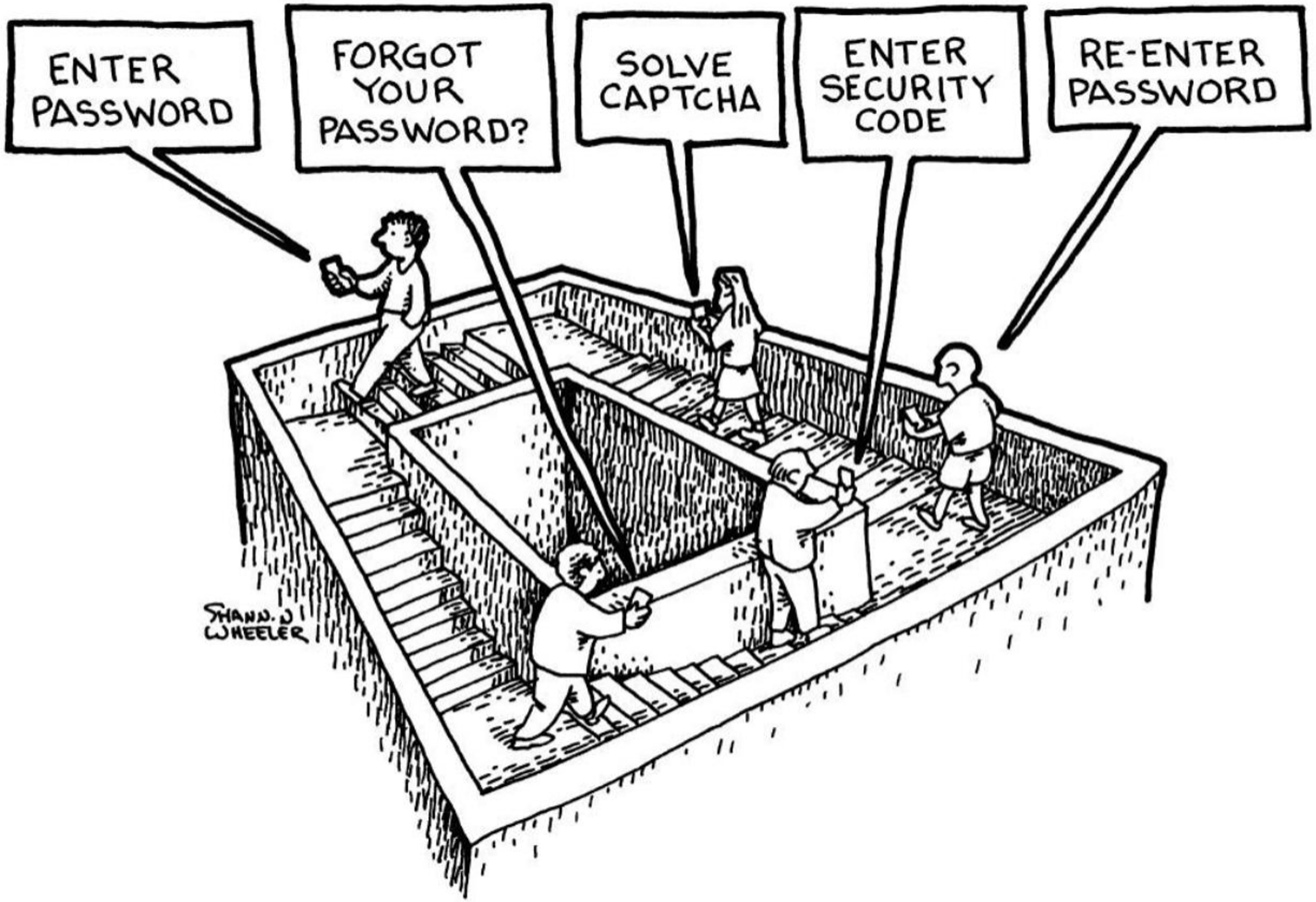
Going passwordless

Faster, easier, and more secure customer logins with passkeys

Toby Allen



ENTER PASSWORD
FORGOT YOUR PASSWORD?
SOLVE CAPTCHA
ENTER SECURITY CODE
RE-ENTER PASSWORD
SHAWN WHEELER

Lower conversions, weaker security, & more costs

43%

of lost revenue due to passwords

Okta Customer Identity Trends Report

49%

of breaches involve stolen credentials

Verizon Data Breach Investigation Report

$20

cost per call center password reset

Forrester: FIDO Passkeys and the Future of Authentication

Passwords are insecure and inconvenient resulting in breaches and lower conversion rates.

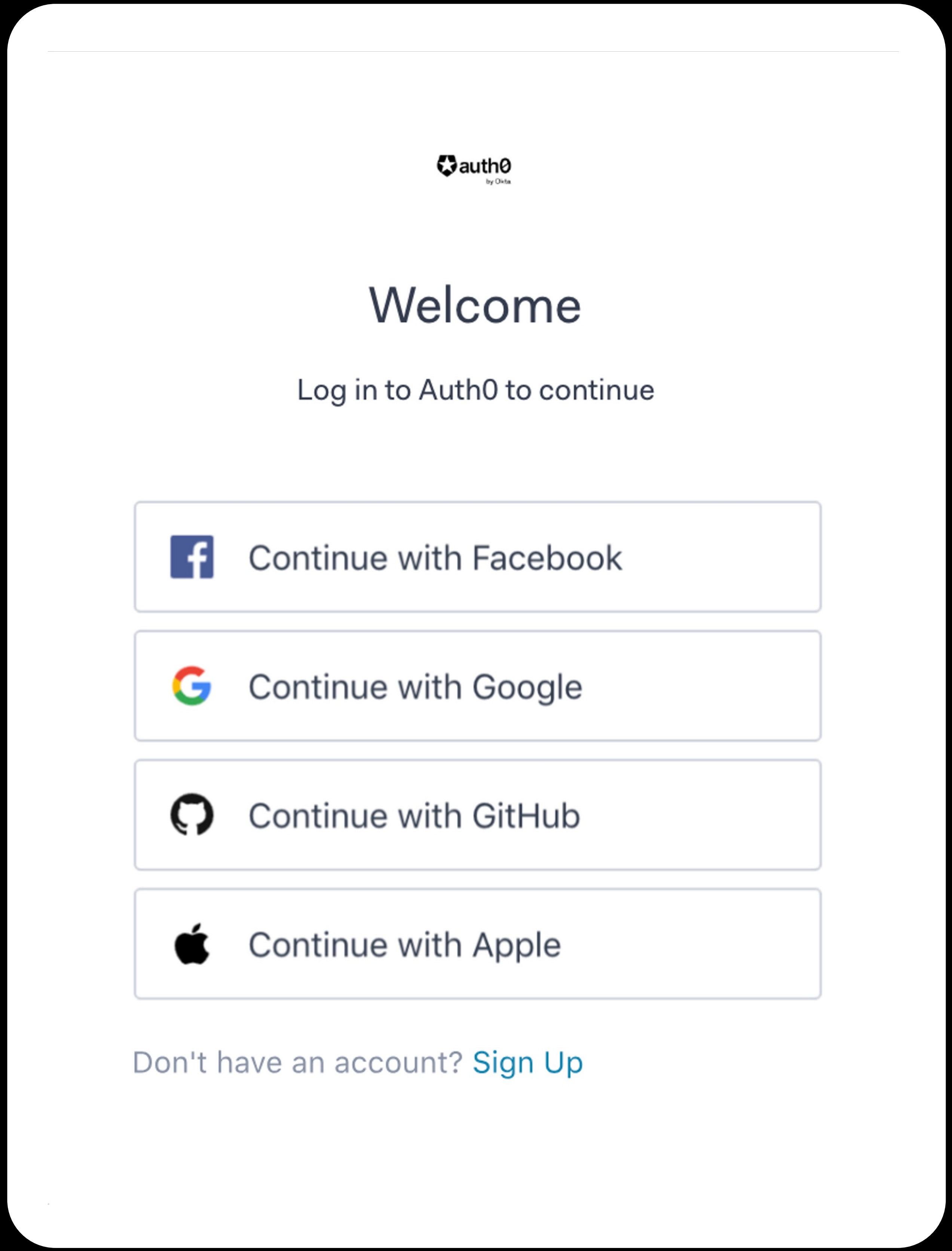
Common Passwordless Login Options

A password is an authenticator

It can be substituted by any other

Common Passwordless Approaches

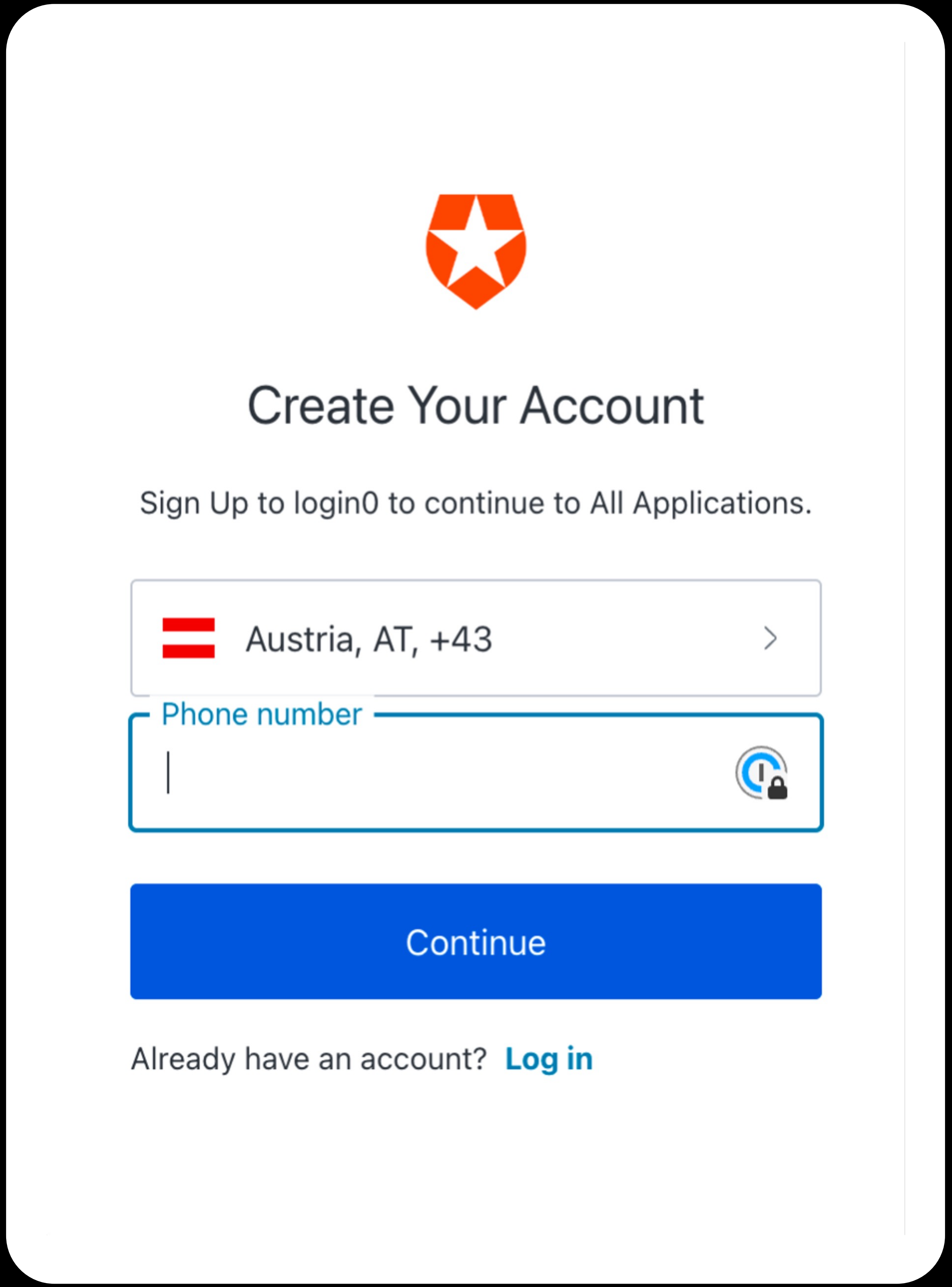
- OTP via SMS
- Email Magic Link
- Social Login
- Push Notifications
- WebAuthN?



Welcome

Log in to Auth0 to continue

Don't have an account? Sign Up



Create Your Account

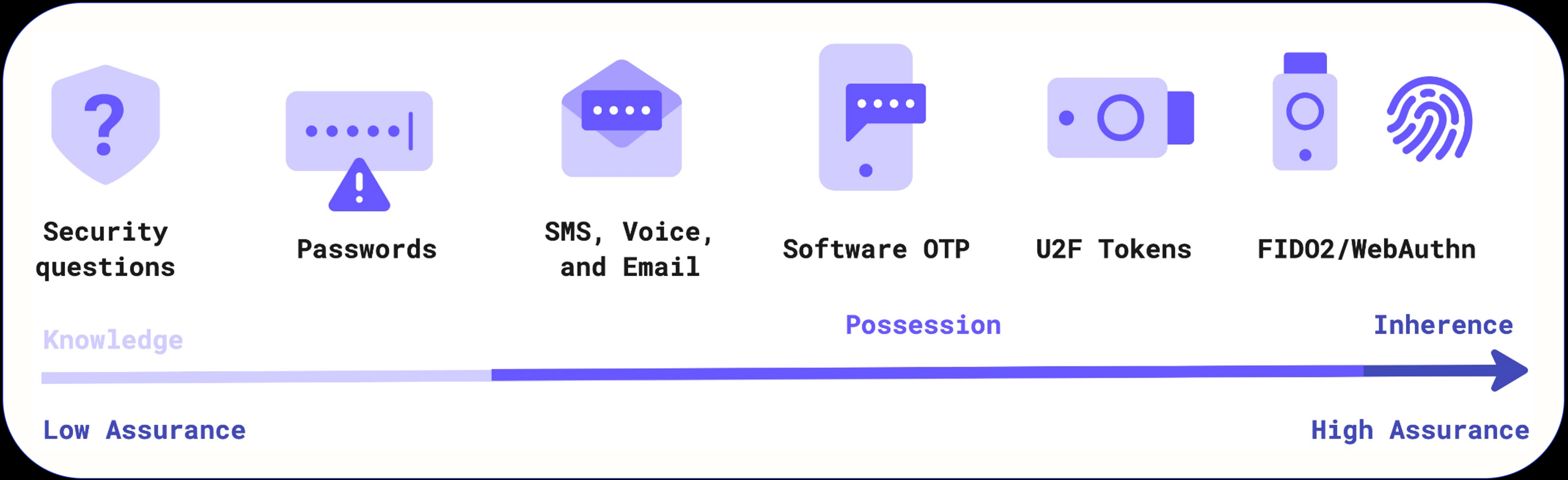
Sign Up to login0 to continue to All Applications.

Austria, AT, +43

Phone number

Already have an account? Log in

Not all Factors Are Created Equal



Security questions

Passwords

SMS, Voice, and Email

Software OTP

U2F Tokens

FIDO2/WebAuthn

Knowledge

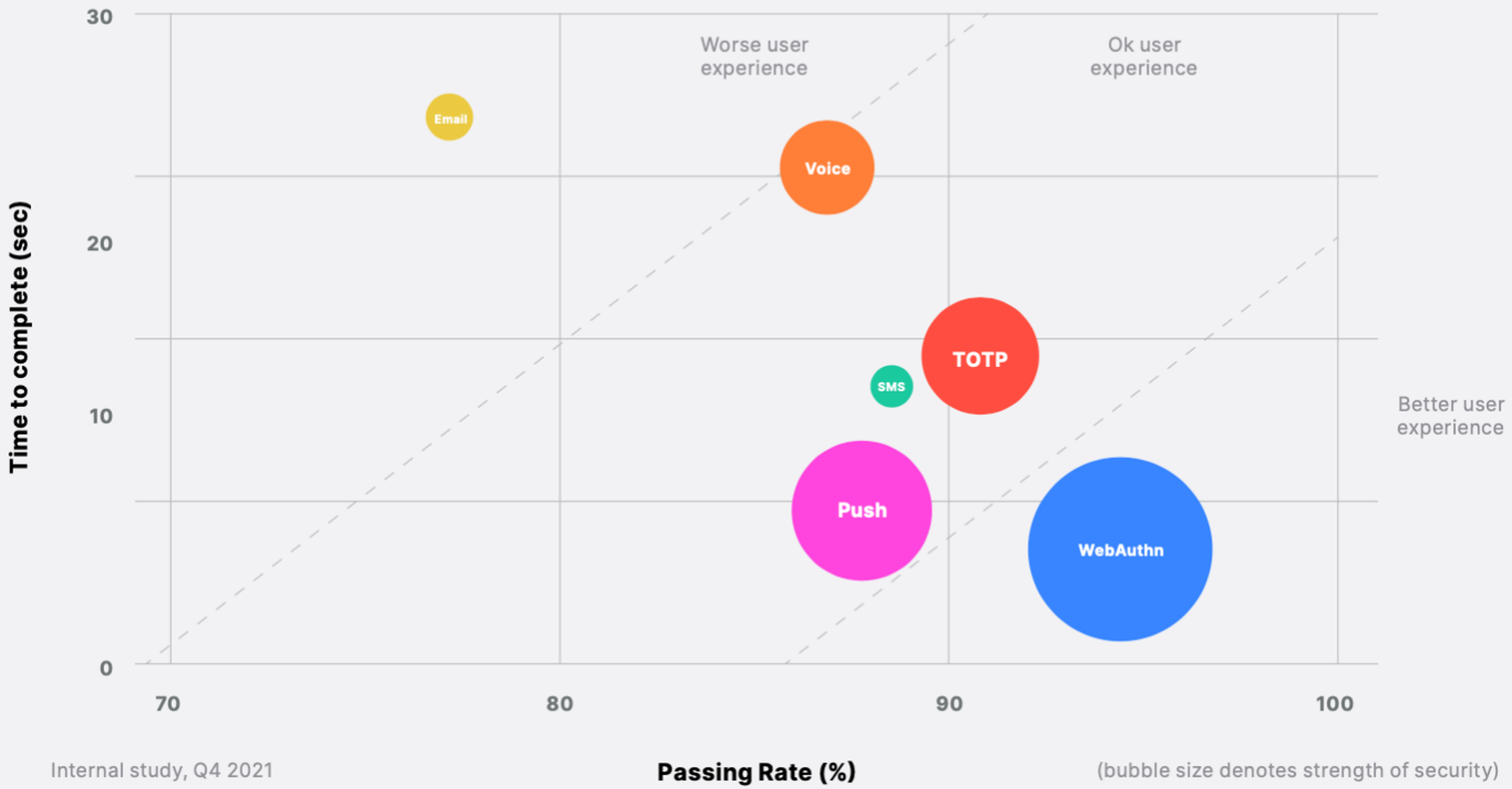
Possession

Inherence

Low Assurance

High Assurance

Not all Factors Are Created Equal

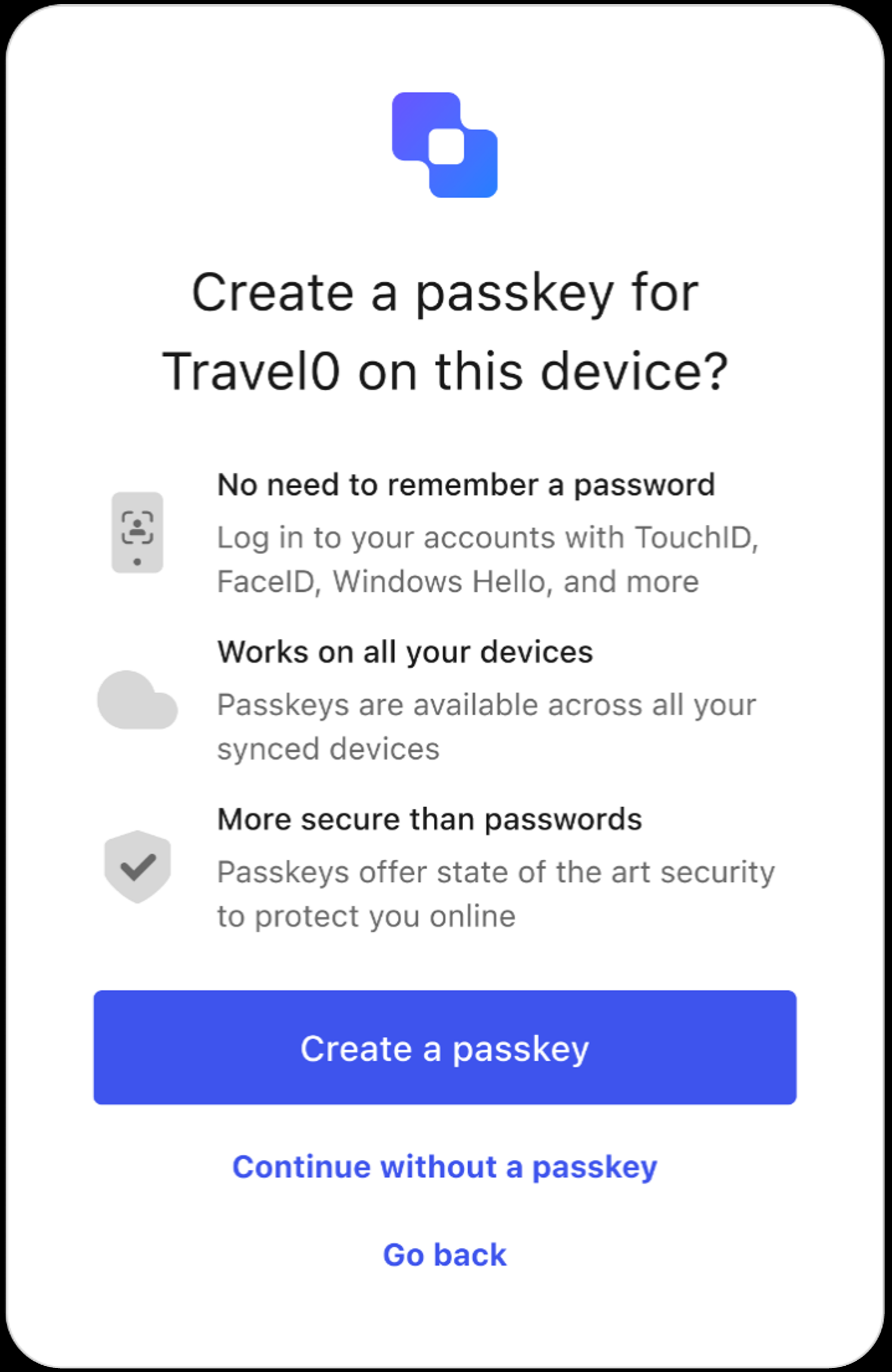


Internal study, Q4 2021

(bubble size denotes strength of security)

