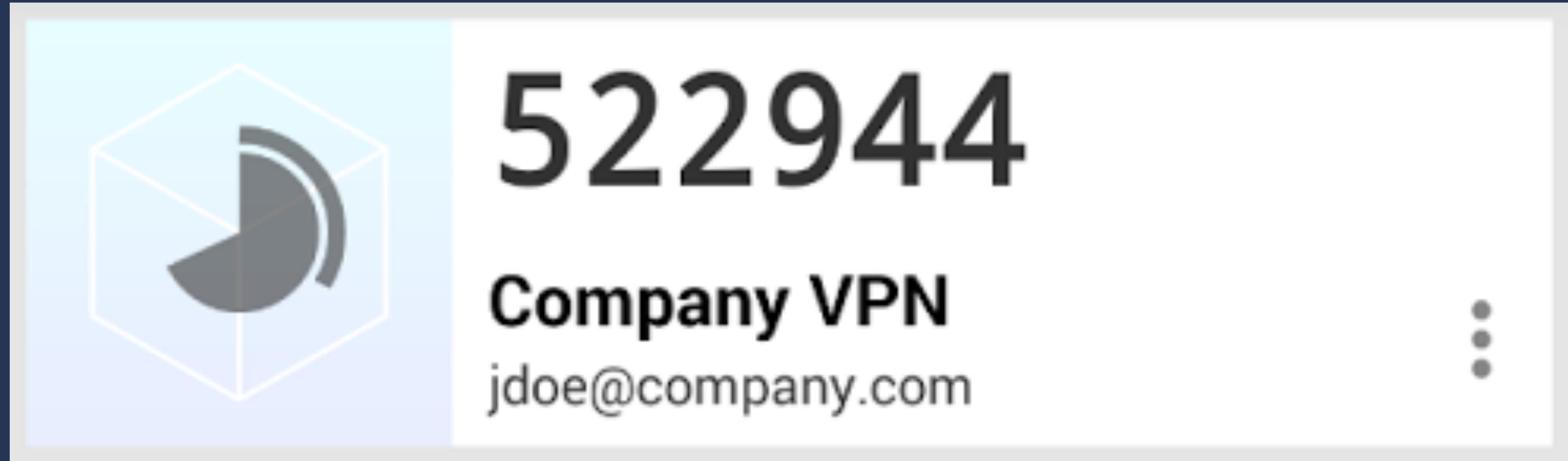
1

Scan this barcode in your authenticator app ([Help](#)):



Can't use the barcode? Type in this secret key instead: **tvdn4prjecbn6xvaybs2qxlyoi**

TOTP registration



TOTP registration

- 2 Enter the 6-digit code from your app that appears after scanning the barcode:

522944

TOTP authentication

Enter the 6-digit code from the authenticator app on your phone:

414337

Don't require two-step verification again on this device

Verify

TOTP hardware token



TOTP hardware token

1

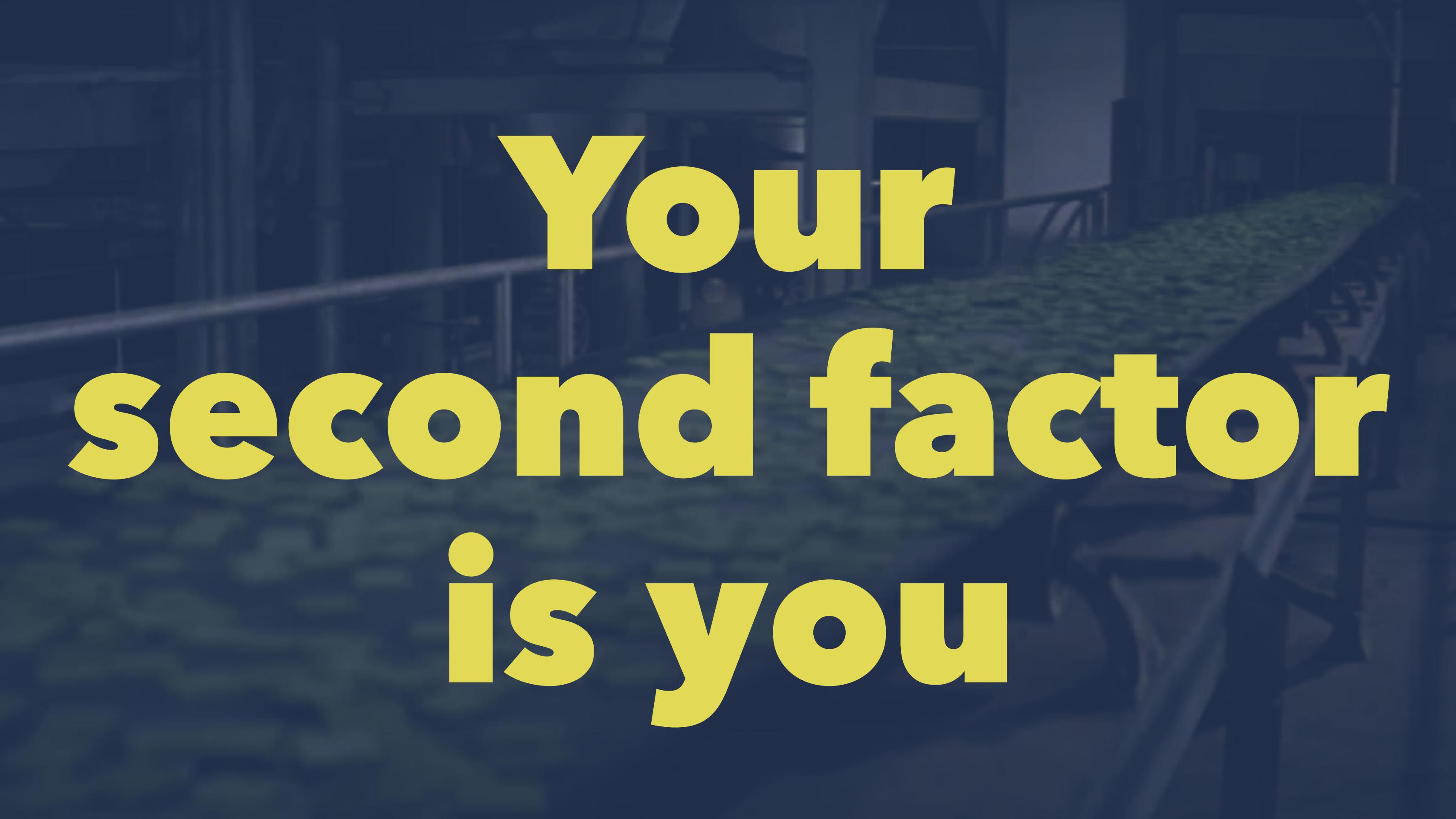
Enter the secret key that came with your device:

eecweudo524oa3homvtgnbe5e|

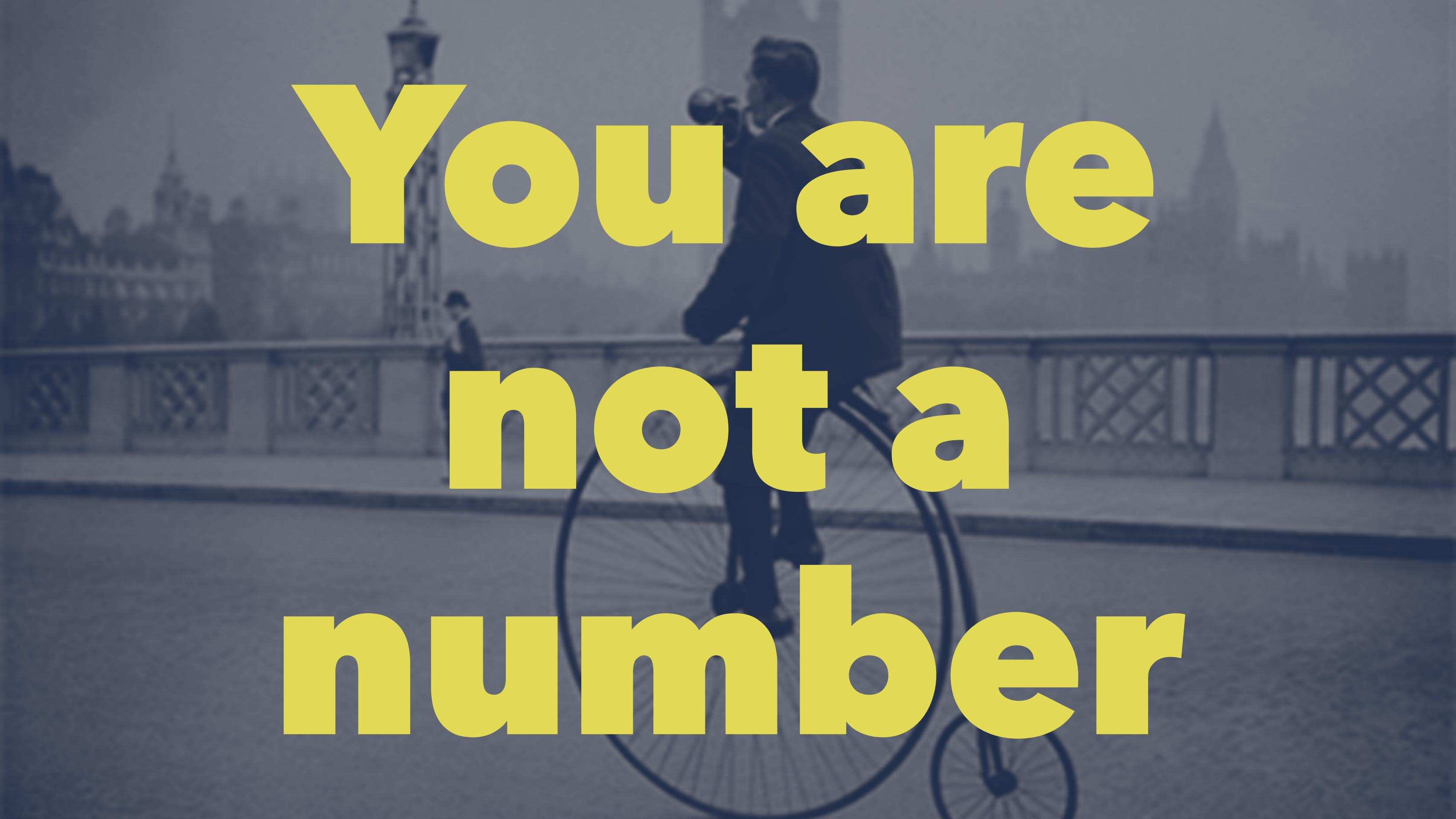


THUMBS UP

www.thumbsup.com

A dark, grainy photograph of a person running on a track field at night. The runner is blurred, suggesting motion. In the background, stadium lights illuminate the field and stands. The foreground is mostly in shadow.