Enrollment friction sidelined WebAuthn

Faster, easier, and more secure customer logins with passkeys



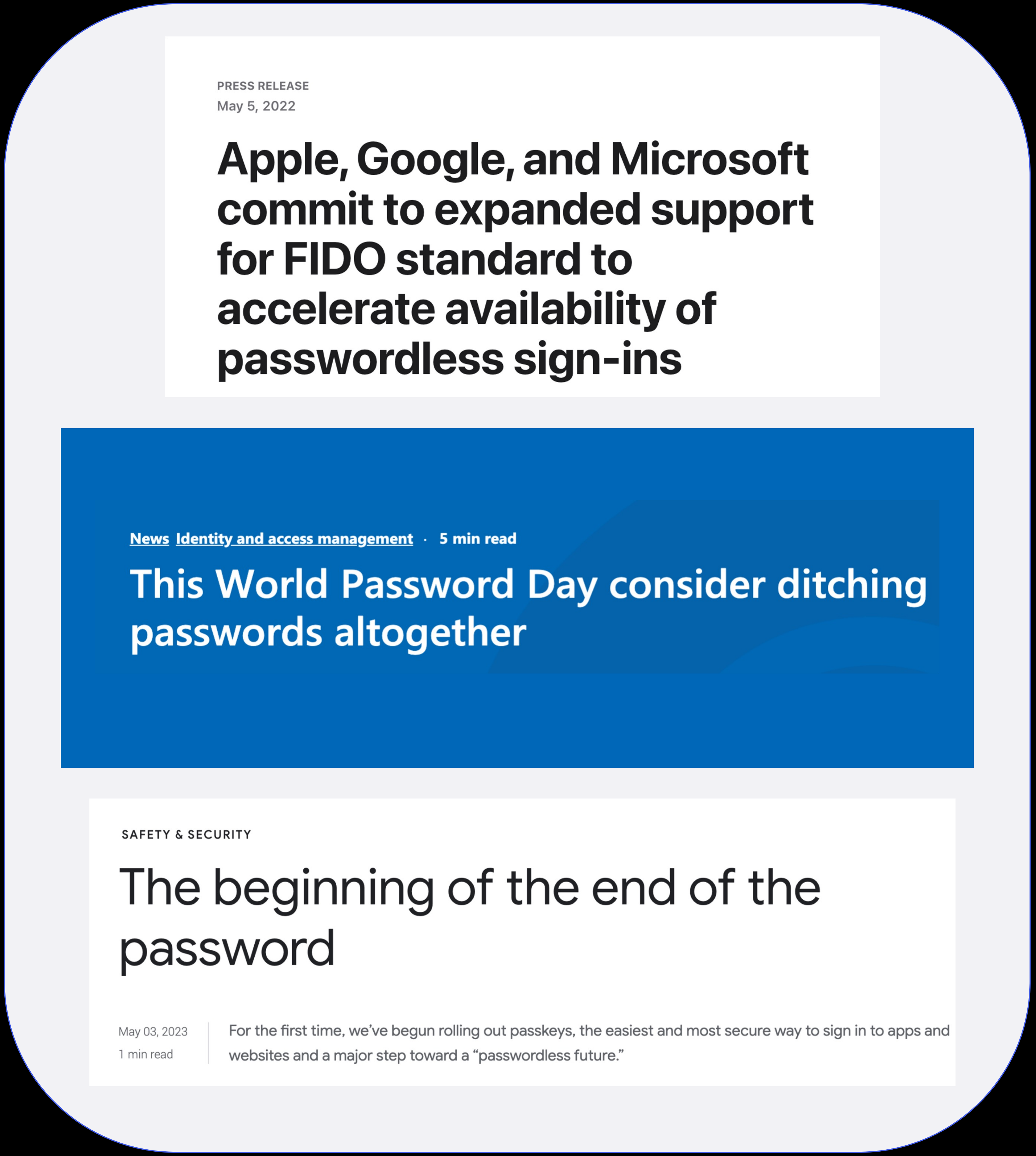
Create a passkey for Travel0 on this device?

No need to remember a password
Log in to your accounts with TouchID, FaceID, Windows Hello, and more

Works on all your devices
Passkeys are available across all your synced devices

More secure than passwords
Passkeys offer state of the art security to protect you online

Platform players commit to a passwordless future



PRESS RELEASE
May 5, 2022

Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless sign-ins

News Identity and access management · 5 min read

This World Password Day consider ditching passwords altogether

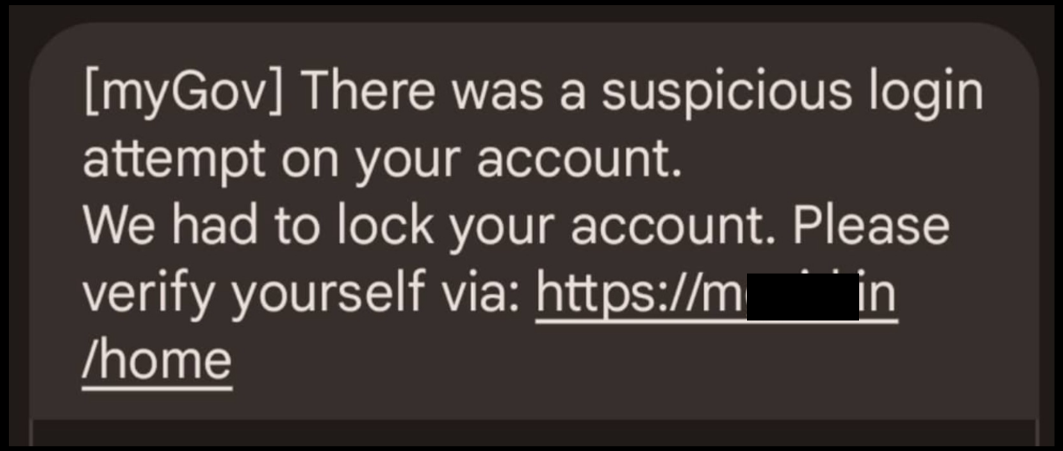
SAFETY & SECURITY

The beginning of the end of the password

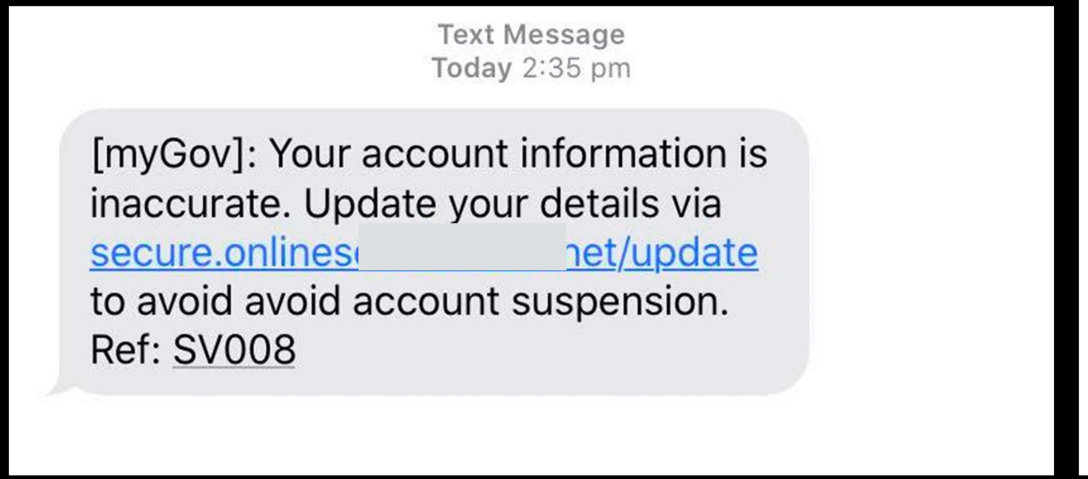
May 03, 2023
1 min read

For the first time, we've begun rolling out passkeys, the easiest and most secure way to sign in to apps and websites and a major step toward a "passwordless future."

Australia to introduce passkeys for myGov login

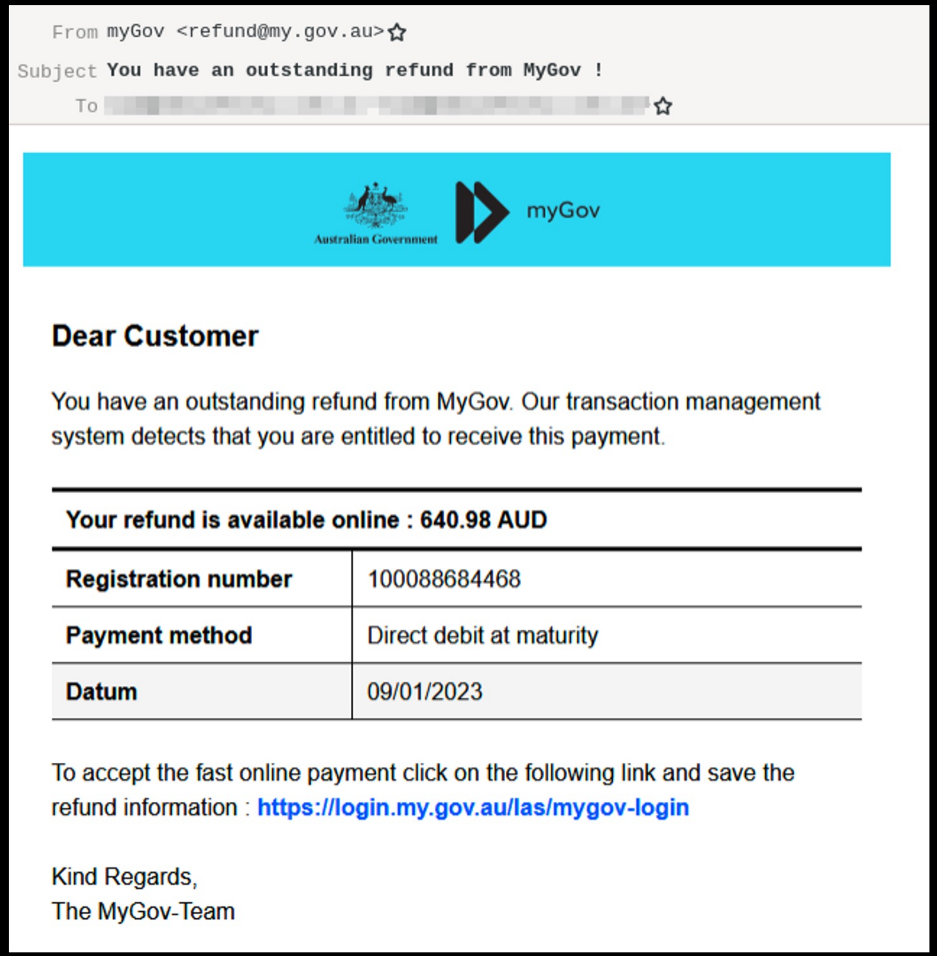


[myGov] There was a suspicious login attempt on your account.
We had to lock your account. Please verify yourself via: https://m[redacted]in/home



Text Message
Today 2:35 pm

[myGov]: Your account information is inaccurate. Update your details via secure.onlines[redacted]net/update to avoid avoid account suspension.
Ref: SV008



From myGov <refund@my.gov.au>
Subject You have an outstanding refund from MyGov !
To [redacted]

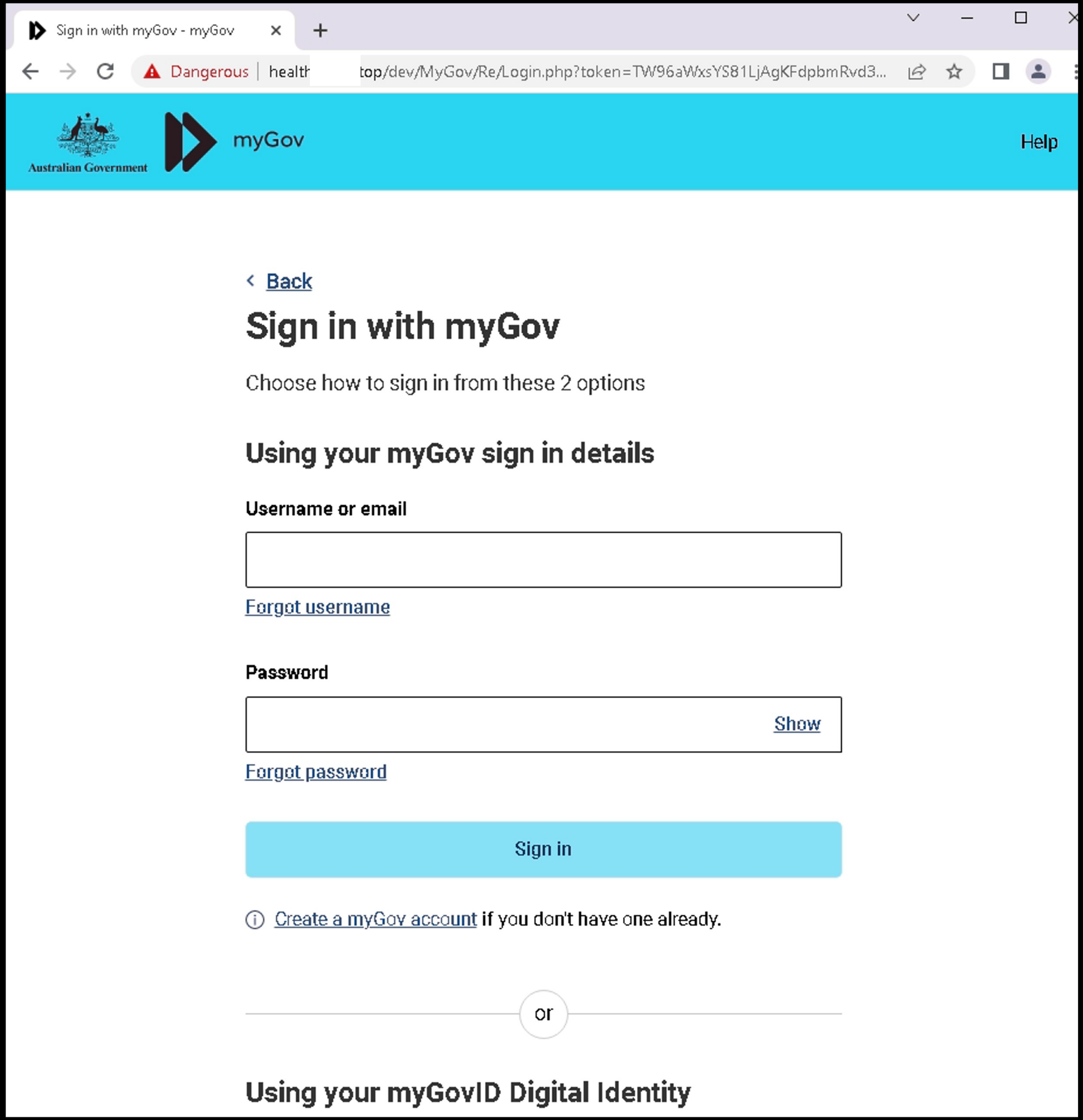
Dear Customer

You have an outstanding refund from MyGov. Our transaction management system detects that you are entitled to receive this payment.

Your refund is available online : 640.98 AUD	
Registration number	100088684468
Payment method	Direct debit at maturity
Datum	09/01/2023

To accept the fast online payment click on the following link and save the refund information : **https://login.my.gov.au/las/mygov-login**

Kind Regards,
The MyGov-Team



Sign in with myGov - myGov
Dangerous | health
top/dev/MyGov/Re/Login.php?token=TW96aWxsYS81LjAgKFdpbmRvd3...
Australian Government
myGov
Help

‹ Back

Sign in with myGov

Choose how to sign in from these 2 options

Using your myGov sign in details

Username or email

Forgot username

Password

Show

Forgot password

Sign in

ⓘ Create a myGov account if you don't have one already.

or

Using your myGovID Digital Identity

Australians have already lost **$3.1bn** to scams this year and myGov – which hosts Centrelink, Australian Tax Office and Medicare data – is an attractive target for criminals looking to steal sensitive information.

Source: https://www.mailguard.com.au/

Passkeys are a password replacement that provide faster, easier, and more secure sign-ins to websites and apps across a user’s devices. Unlike passwords, passkeys are resistant to phishing, are always strong, and are designed so that there are no shared secrets.

– FIDO Alliance

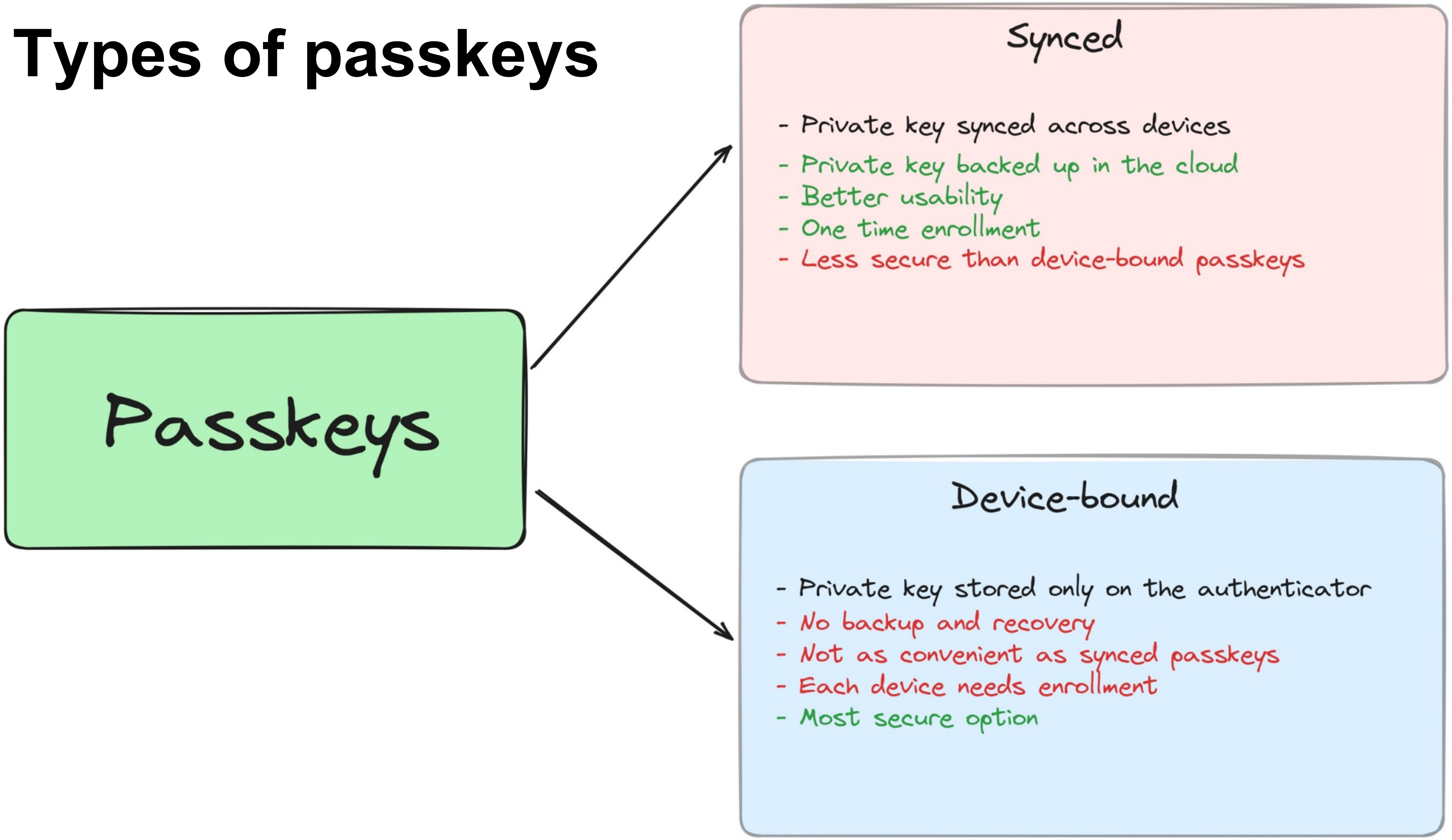
So… What are passkeys?