Your
second factor
is you



You are
not a
number



Phishing

Dignitaries

ENTERTAIN

usability

Helioscissor Scanner

Beeping Trapezoid



Direct Orders

DISOBEY

Onions

CARAMELIZE

Disbelief

SUSPEND

EULOGIZE



Previous Cray

universal

two-factor

Universal two-factor

- Open standard for a two-factor device
 - FIDO Alliance
 - Multiple hardware manufacturers
 - USB, NFC or Bluetooth
 - Multiple server and host implementations



Universal two-factor

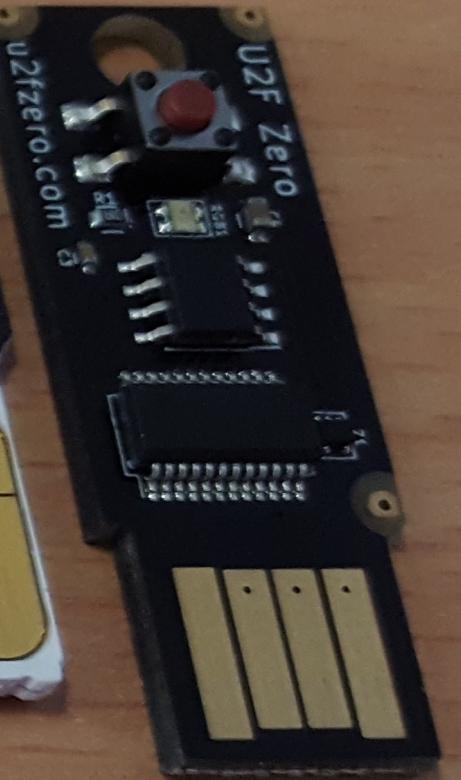
- Active device
 - Participates directly in authentication process
 - Public key crypto



Universal two-factor

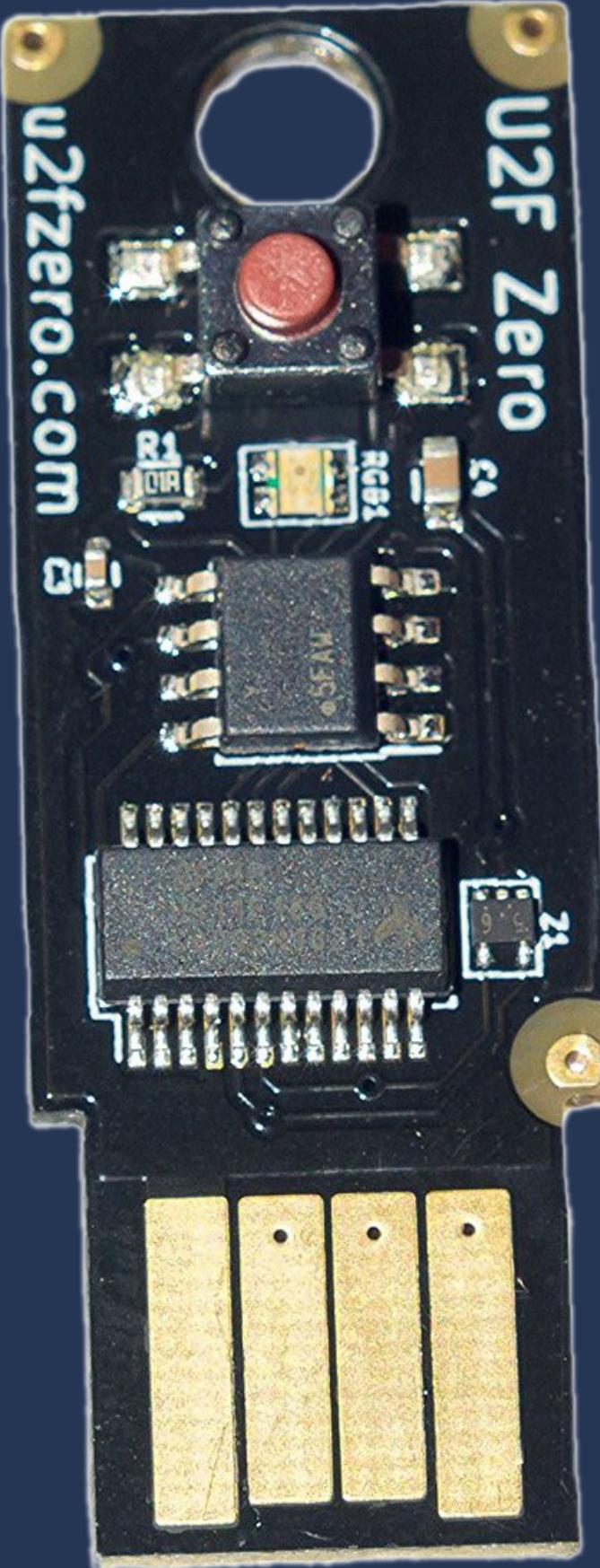
- One device, multiple sites
- Phishing protection
- Cloning protection
- Device properties