Passkeys are an intuitive discoverable credential

Passkey properties

- Discoverable
- Phishing Resistant
- Remote attack resistant
- Breach resistant
- Not reusable / unique per service
- Not easily shareable*
- Allow Cross-device Authentication

Types of passkeys



Passkeys

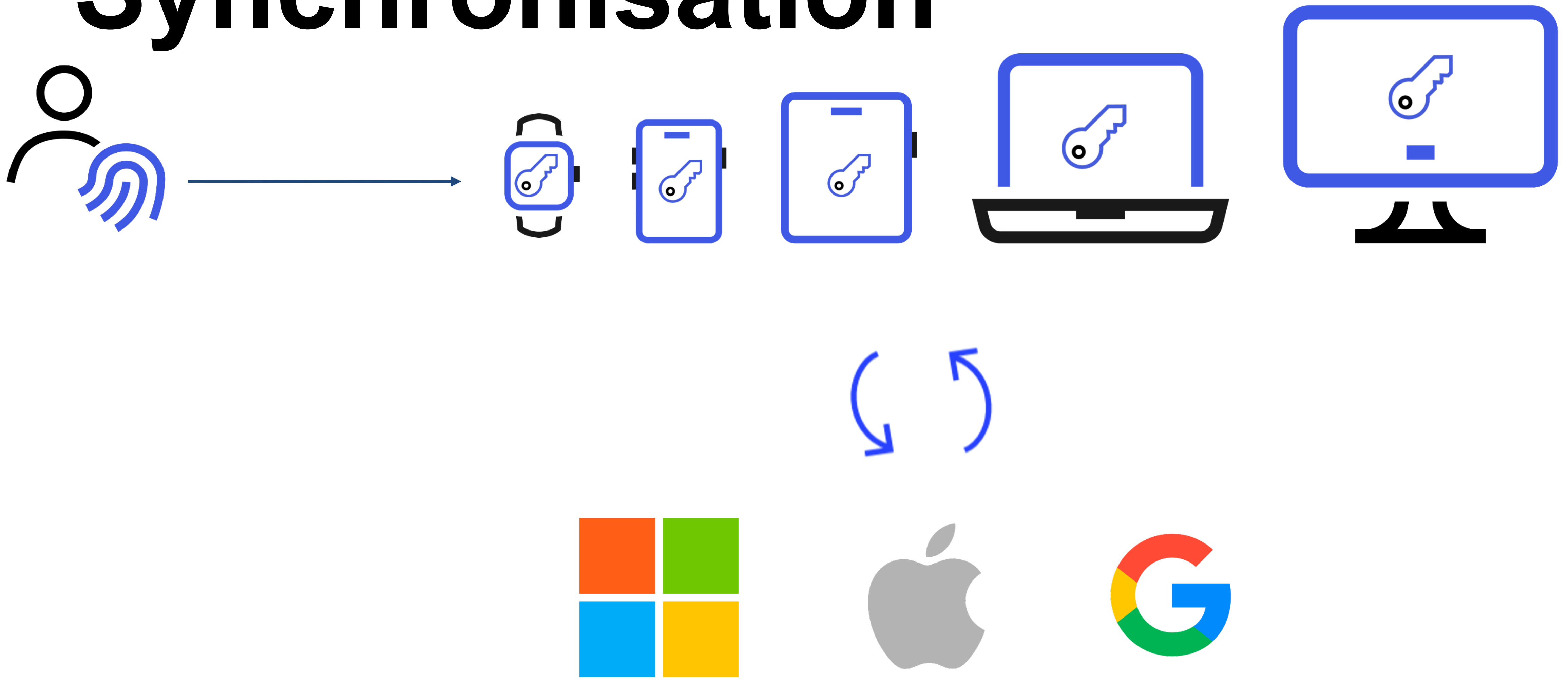
Synced

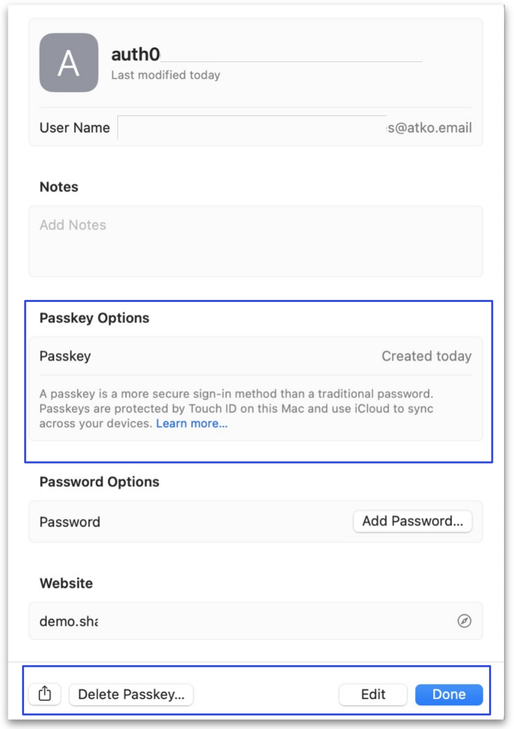
- Private key synced across devices
- Private key backed up in the cloud
- Better usability
- One time enrollment
- Less secure than device-bound passkeys

Device-bound

- Private key stored only on the authenticator
- No backup and recovery
- Not as convenient as synced passkeys
- Each device needs enrollment
- Most secure option

Synchronisation





auth0

Last modified today

User Name s@atko.email

Notes

Add Notes

Passkey Options

Passkey — Created today

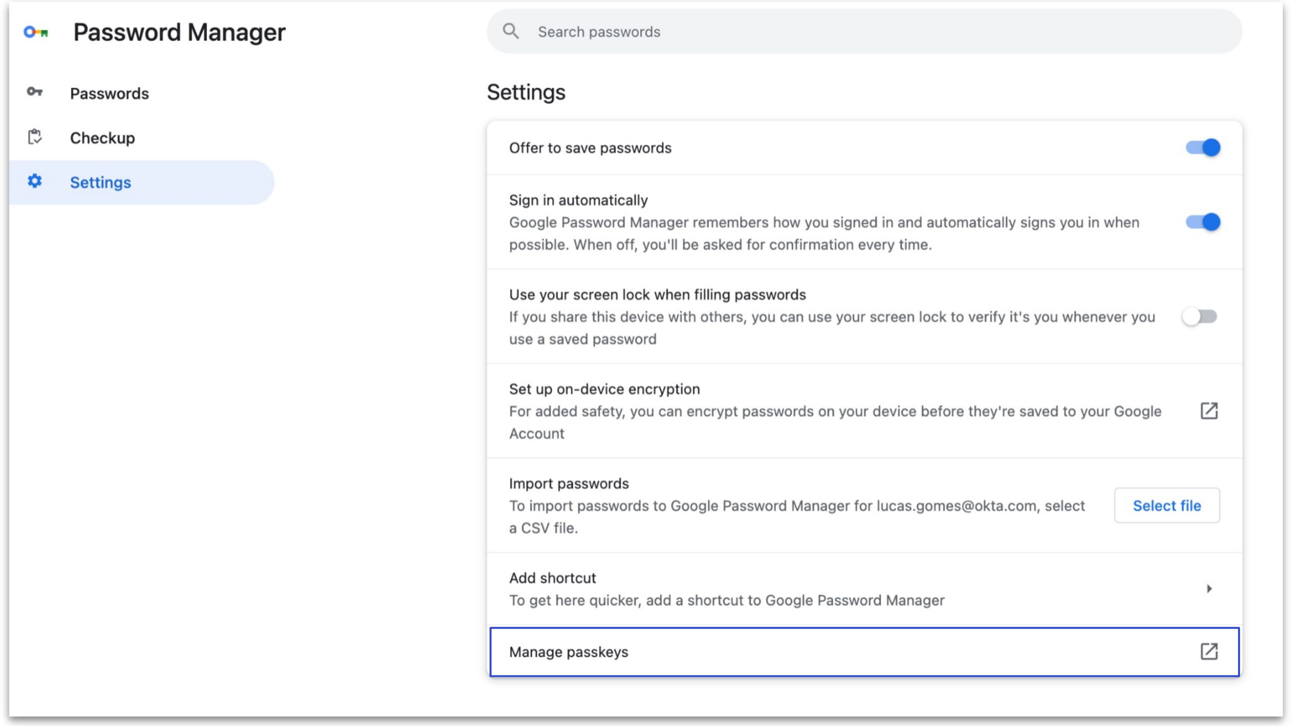
A passkey is a more secure sign-in method than a traditional password. Passkeys are protected by Touch ID on this Mac and use iCloud to sync across your devices. Learn more...

Password Options

Password — Add Password...

Website

demo.shi



Password Manager

Settings

- Offer to save passwords — on
- 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. — on
- Use your screen lock when filling passwords
  If you share this device with others, you can use your screen lock to verify it's you whenever you use a saved password — off
- Set up on-device encryption
  For added safety, you can encrypt passwords on your device before they're saved to your Google Account
- Import passwords
  To import passwords to Google Password Manager for lucas.gomes@okta.com, select a CSV file. — Select file
- Add shortcut
  To get here quicker, add a shortcut to Google Password Manager
- Manage passkeys

- Make passkeys available automatically across devices within the same platform
  - Apple iCloud keychain
  - Google Password Manager
  - Microsoft Hello (soon!! maybe
  - Password managers
    - 1Password
    - Dashlane
    - Bitwarden
    - …

- Backup, recovery and security are therefore vendor/platform dependent.

WebAuthN vs passkeys

- **Platform authenticators**: built into a user's device.

- **Roaming authenticators**: A removable authenticator usable with any device the user is trying to sign in from.

- A passkey is like a **syncable** platform authenticator

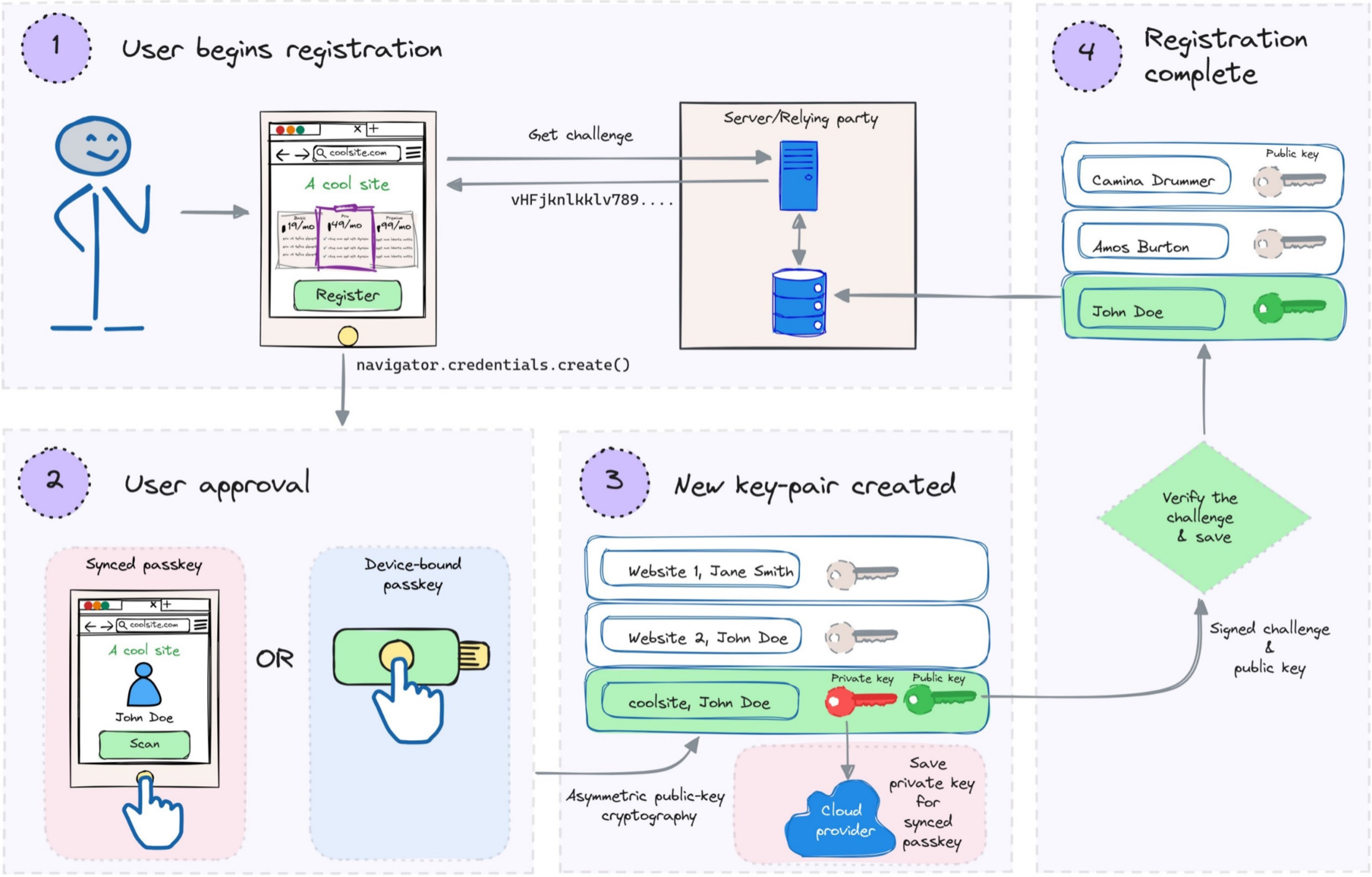
WebAuthN vs passkeys

- passkeys are discoverable
- WebAuthn MFA are non-discoverable/server-side credentials
- WebAuthN does not have a synced option
- passkeys can be a **FIRST** factor

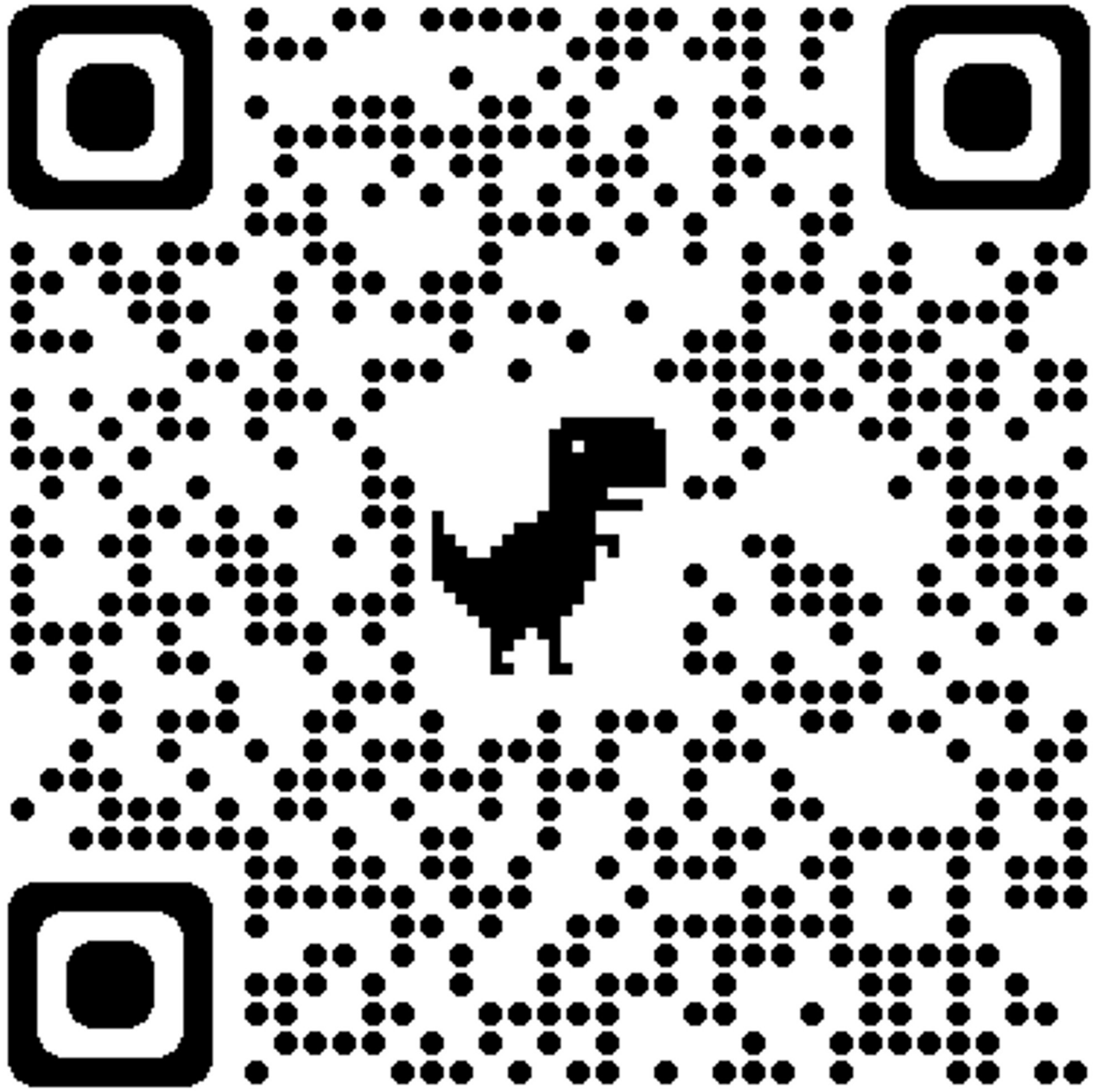
passkeys at work?

- Use WebAuthN…
- …or any supported phishing resistant authenticator

User Journeys

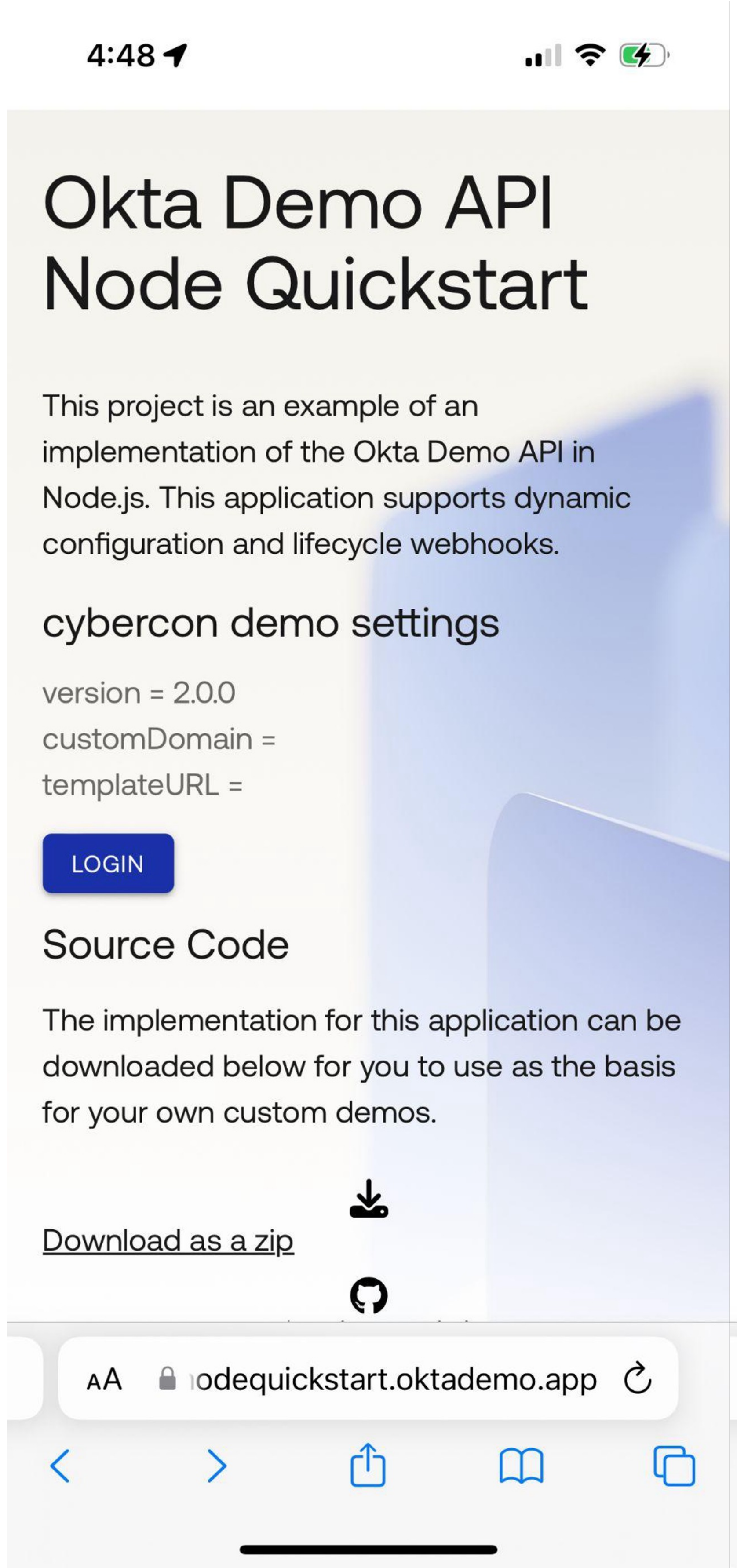

1
User begins registration
coolsite.com
A cool site
Basic
$19/mo
Pro
$49/mo
Premium
$99/mo
Register
Get challenge
vHFjknlkklv789....
Server/Relying party
navigator.credentials.create()
2
User approval
Synced passkey
coolsite.com
A cool site
John Doe
Scan
OR
Device-bound passkey
3
New key-pair created
Website 1, Jane Smith
Website 2, John Doe
coolsite, John Doe
Private key
Public key
Asymmetric public-key cryptography
Cloud provider
Save private key for synced passkey
4
Registration complete
Public key
Camina Drummer
Amos Burton
John Doe
Verify the challenge & save
Signed challenge & public key

Interactive Demo



cybercon.nodequickstart.oktademo.app

Interactive Demo



Okta Demo API Node Quickstart

This project is an example of an implementation of the Okta Demo API in Node.js. This application supports dynamic configuration and lifecycle webhooks.