U2F Zero

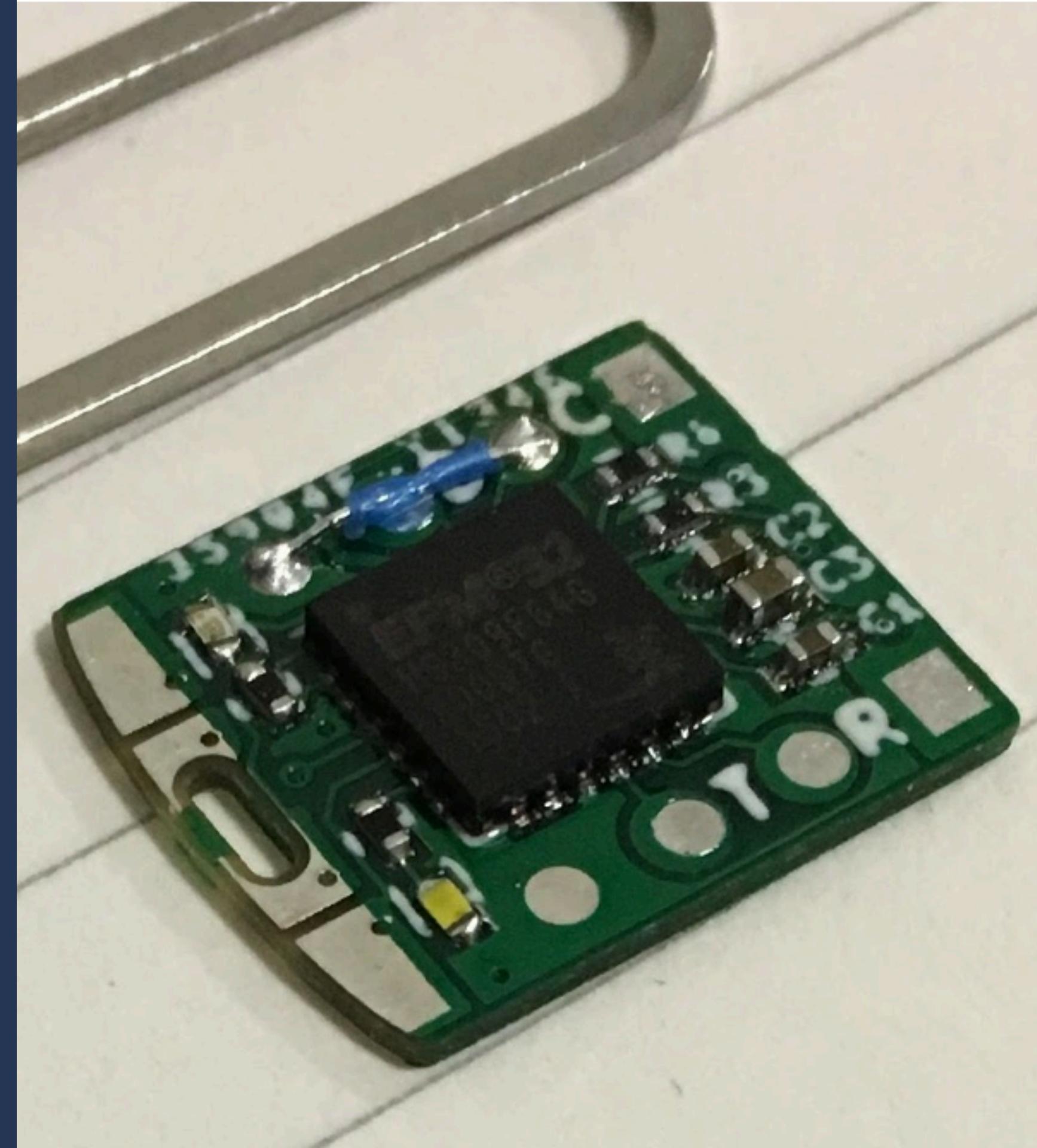
<https://u2fzero.com/>



Tomu

<https://tomu.im/>

- A tiny computer that fits inside your USB port
 - ARM CPU
 - Two buttons
 - Two LEDs
- Open Hardware Certified



Tomu

<https://tomu.im/>

- Designed by Tim Ansell
- Planned to be a U2F device
- Needs software
- You can help!



U2F registration

Set Up Security Key

1 Insert your security key into the computer. Then if it has a button, press it.



Waiting for device

U2F registration

Set Up Security Key

1 Insert your security key into the computer. Then if it has a button, press it.



Got it

U2F authentication

Insert your security key into the computer. Then if it has a button, press it.