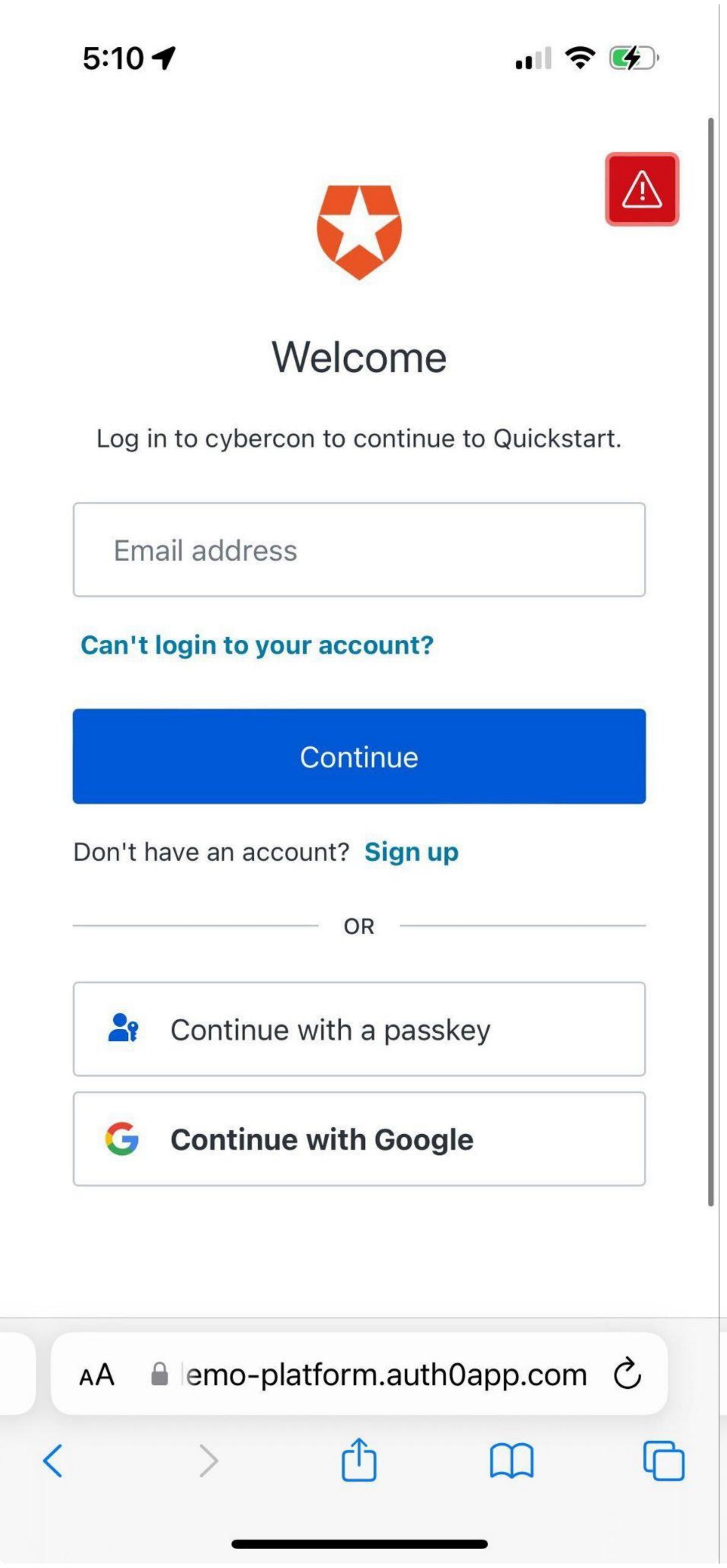
cybercon demo settings

version = 2.0.0
customDomain =
templateURL =

Source Code

The implementation for this application can be downloaded below for you to use as the basis for your own custom demos.

Download as a zip



Welcome

Log in to cybercon to continue to Quickstart.

Email address

Can't login to your account?

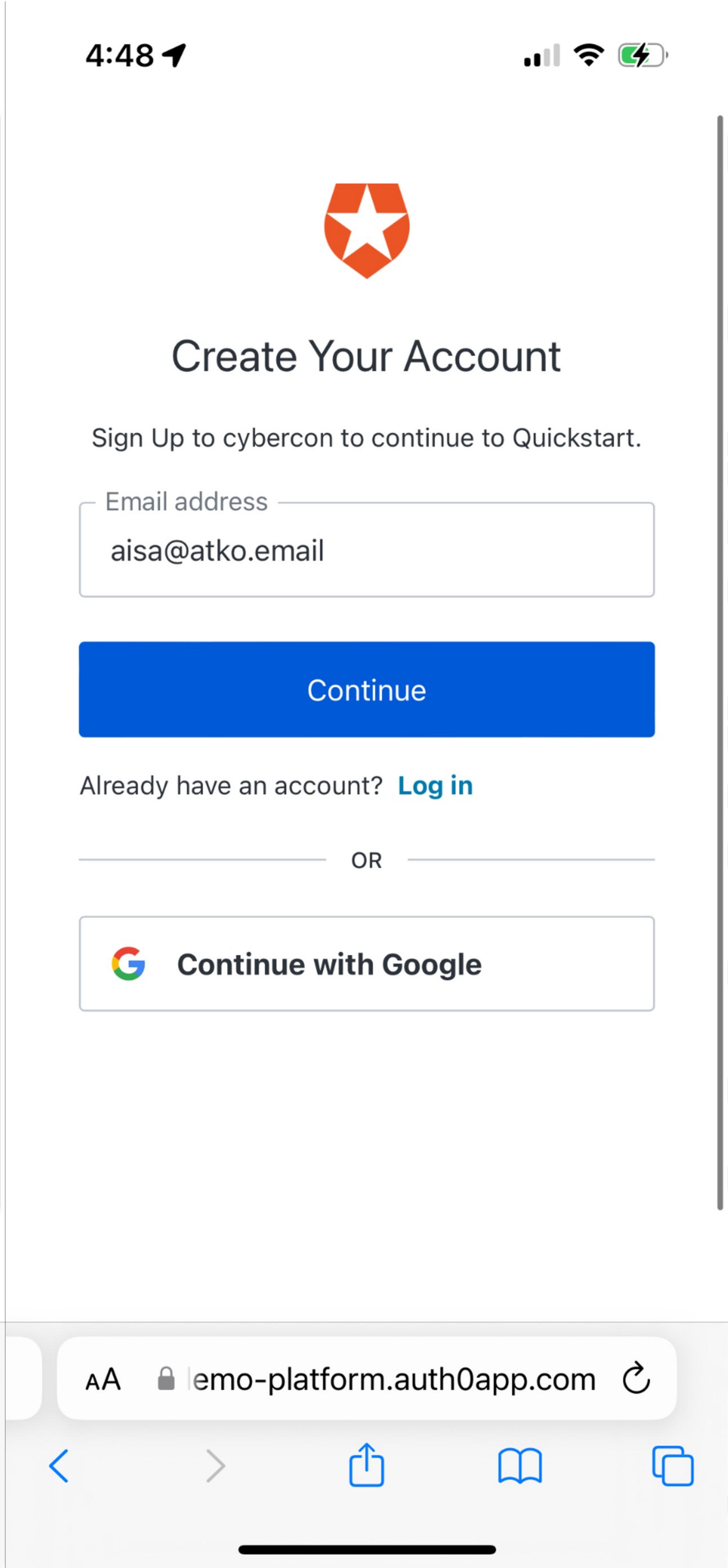
Continue

Don't have an account? Sign up

OR

Continue with a passkey

Continue with Google



Create Your Account

Sign Up to cybercon to continue to Quickstart.

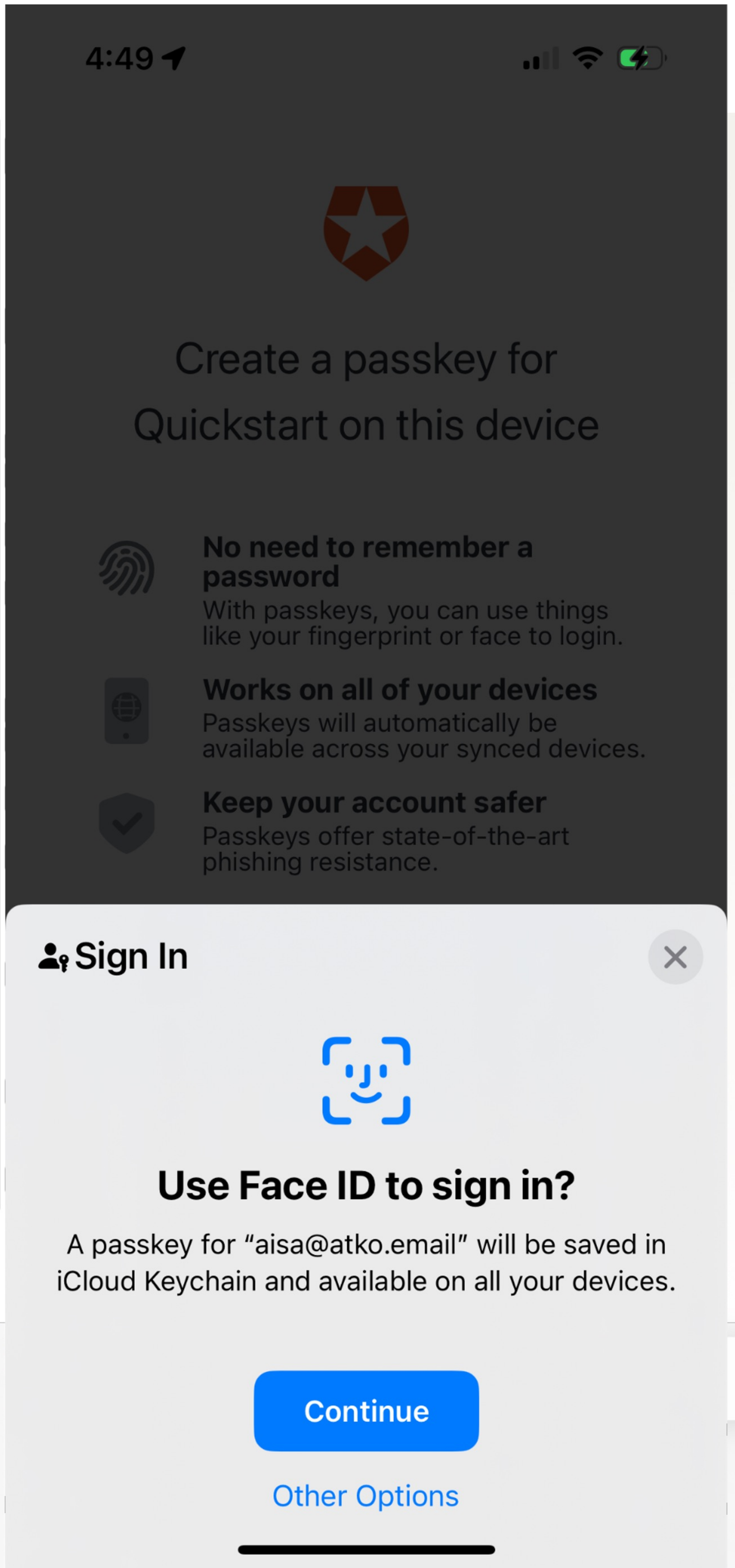
Email address: aisa@atko.email

Continue

Already have an account? Log in

OR

Continue with Google



Create a passkey for Quickstart on this device

No need to remember a password
With passkeys, you can use things like your fingerprint or face to login.

Works on all of your devices
Passkeys will automatically be available across your synced devices.

Keep your account safer
Passkeys offer state-of-the-art phishing resistance.

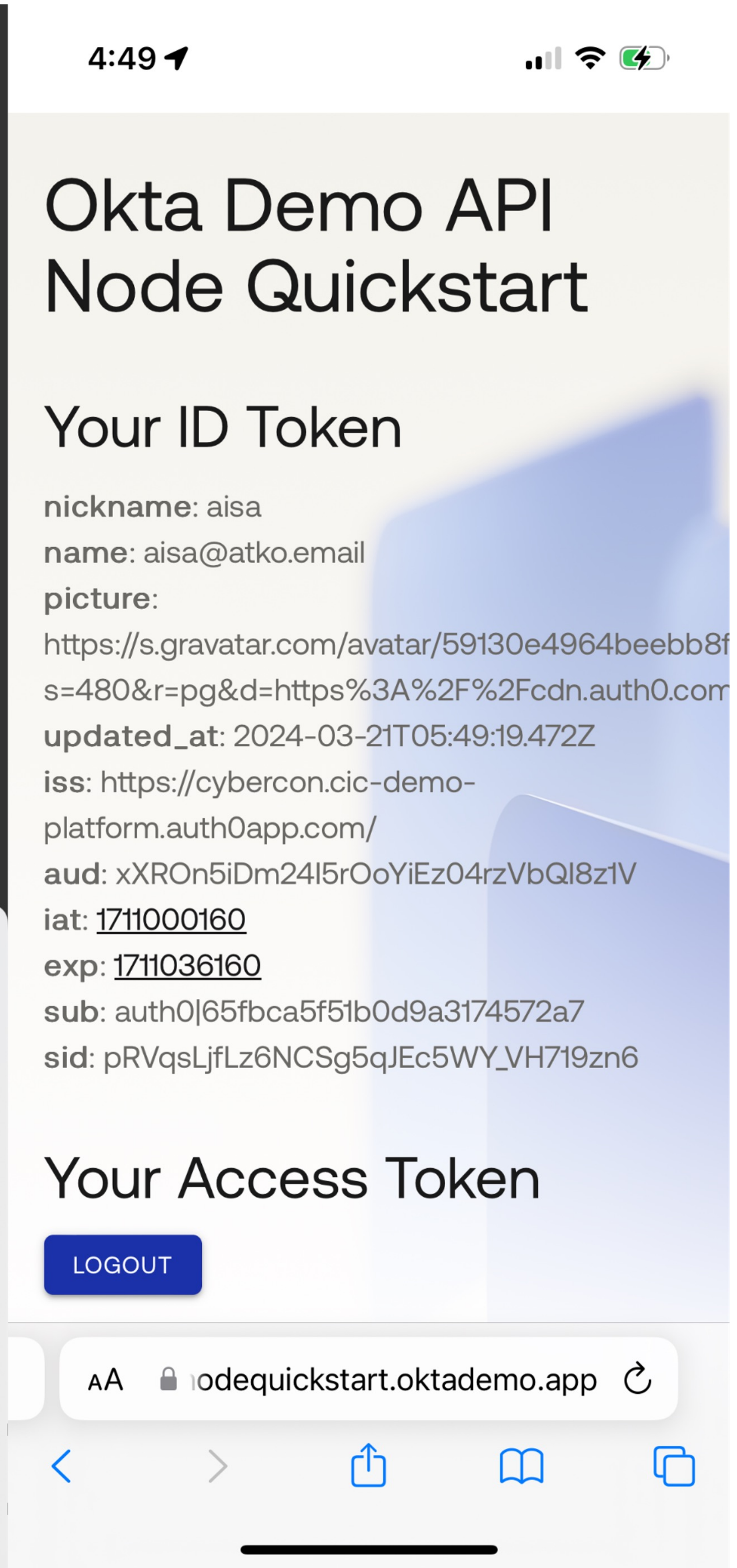
Sign In

Use Face ID to sign in?

A passkey for “aisa@atko.email” will be saved in iCloud Keychain and available on all your devices.

Continue

Other Options

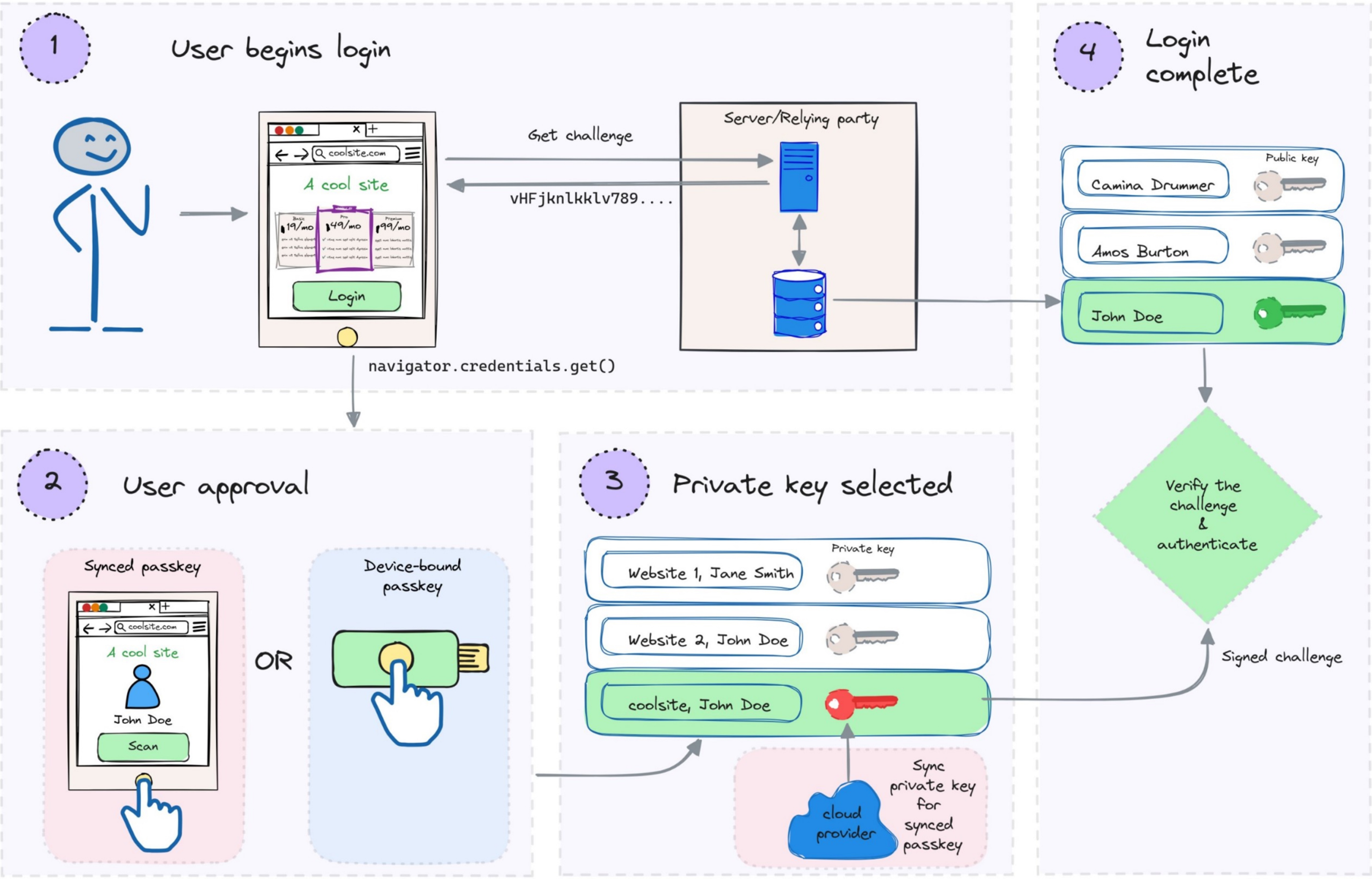


Okta Demo API Node Quickstart

Your ID Token

nickname: aisa
name: aisa@atko.email
picture:
https://s.gravatar.com/avatar/59130e4964beebb8f
s=480&r=pg&d=https%3A%2F%2Fcdn.auth0.com
updated_at: 2024-03-21T05:49:19.472Z
iss: https://cybercon.cic-demo-platform.auth0app.com/
aud: xXROn5iDm24I5rOoYiEz04rzVbQI8z1V
iat: 1711000160
exp: 1711036160
sub: auth0|65fbca5f51b0d9a3174572a7
sid: pRVqsLjfLz6NCSg5qJEc5WY_VH719zn6

Your Access Token



1 User begins login

2 User approval

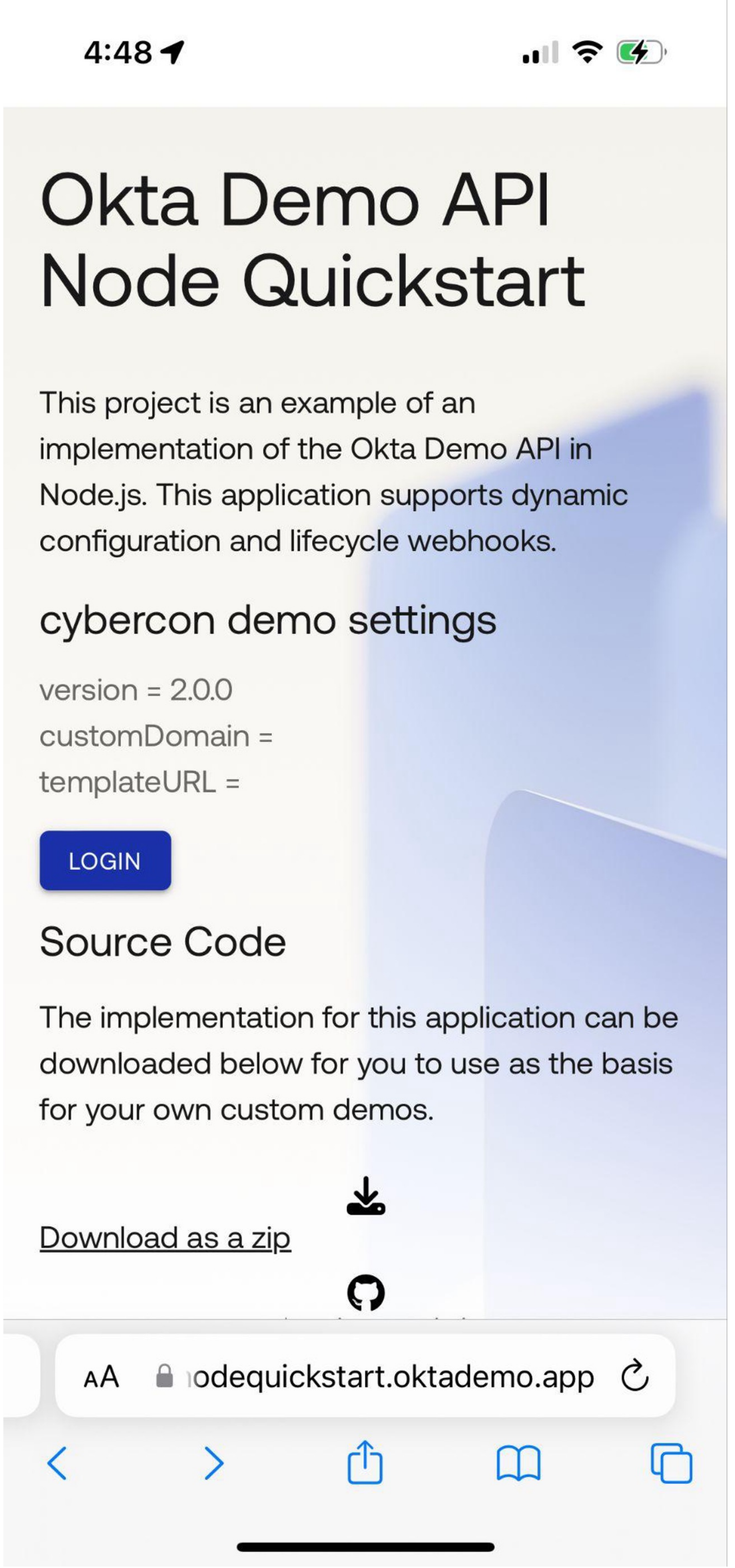
3 Private key selected

4 Login complete

Interactive Demo

cybercon.nodequickstart.oktademo.app

Interactive Demo



Okta Demo API Node Quickstart

This project is an example of an implementation of the Okta Demo API in Node.js. This application supports dynamic configuration and lifecycle webhooks.

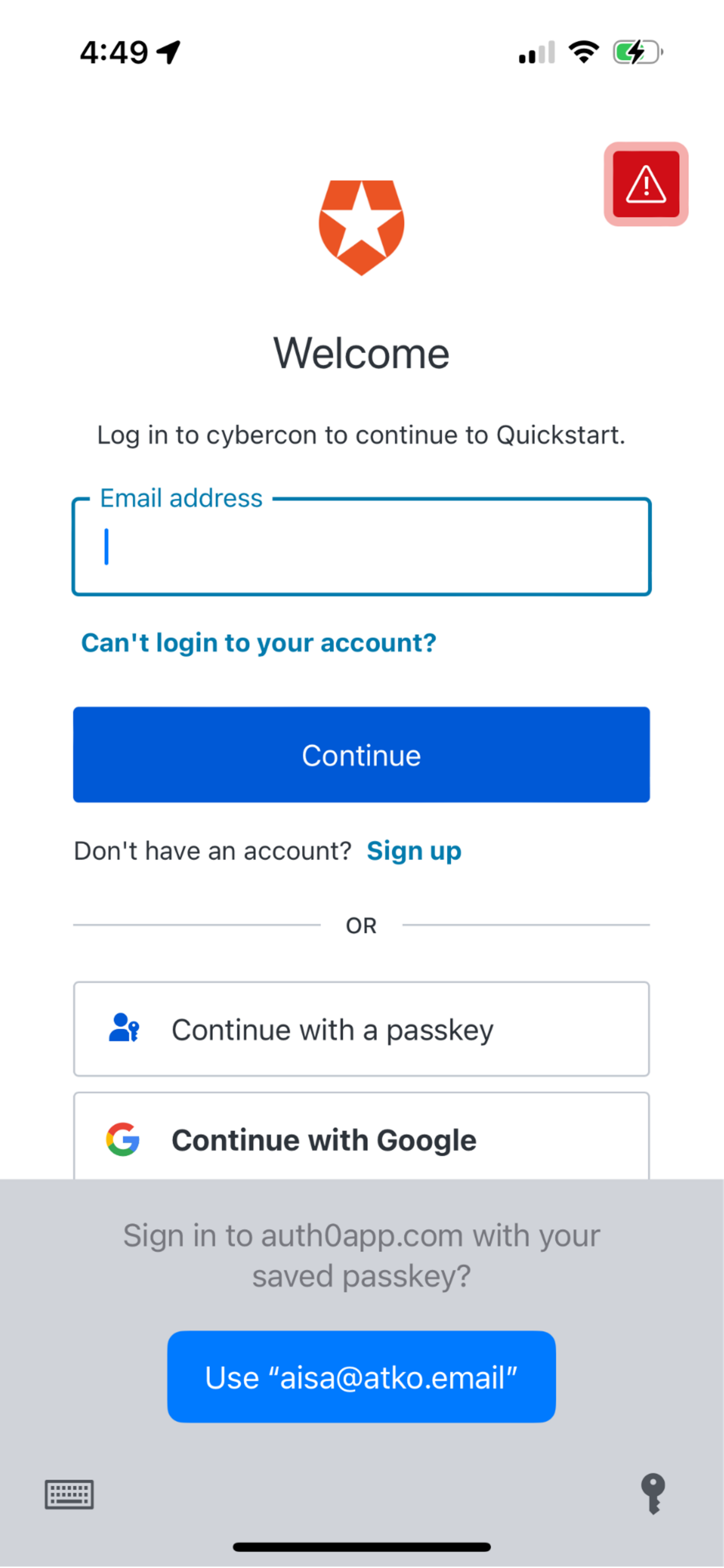
cybercon demo settings

version = 2.0.0
customDomain =
templateURL =

Source Code

The implementation for this application can be downloaded below for you to use as the basis for your own custom demos.

Download as a zip



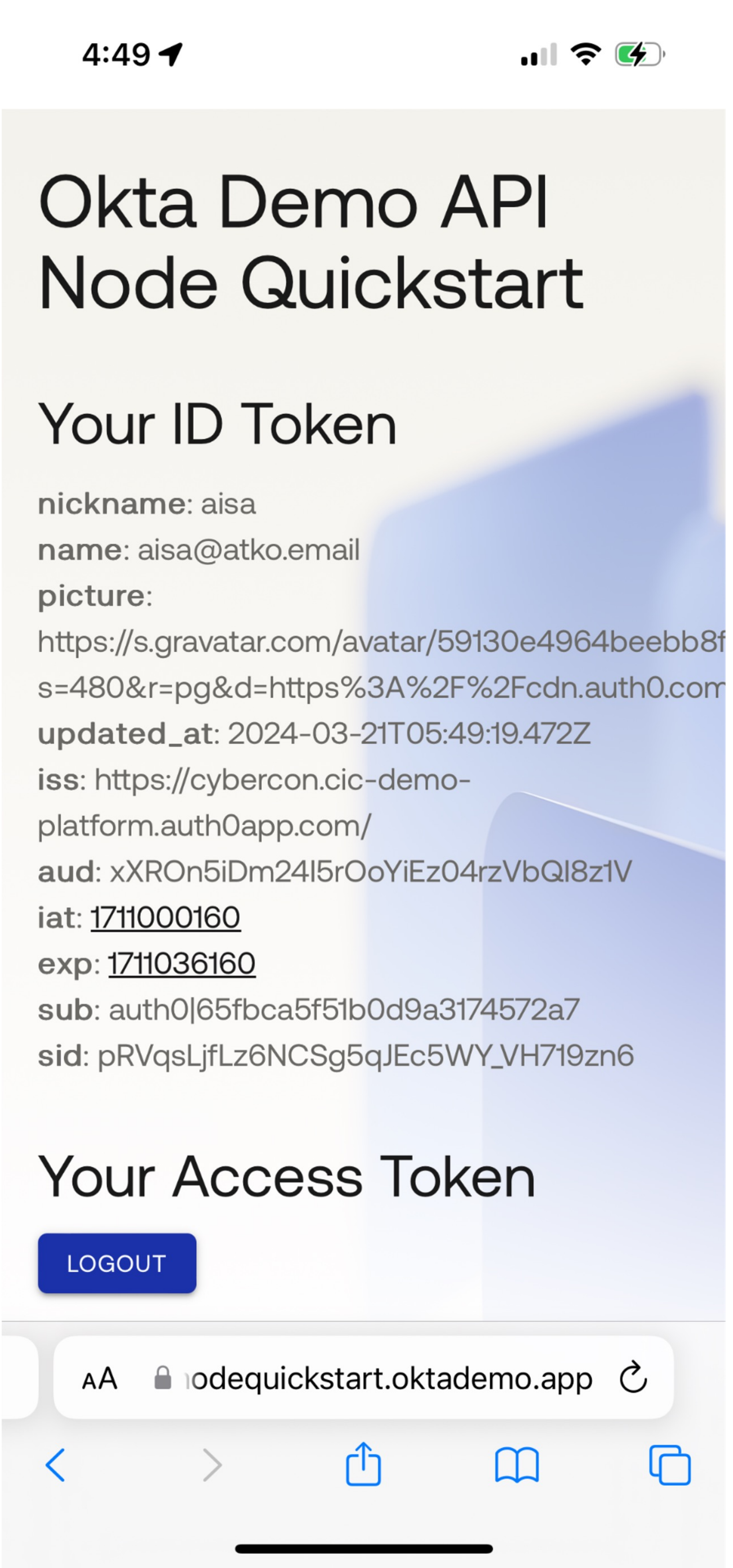
Welcome

Log in to cybercon to continue to Quickstart.

Email address

Don't have an account? Sign up

Sign in to auth0app.com with your saved passkey?



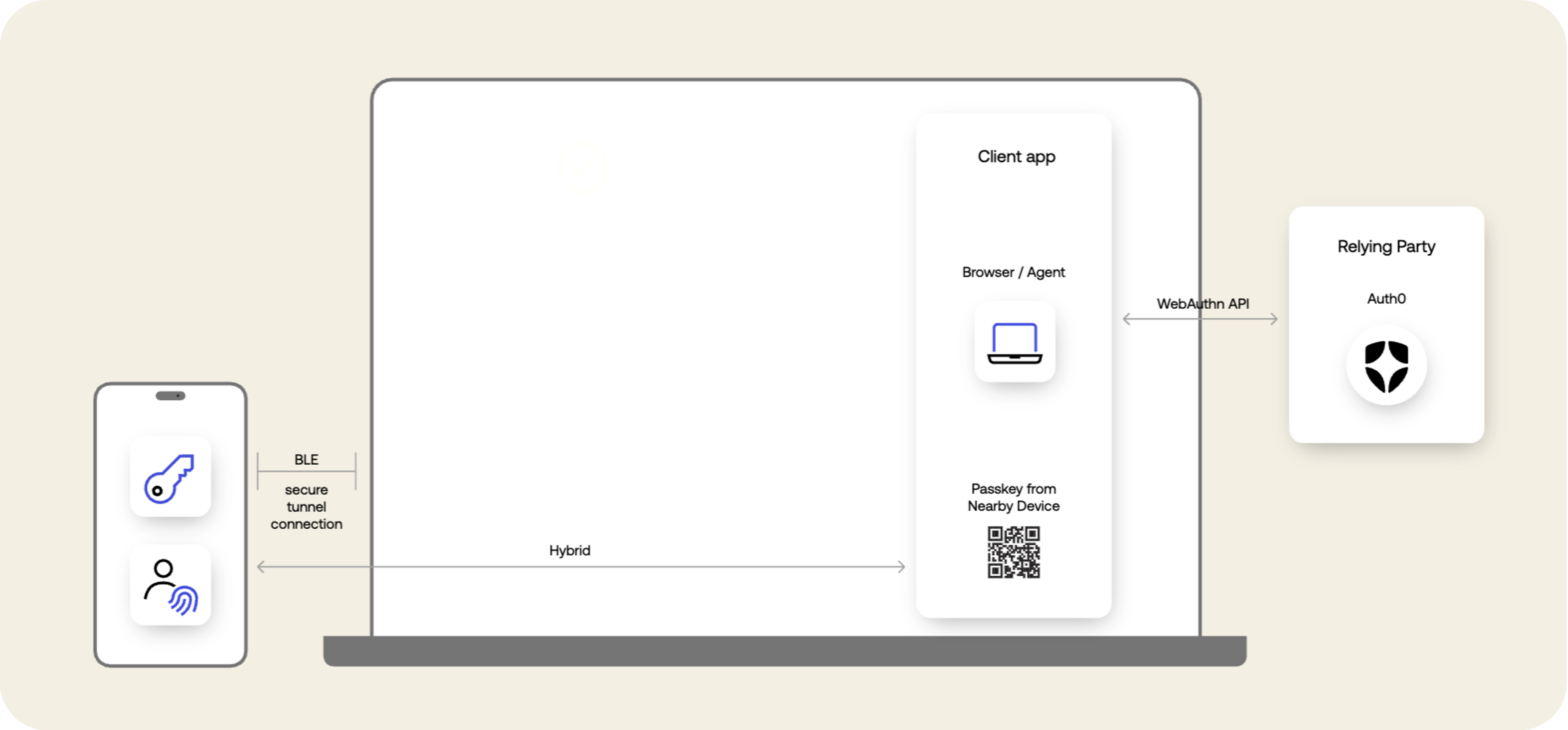
Okta Demo API Node Quickstart

Your ID Token

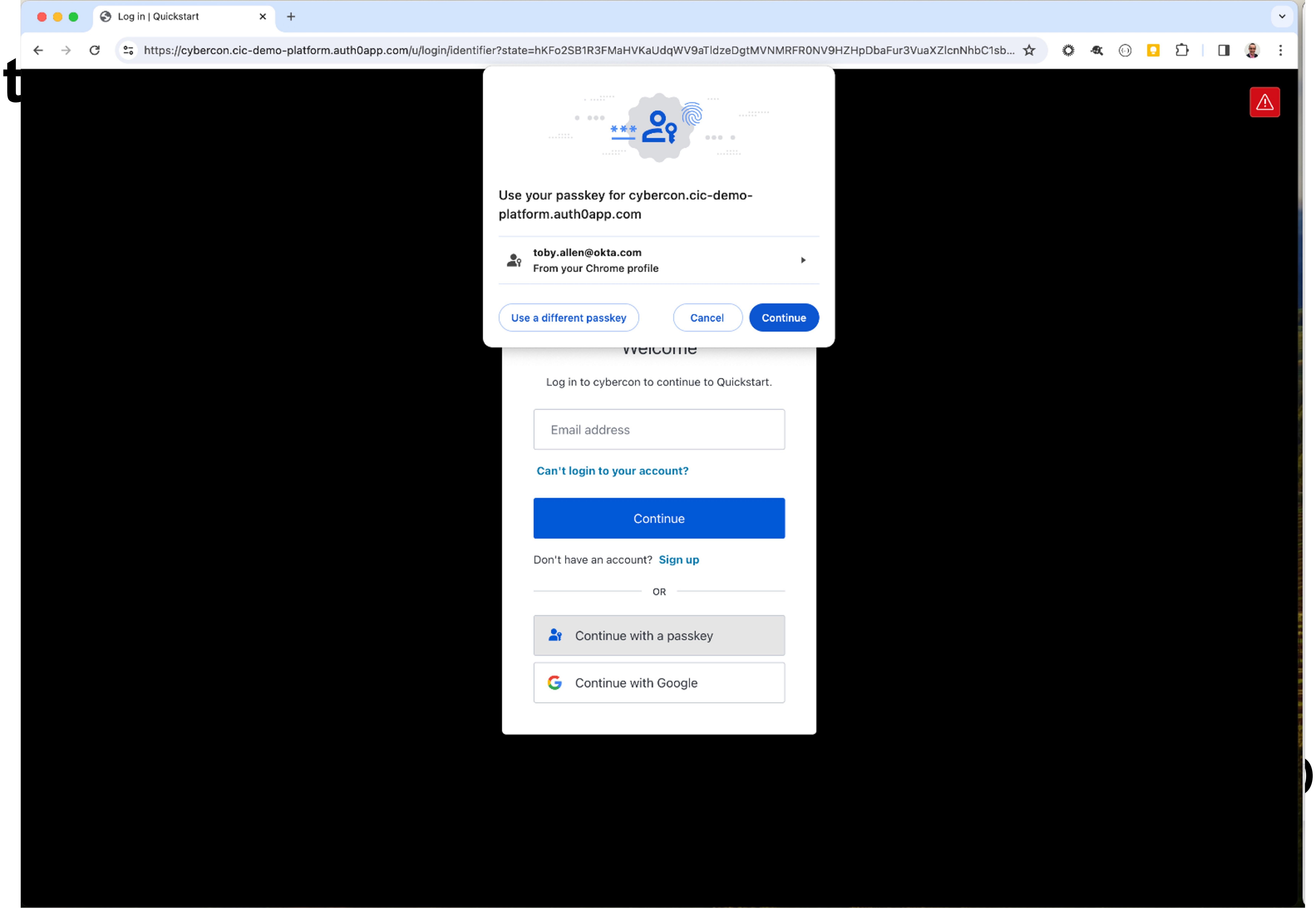
nickname: aisa
name: aisa@atko.email
picture:
https://s.gravatar.com/avatar/59130e4964beebb8f
s=480&r=pg&d=https%3A%2F%2Fcdn.auth0.com
updated_at: 2024-03-21T05:49:19.472Z
iss: https://cybercon.cic-demo-platform.auth0app.com/
aud: xXROn5iDm24I5rOoYiEz04rzVbQI8z1V
iat: 1711000160
exp: 1711036160
sub: auth0|65fbca5f51b0d9a3174572a7
sid: pRVqsLjfLz6NCSg5qJEc5WY_VH719zn6

Your Access Token

Cross Device Authentication



Int



https://cybercon.cic-demo-platform.auth0app.com/u/login/identifier?state=hKFo2SB1R3FMaHVKaUdqWV9aTldzeDgtMVNMRFR0NV9HZHpDbaFur3VuaXZlcnNhbC1sb...

Use your passkey for cybercon.cic-demo-platform.auth0app.com

toby.allen@okta.com
From your Chrome profile

Welcome

Log in to cybercon to continue to Quickstart.

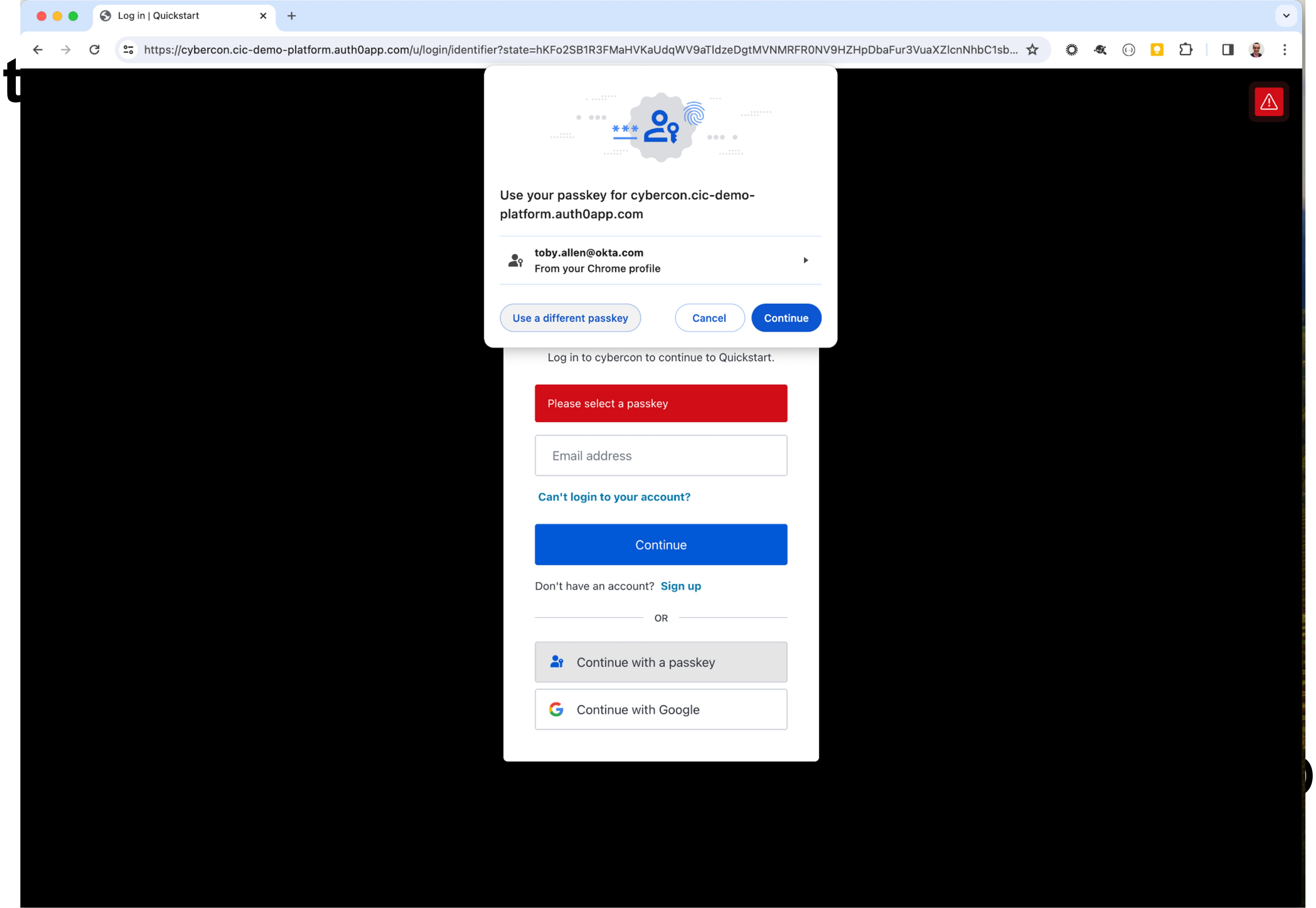
Email address

Can't login to your account?