Waiting for device

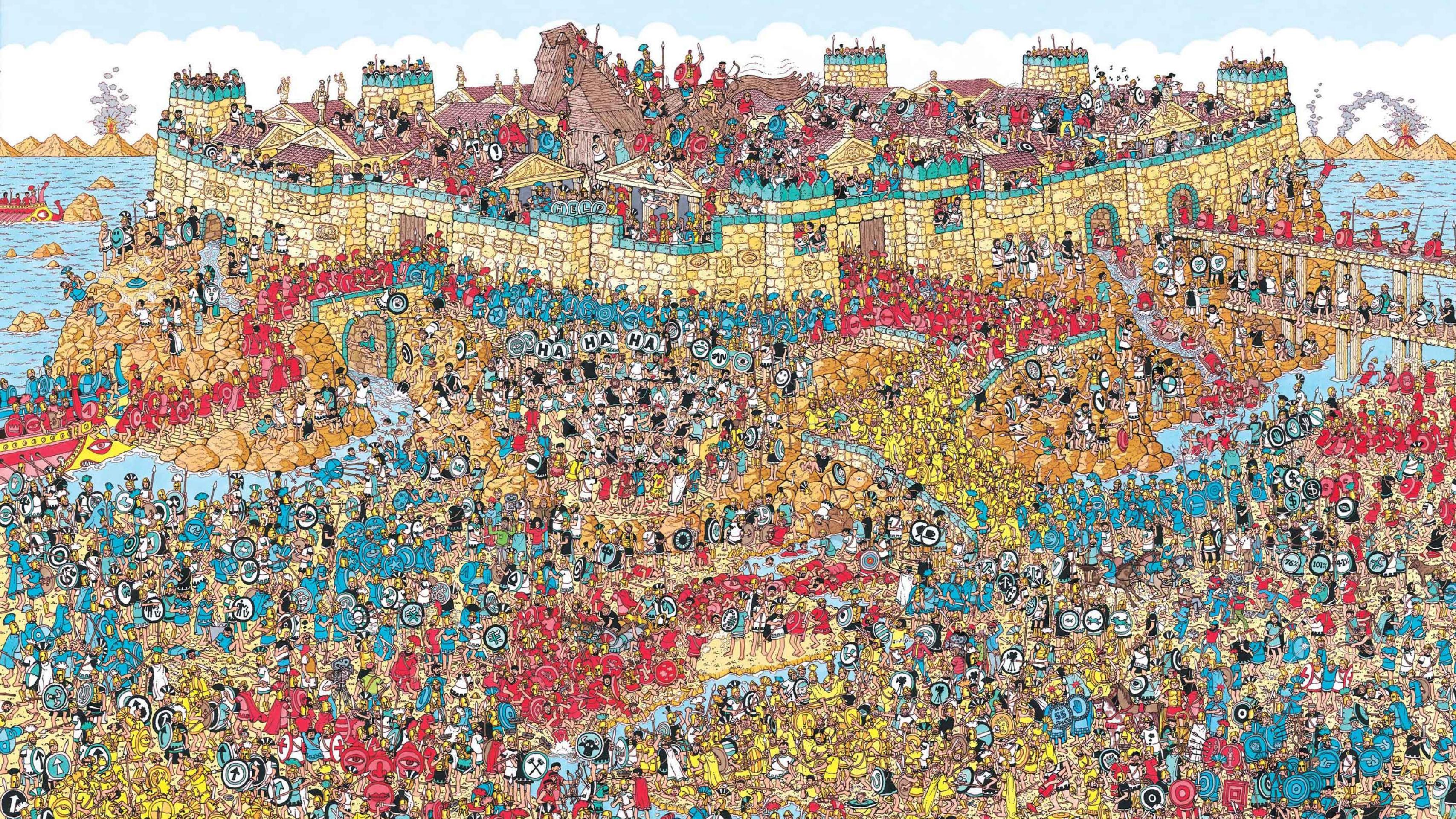
Don't require two-step verification again on this device

U2F authentication

Insert your security key into the computer. Then if it has a button, press it.