Don't have an account? Sign up

OR

Int



Log in | Quickstart

https://cybercon.cic-demo-platform.auth0app.com/u/login/identifier?state=hKFo2SB1R3FMaHVKaUdqWV9aTldzeDgtMVNMRFR0NV9HZHpDbaFur3VuaXZlcnNhbC1sb...

Use your passkey for cybercon.cic-demo-platform.auth0app.com

toby.allen@okta.com
From your Chrome profile

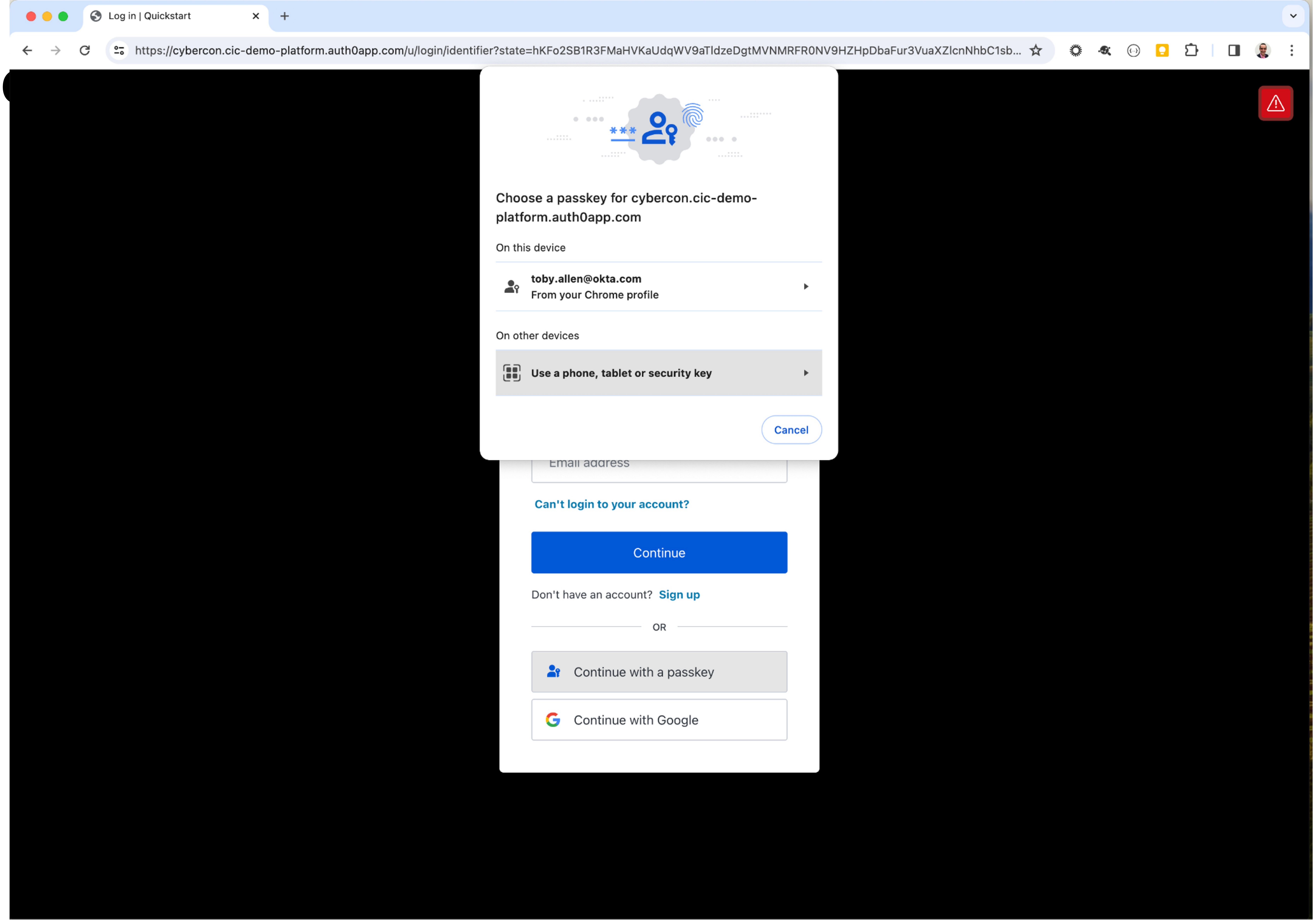
Log in to cybercon to continue to Quickstart.

Please select a passkey

Email address

Don't have an account? Sign up

Int



Log in | Quickstart

https://cybercon.cic-demo-platform.auth0app.com/u/login/identifier?state=hKFo2SB1R3FMaHVKaUdqWV9aTldzeDgtMVNMRFR0NV9HZHpDbaFur3VuaXZlcnNhbC1sb...

Choose a passkey for cybercon.cic-demo-platform.auth0app.com

On this device

toby.allen@okta.com
From your Chrome profile

On other devices

Use a phone, tablet or security key

Cancel

Email address

Can't login to your account?

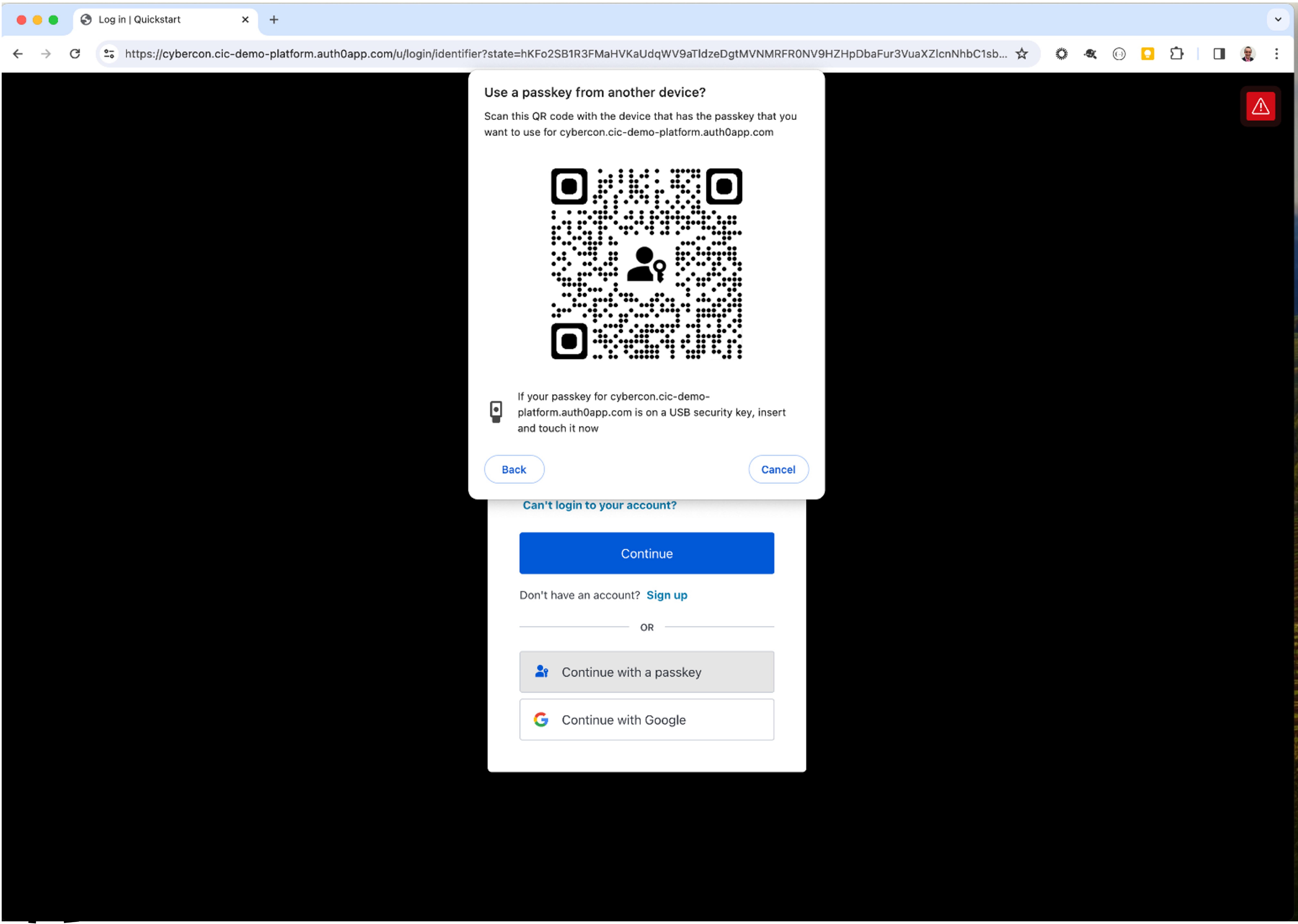
Continue

Don't have an account? **Sign up**

OR

Continue with a passkey

Continue with Google



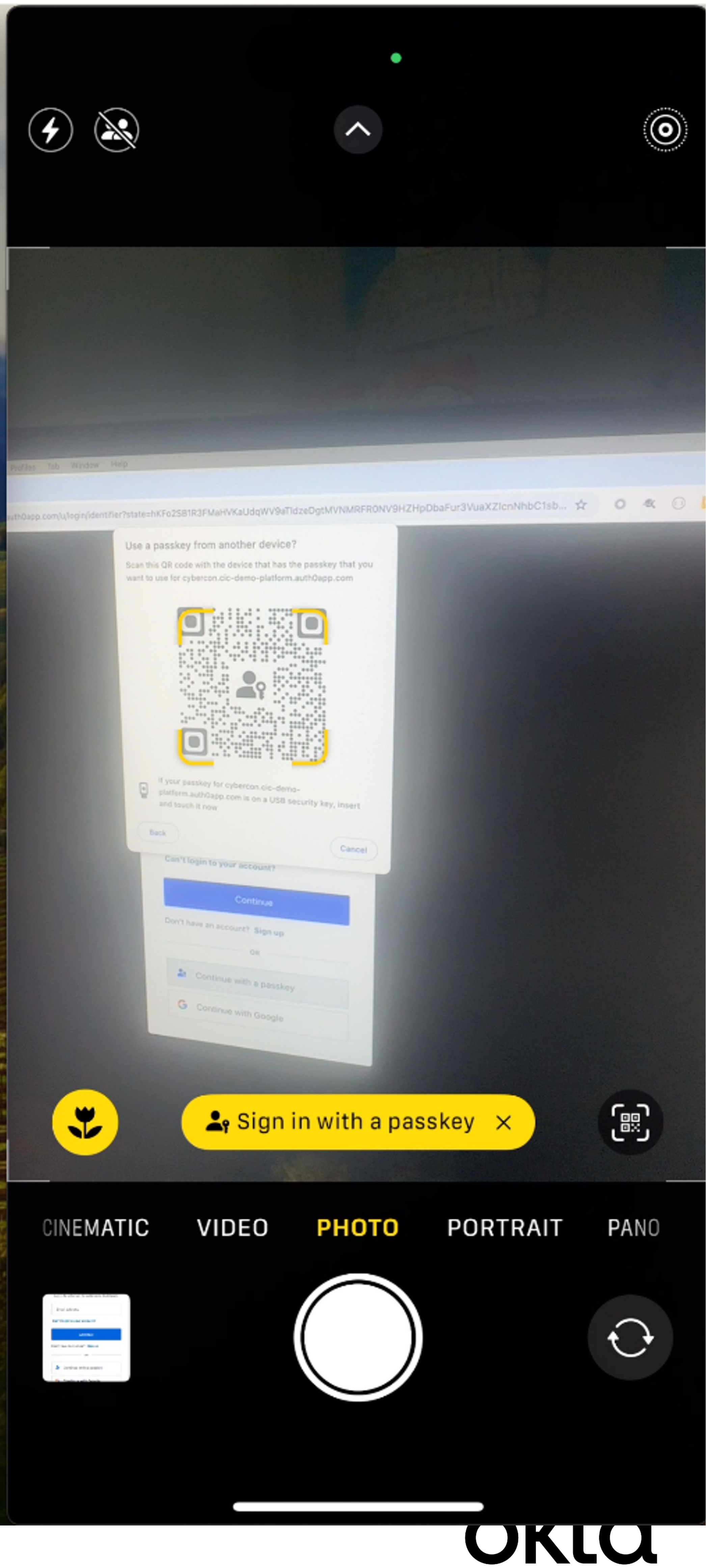
Log in | Quickstart

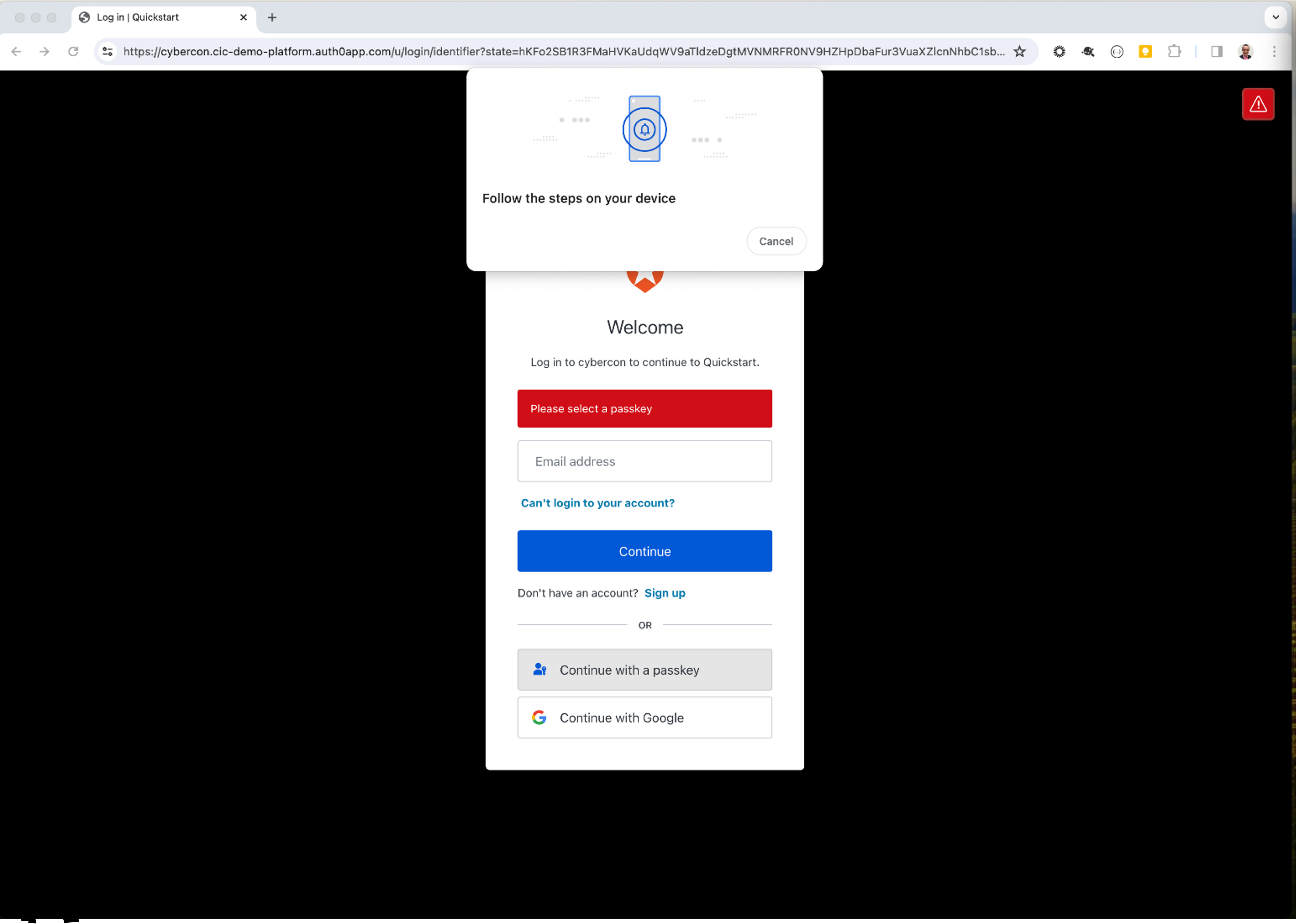
https://cybercon.cic-demo-platform.auth0app.com/u/login/identifier?state=hKFo2SB1R3FMaHVKaUdqWV9aTldzeDgtMVNMRFR0NV9HZHpDbaFur3VuaXZlcnNhbC1sb...

Use a passkey from another device?

Scan this QR code with the device that has the passkey that you want to use for cybercon.cic-demo-platform.auth0app.com

If your passkey for cybercon.cic-demo-platform.auth0app.com is on a USB security key, insert and touch it now





Log in | Quickstart

https://cybercon.cic-demo-platform.auth0app.com/u/login/identifier?state=hKFo2SB1R3FMaHVKaUdqWV9aTldzeDgtMVNMRFR0NV9HZHpDbaFur3VuaXZlcnNhbC1sb...

Follow the steps on your device

Cancel

Welcome

Log in to cybercon to continue to Quickstart.

Please select a passkey

Email address

Can't login to your account?