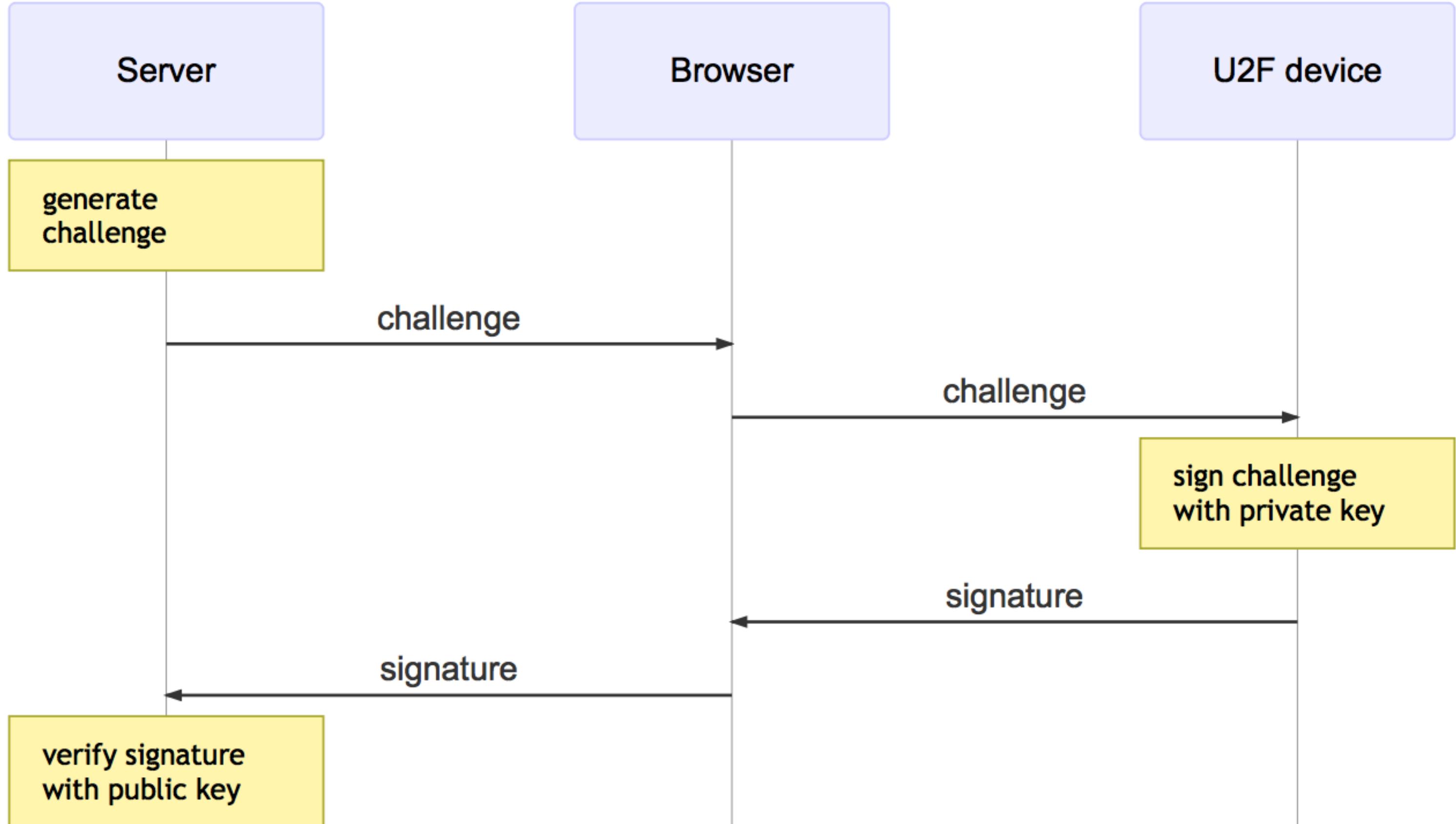
Got it

Don't require two-step verification again on this device



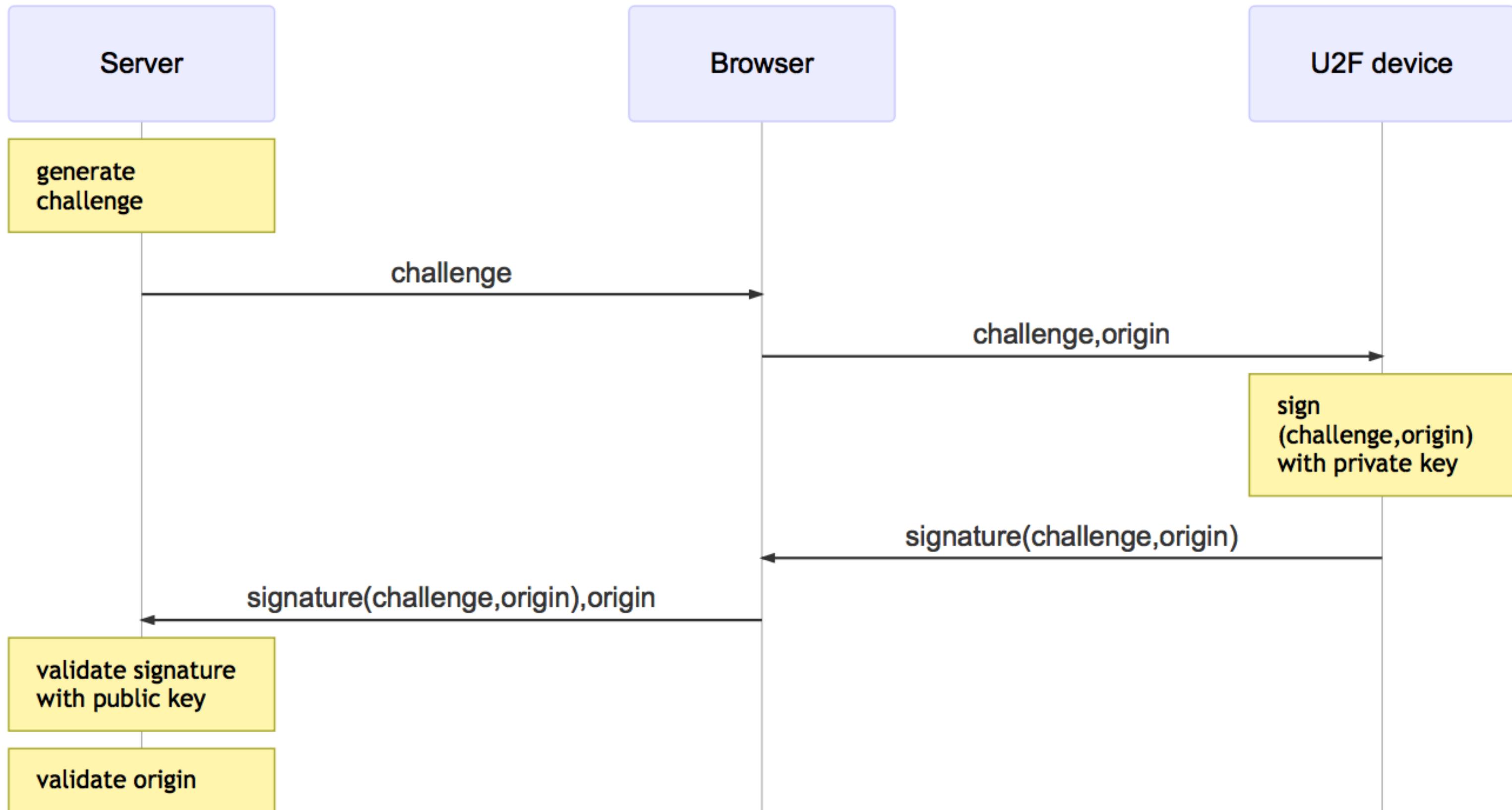


Authentication flow



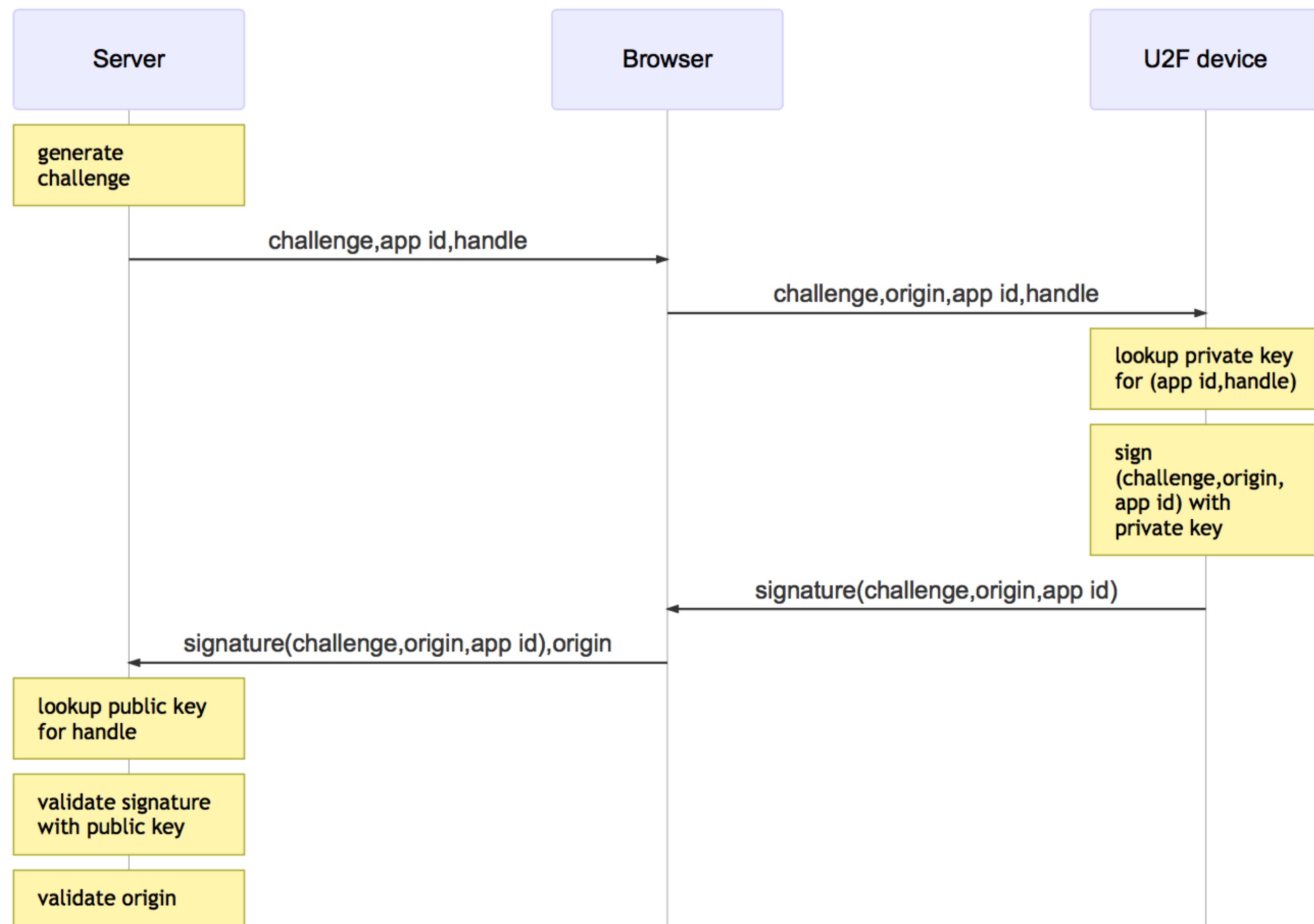
A fluffy brown and white cat is sitting on a wooden surface, looking down at a clear glass bowl filled with colorful marbles. The cat's fur is soft and textured, and it appears curious about the marbles. The background is slightly blurred, showing more of the wooden floor and some household items.