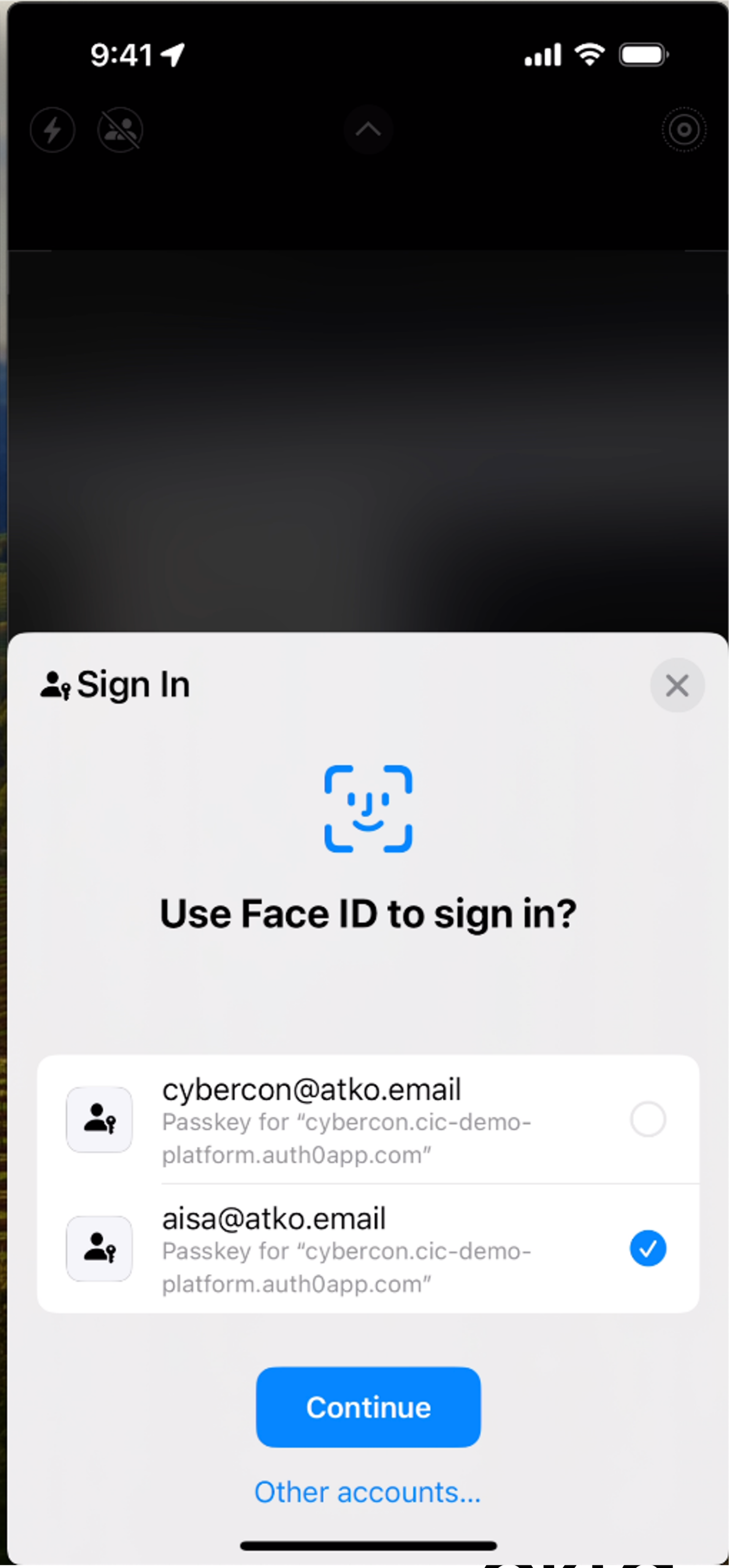
Continue

Don't have an account? Sign up

OR

Continue with a passkey

Continue with Google



9:41

Sign In

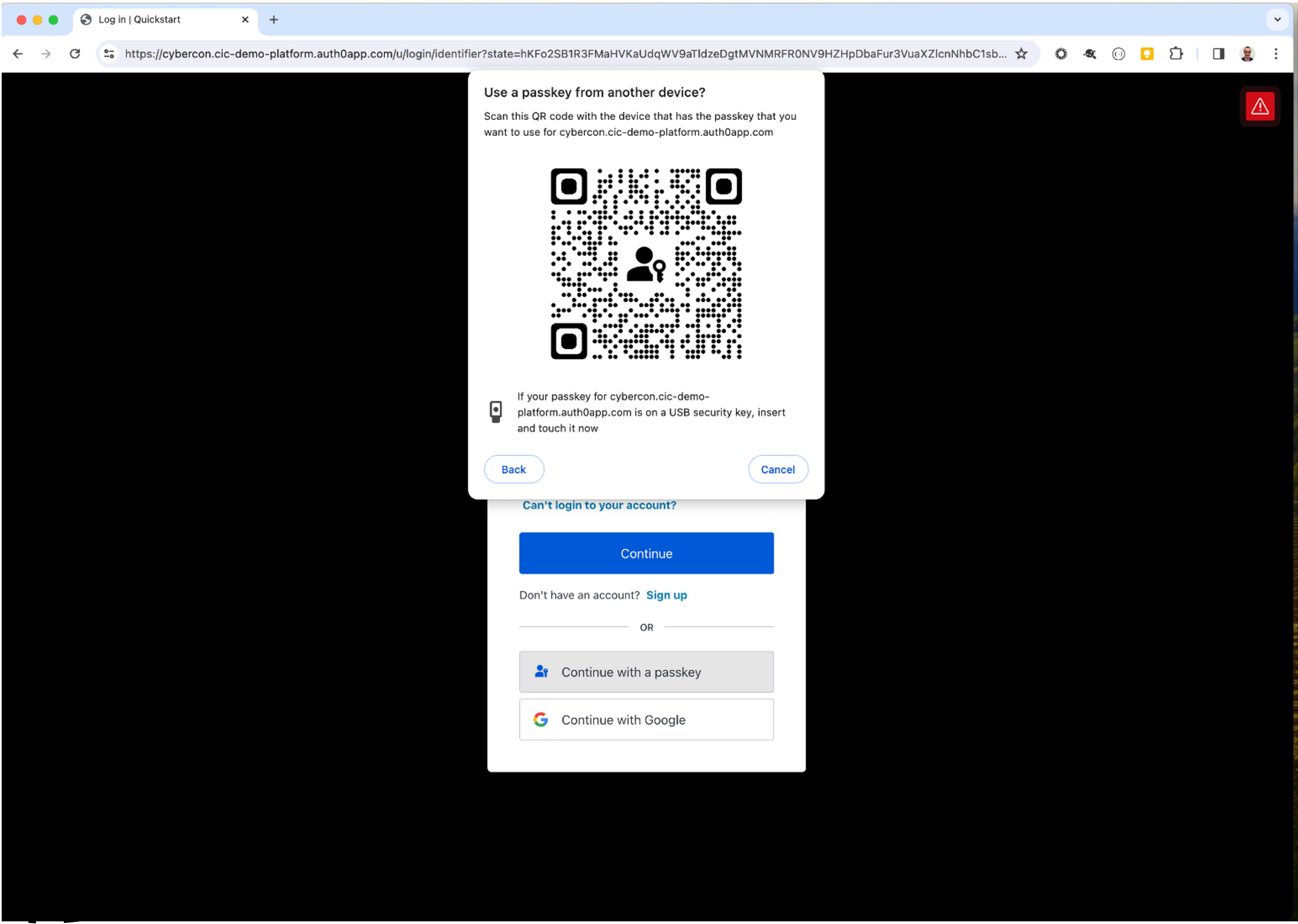
Use Face ID to sign in?

○ cybercon@atko.email
Passkey for "cybercon.cic-demo-platform.auth0app.com"

✓ aisa@atko.email
Passkey for "cybercon.cic-demo-platform.auth0app.com"

Continue

Other accounts...



Log in | Quickstart

https://cybercon.cic-demo-platform.auth0app.com/u/login/identifier?state=hKFo2SB1R3FMaHVKaUdqWV9aTldzeDgtMVNMRFR0NV9HZHpDbaFur3VuaXZlcnNhbC1sb...

Use a passkey from another device?

Scan this QR code with the device that has the passkey that you want to use for cybercon.cic-demo-platform.auth0app.com

If your passkey for cybercon.cic-demo-platform.auth0app.com is on a USB security key, insert and touch it now

Back

Cancel

Can't login to your account?

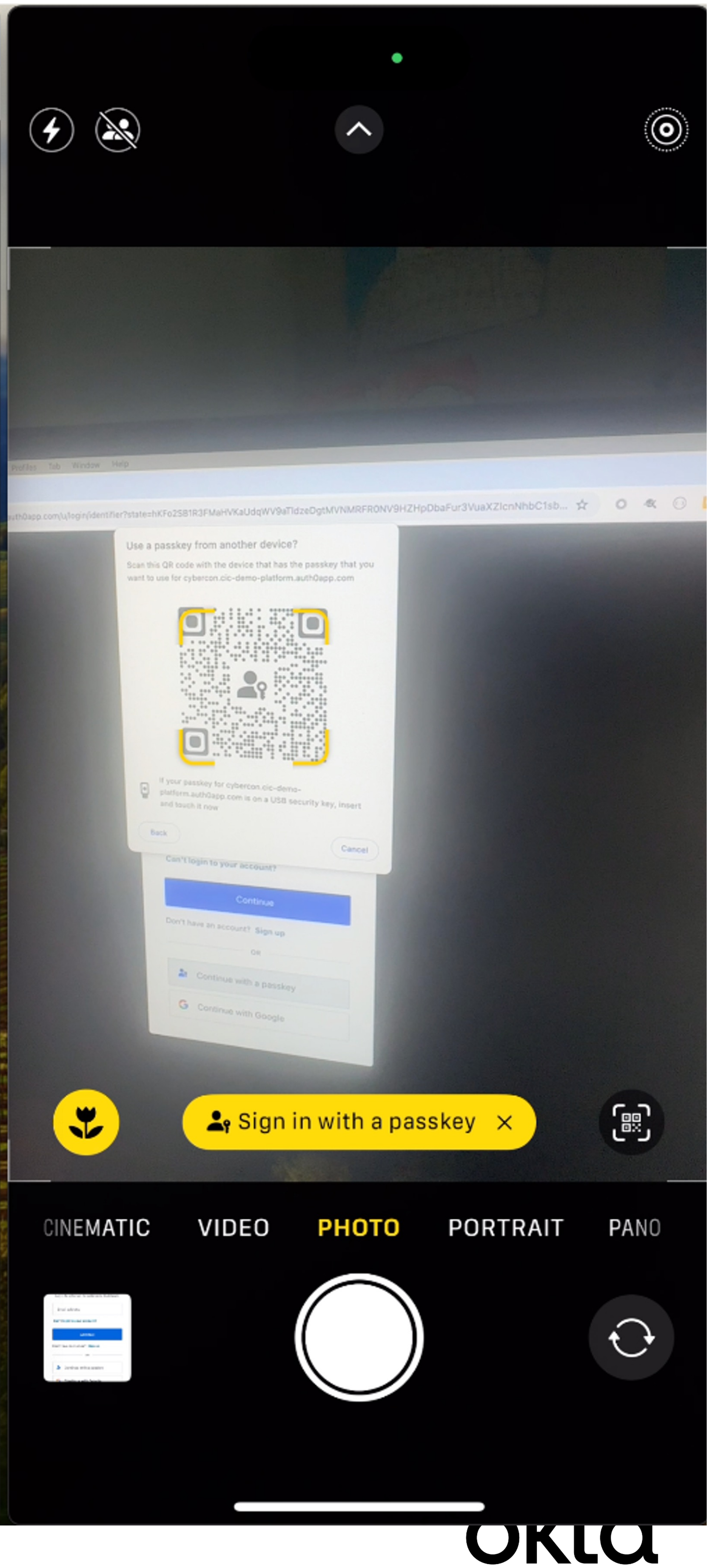
Continue

Don't have an account? Sign up

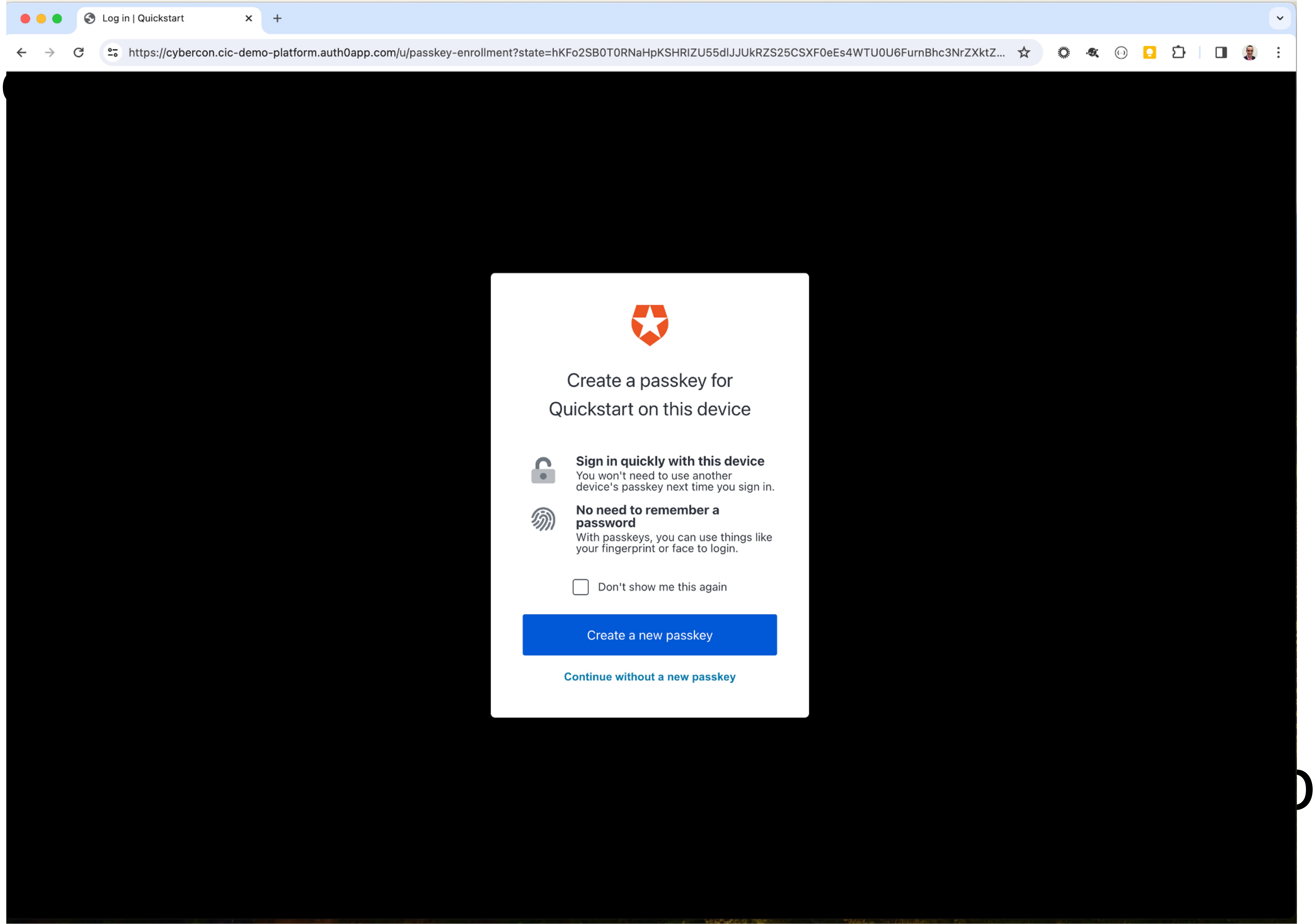
OR

Continue with a passkey

Continue with Google



Int



Log in | Quickstart

https://cybercon.cic-demo-platform.auth0app.com/u/passkey-enrollment?state=hKFo2SB0T0RNaHpKSHRIZU55dlJJUkRZS25CSXF0eEs4WTU0U6FurnBhc3NrZXktZ...

Create a passkey for Quickstart on this device

Sign in quickly with this device
You won't need to use another device's passkey next time you sign in.

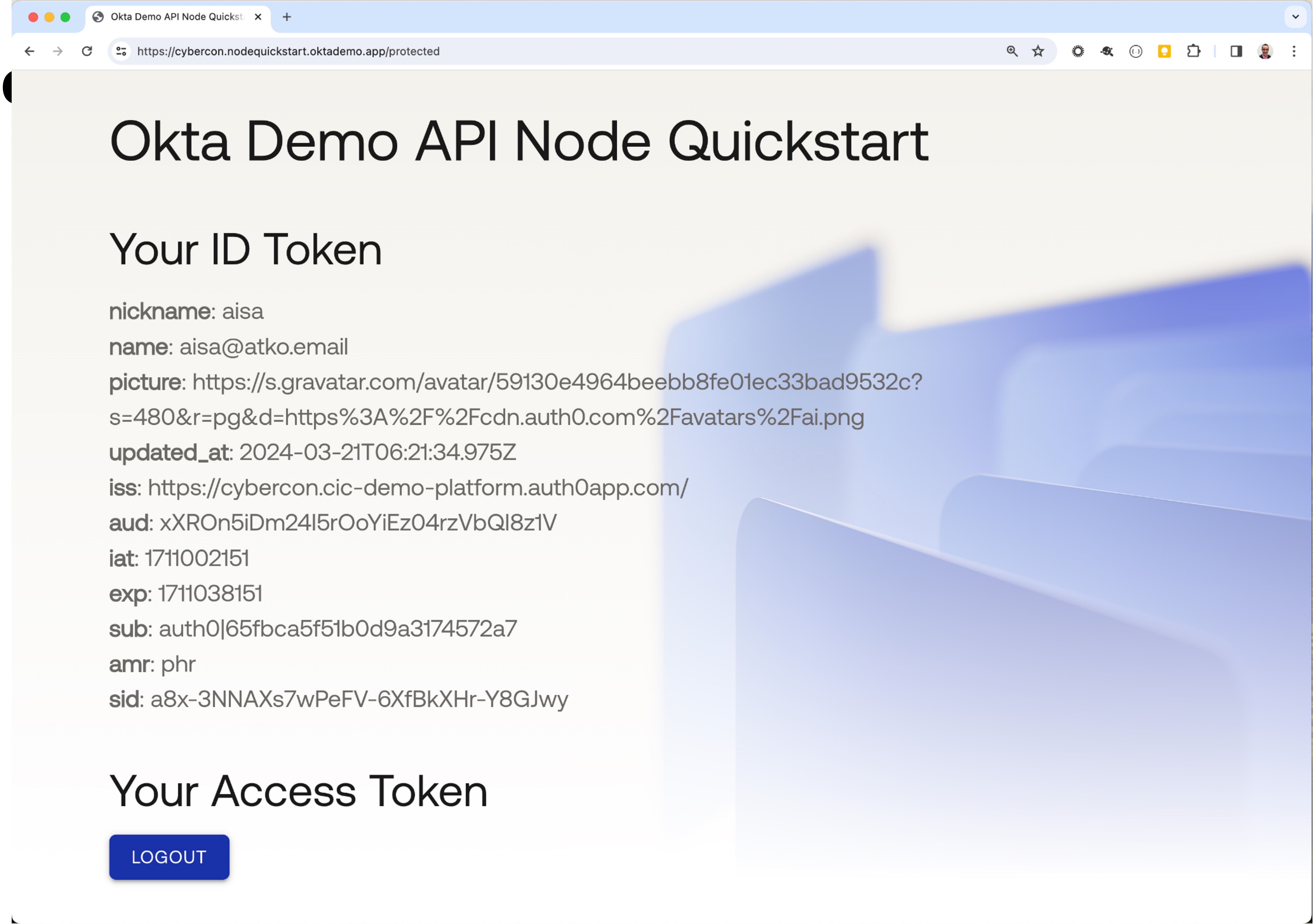
No need to remember a password
With passkeys, you can use things like your fingerprint or face to login.

□ Don't show me this again

Create a new passkey

Continue without a new passkey

Int


Okta Demo API Node Quickst
https://cybercon.nodequickstart.oktademo.app/protected

Okta Demo API Node Quickstart

Your ID Token

nickname: aisa

name: aisa@atko.email

picture: https://s.gravatar.com/avatar/59130e4964beebb8fe01ec33bad9532c?s=480&r=pg&d=https%3A%2F%2Fcdn.auth0.com%2Favatars%2Fai.png

updated_at: 2024-03-21T06:21:34.975Z

iss: https://cybercon.cic-demo-platform.auth0app.com/

aud: xXROn5iDm24I5rOoYiEz04rzVbQI8z1V

iat: 1711002151

exp: 1711038151

sub: auth0|65fbca5f51b0d9a3174572a7

amr: phr

sid: a8x-3NNAXs7wPeFV-6XfBkXHr-Y8GJwy

Your Access Token

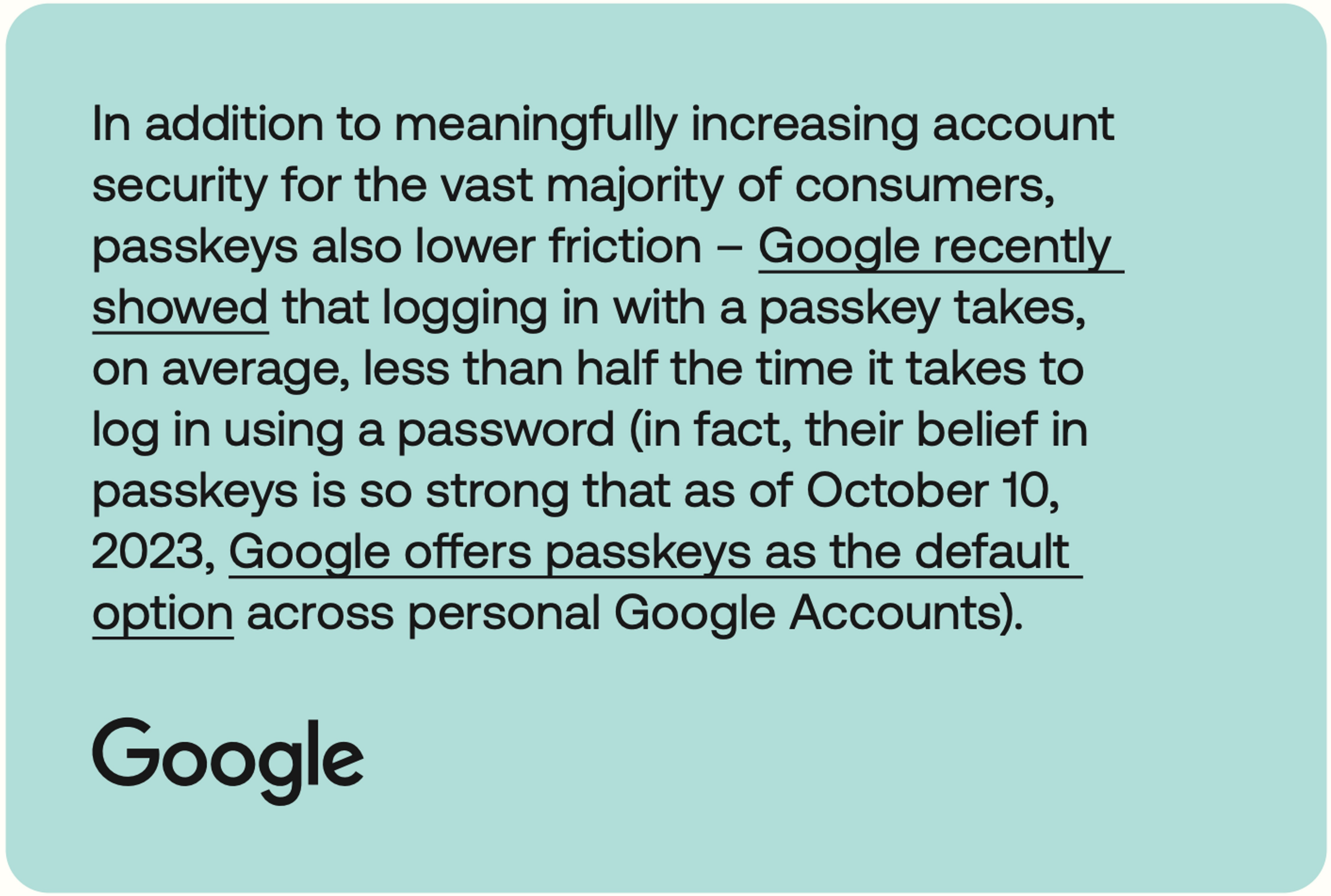
Cross Device Authentication

Allows a passkey on an Android or iOS device to be leveraged for signin on another device or desktop.
Leverages WebAuthN API and BLE for proximity.