Phishing protection



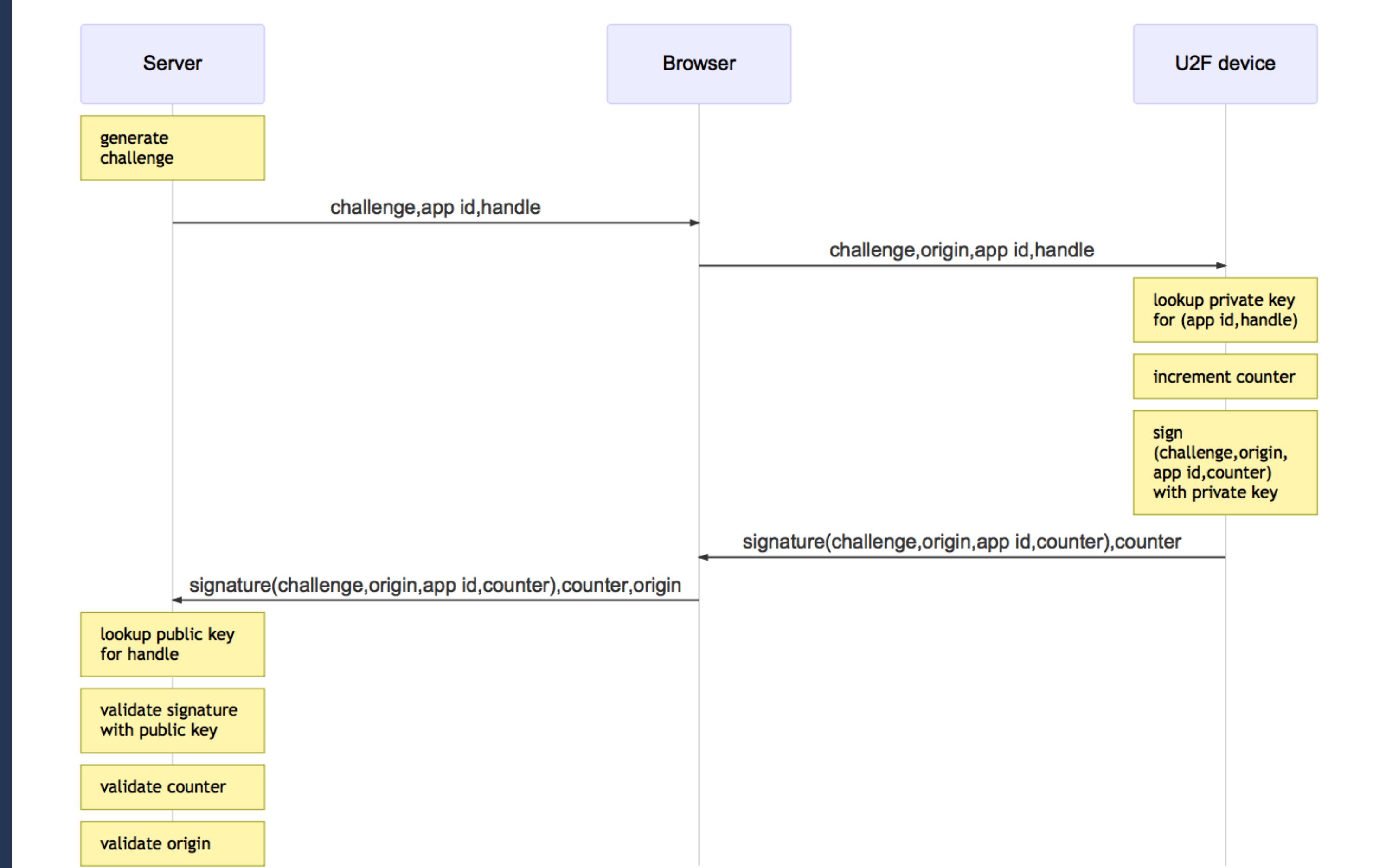


**Application-
specific
keys**



A photograph of a group of white sheep grazing in a green field. In the background, there is a line of trees under a clear sky.

cloning
protection





**Registration
flow**



A large, dark grey seal, possibly a Southern Elephant Seal, is lying on its side on a rocky beach. It has a thick, textured skin and a small patch of reddish-pink skin near its flipper. The background shows a vast, cloudy sky and more seals in the distance.

Attestation certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 776137165 (0x2e42e9cd)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Yubico U2F Root CA Serial 457200631

Validity

Not Before: Aug 1 00:00:00 2014 GMT

Not After : Sep 4 00:00:00 2050 GMT

Subject: CN=Yubico U2F EE Serial 776137165

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

EC Public Key:

pub:

04:49:ba:3d:d4:9c:3b:a1:5b:d5:b8:75:8d:ef:db:
49:2e:2a:8c:3e:3f:70:02:c4:4d:5d:d4:83:3f:9f:
c0:ce:40:9d:91:37:4a:f0:51:7a:f2:00:6a:ba:39:
c2:fb:73:1b:36:71:a0:ce:5c:e9:da:c1:84:b5:61:
95:b9:70:cd:4c

ASN1 OID: prime256v1

Implementation details



Serverland

- Perl, Ruby, Python, PHP, Java, C#, C, Go, Javascript...
- Provide three main functions
 - Generate a challenge
 - Verify a registration response
 - Verify an authentication response

Browserland

- Javascript
- Browser support
 - Chromium-based browsers (Chrome, Opera) via u2f-api.js
 - Firefox via extension (native Real Soon Now™)
 - ...
- Mobile
 - Android + Chrome + Google Authenticator + NFC

Browserland

```
u2f.register(location.origin, // appId
  [{ challenge: '...', version: 'U2F_V2' }],
  [],
  function (r) {
    if (r.errorCode) {
      alert("something bad happened: "+r.errorCode);
      return;
    }
    // send r.registrationData and r.clientData
    // to server via XHR, form POST, etc
  }
);
```

Browserland

```
u2f.sign(location.origin, // appId
  [{ challenge: '...', version: 'U2F_V2' }] ,
  [{ keyHandle: '...', version: 'U2F_V2' }] ,
  function (r) {
    if (r.errorCode) {
      alert("something bad happened: "+r.errorCode);
      return;
    }
    // send r.keyHandle, r.signatureData and r.clientData
    // to server via XHR, form POST, etc
  }
);
```

Browserless



libu2f-host

pam-u2f

Bonus prize round!



U 2 can U2F!



U 2 can U2F!

- U2F is an open standard
- Secure
- Easy to use
- Lots of hardware to choose from, or build your own
- Simple to implement





Questions?