- User opens web app and is offered option to authenticate with nearby device.
- Web app displays QR Code
- A Bluetooth Low Energy (BLE) advertisement is used to verify proximity
- Websocket is established between devices and a cryptographic handshake is completed.
- Device 2 completes sign-in with passkey

- *Best Practice is the application now offers to create a new passkey on initiating device.*

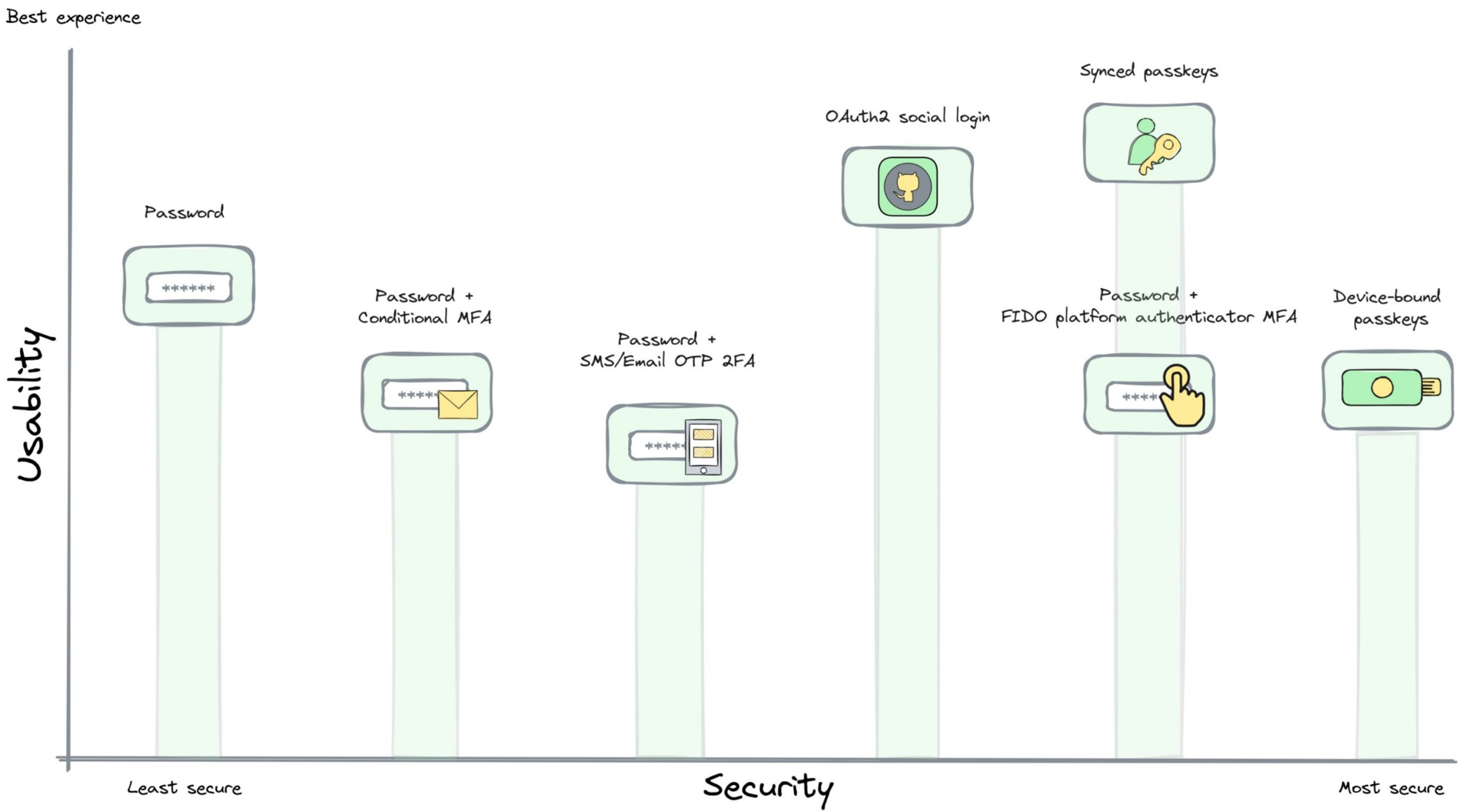
So… What does this mean for customers?



In addition to meaningfully increasing account security for the vast majority of consumers, passkeys also lower friction – Google recently showed that logging in with a passkey takes, on average, less than half the time it takes to log in using a password (in fact, their belief in passkeys is so strong that as of October 10, 2023, Google offers passkeys as the default option across personal Google Accounts).

Google

https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html


Best experience
Usability
Password
******
Password +
Conditional MFA
*****
Password +
SMS/Email OTP 2FA
*****
OAuth2 social login
Synced passkeys
Password +
FIDO platform authenticator MFA
****
Device-bound
passkeys
Least secure
Security
Most secure

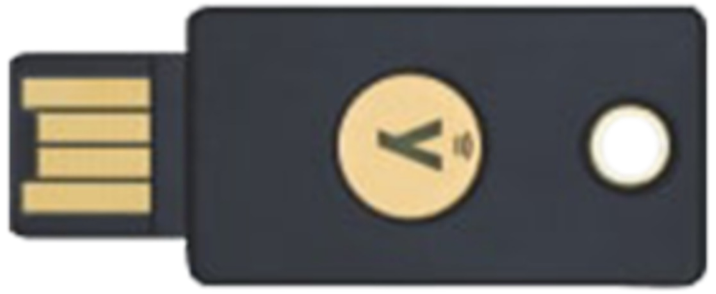
Unfortunately…

there are some rough edges

Device Support

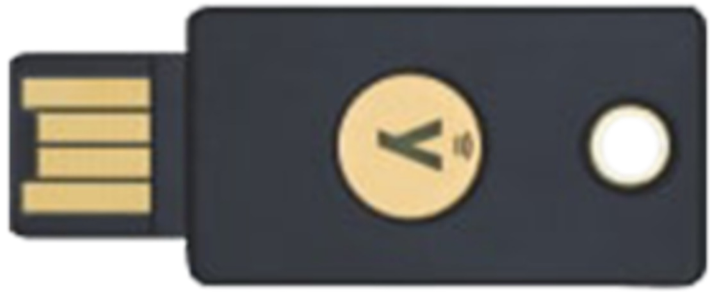
- Who is your customer base?

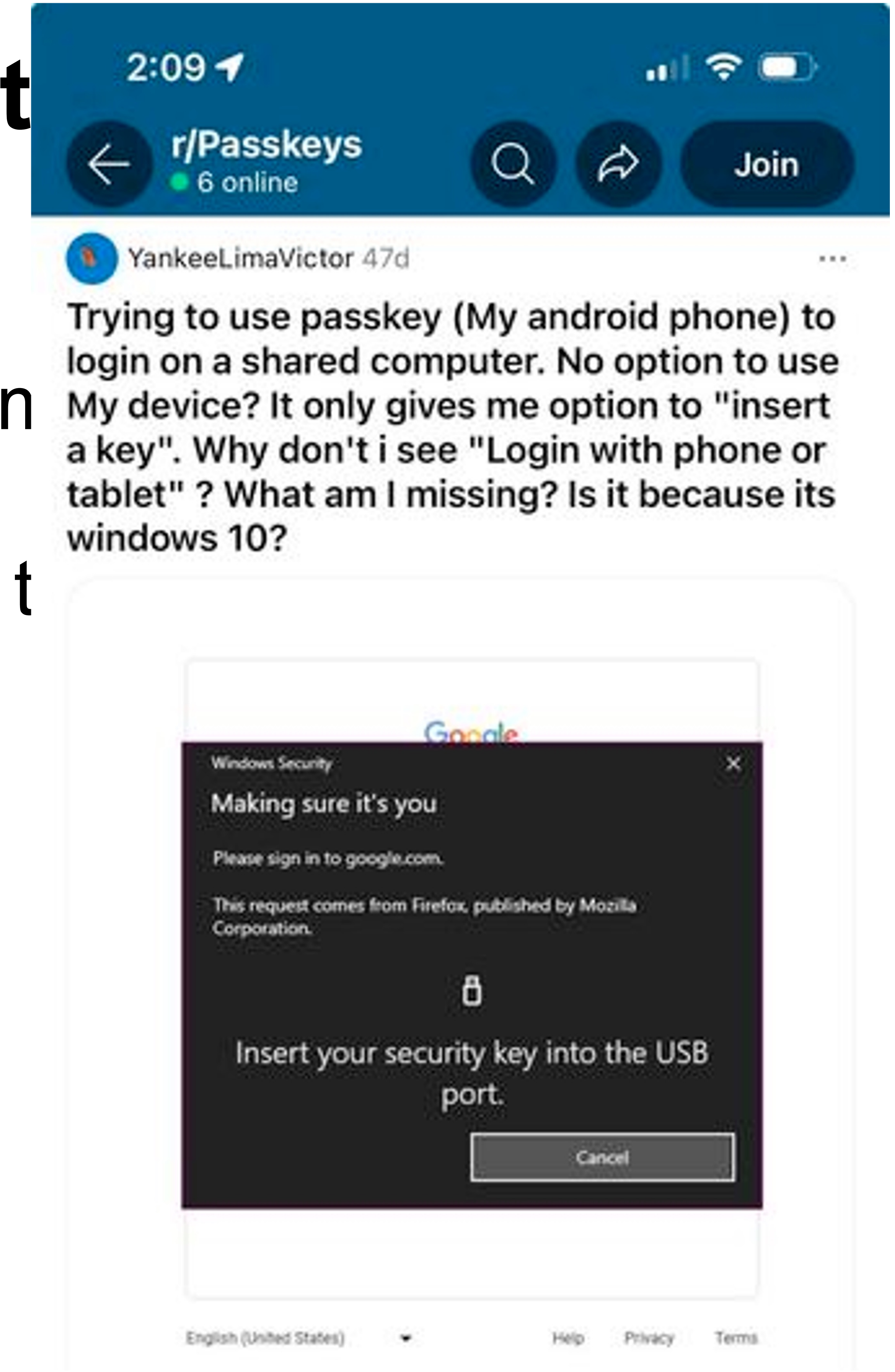
- What devices can they access?



Device Support

- Who is your custon
- What devices can t





YankeeLimaVictor 47d

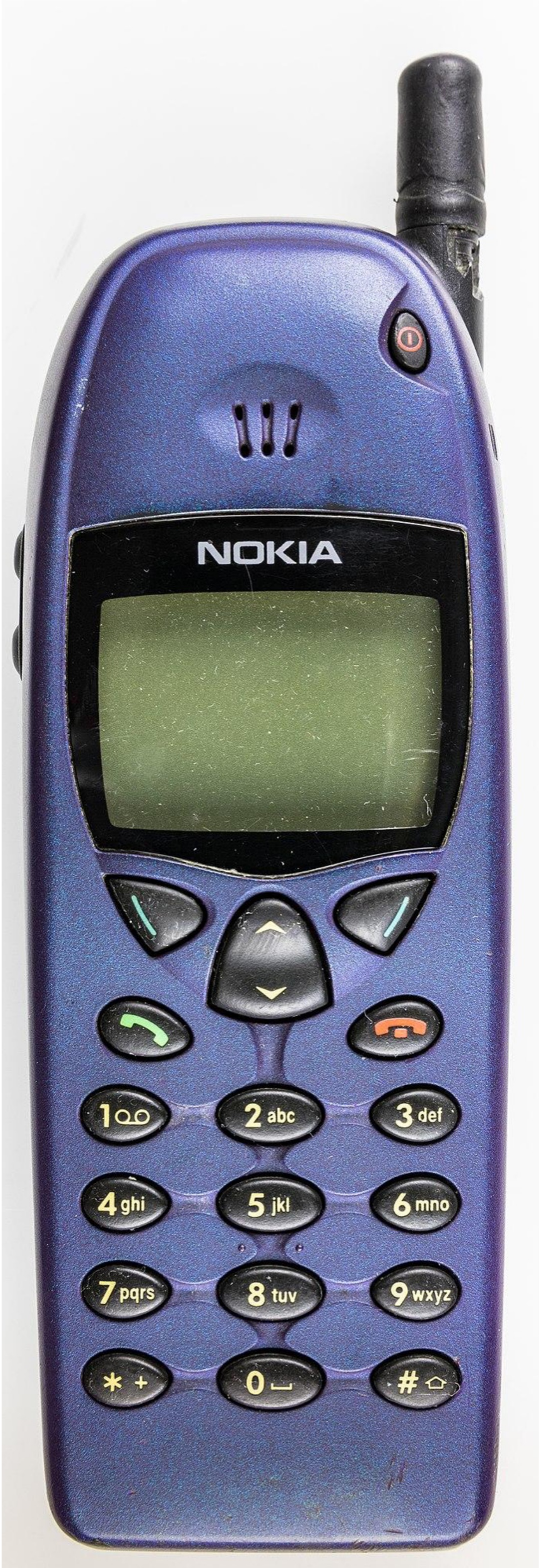
Trying to use passkey (My android phone) to login on a shared computer. No option to use My device? It only gives me option to "insert a key". Why don't i see "Login with phone or tablet" ? What am I missing? Is it because its windows 10?

Making sure it's you

Please sign in to google.com.

This request comes from Firefox, published by Mozilla Corporation.

Insert your security key into the USB port.



~~Device Support~~
Use Case & Access Mode Support

- Where are they accessing it from?

- What devices can they access?

Migration, Reset & Recovery

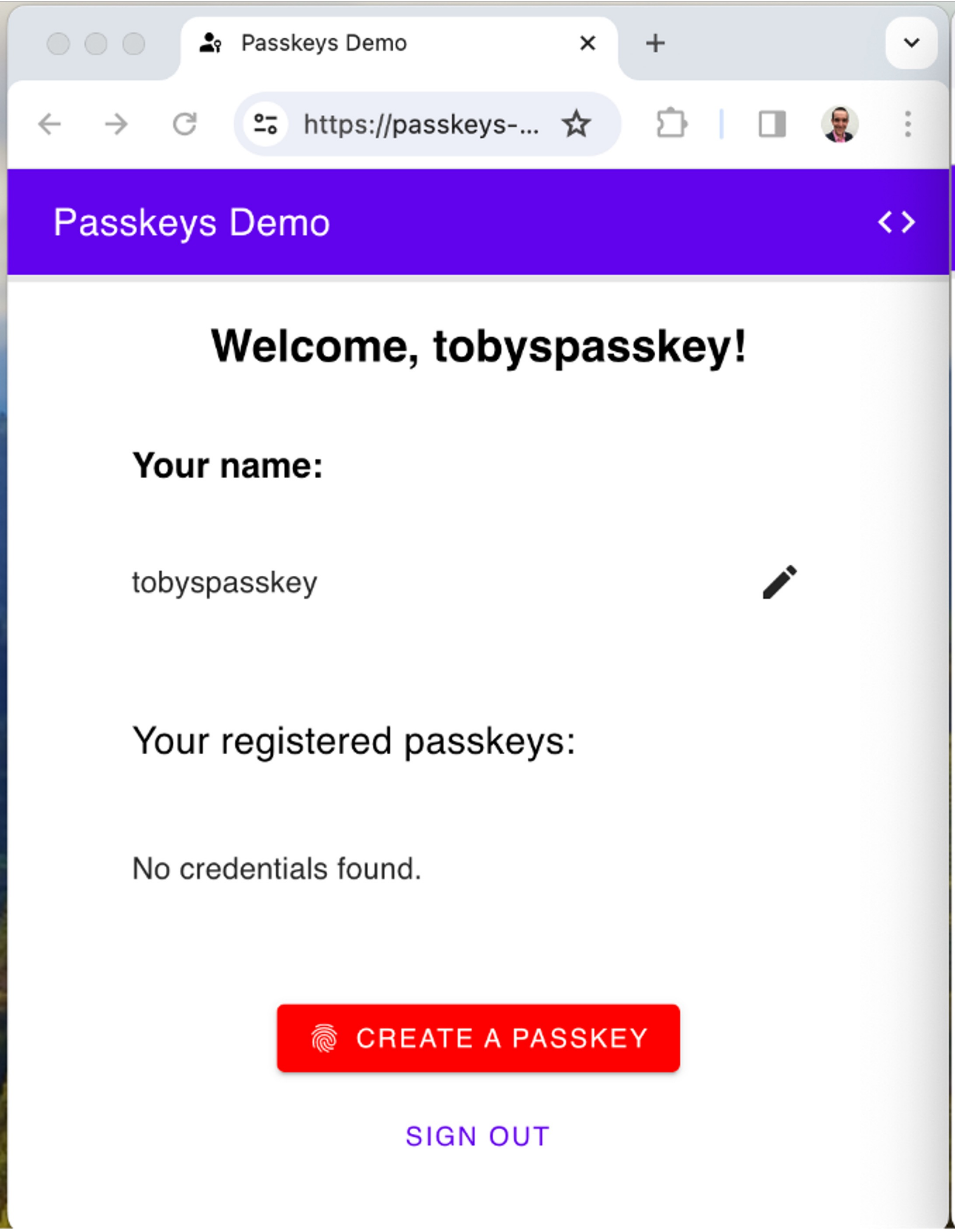
- Recovery processes for specific passkeys fallback to platform/storage solution

- Account Recovery Processes means you still need to validate other authenticators/information

- Encourage registration of multiple authenticators but solve for single device users

- Offer clean migration paths to users, test them

Challenges



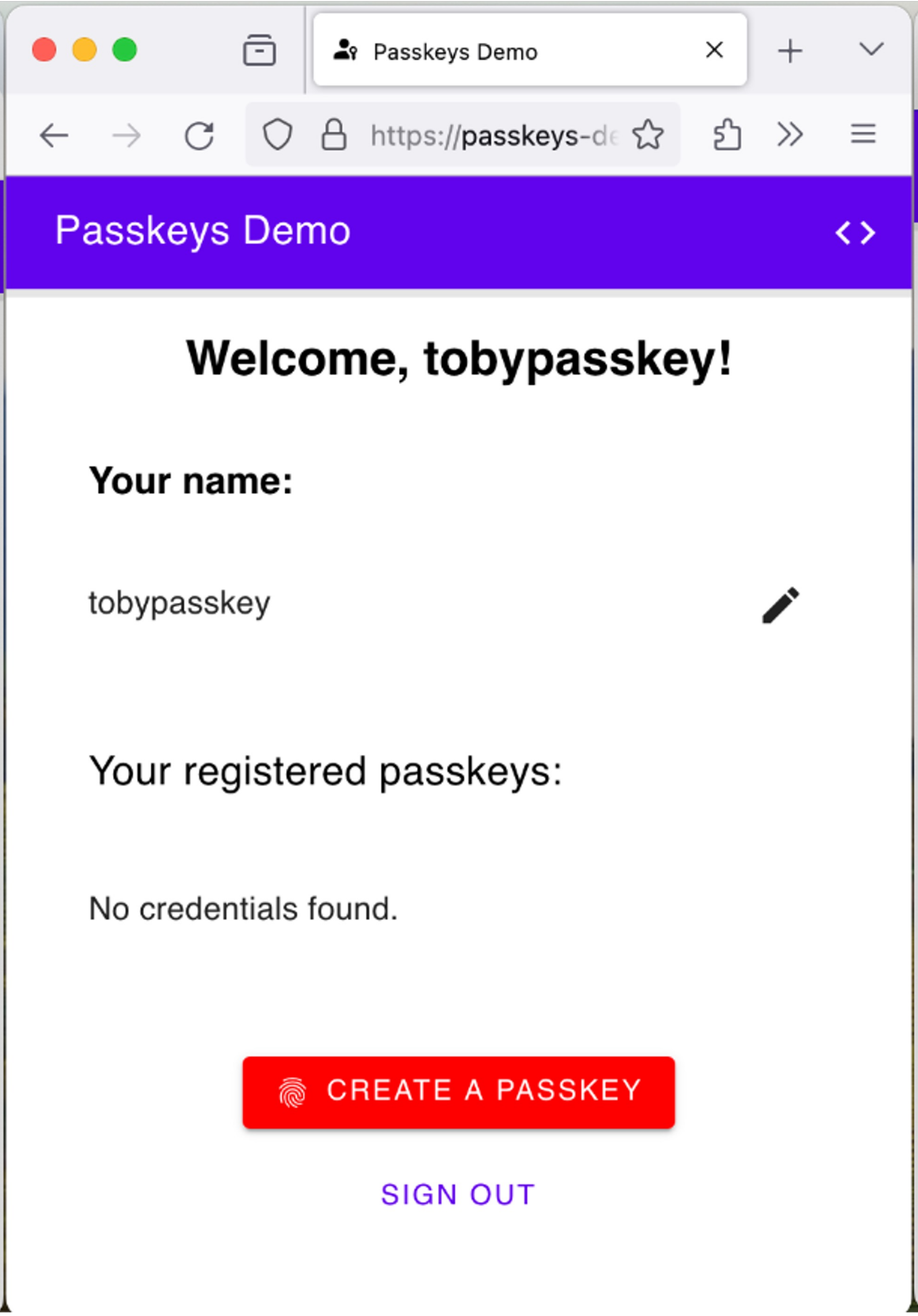
Welcome, tobyspasskey!

Your name:

tobyspasskey

Your registered passkeys:

No credentials found.



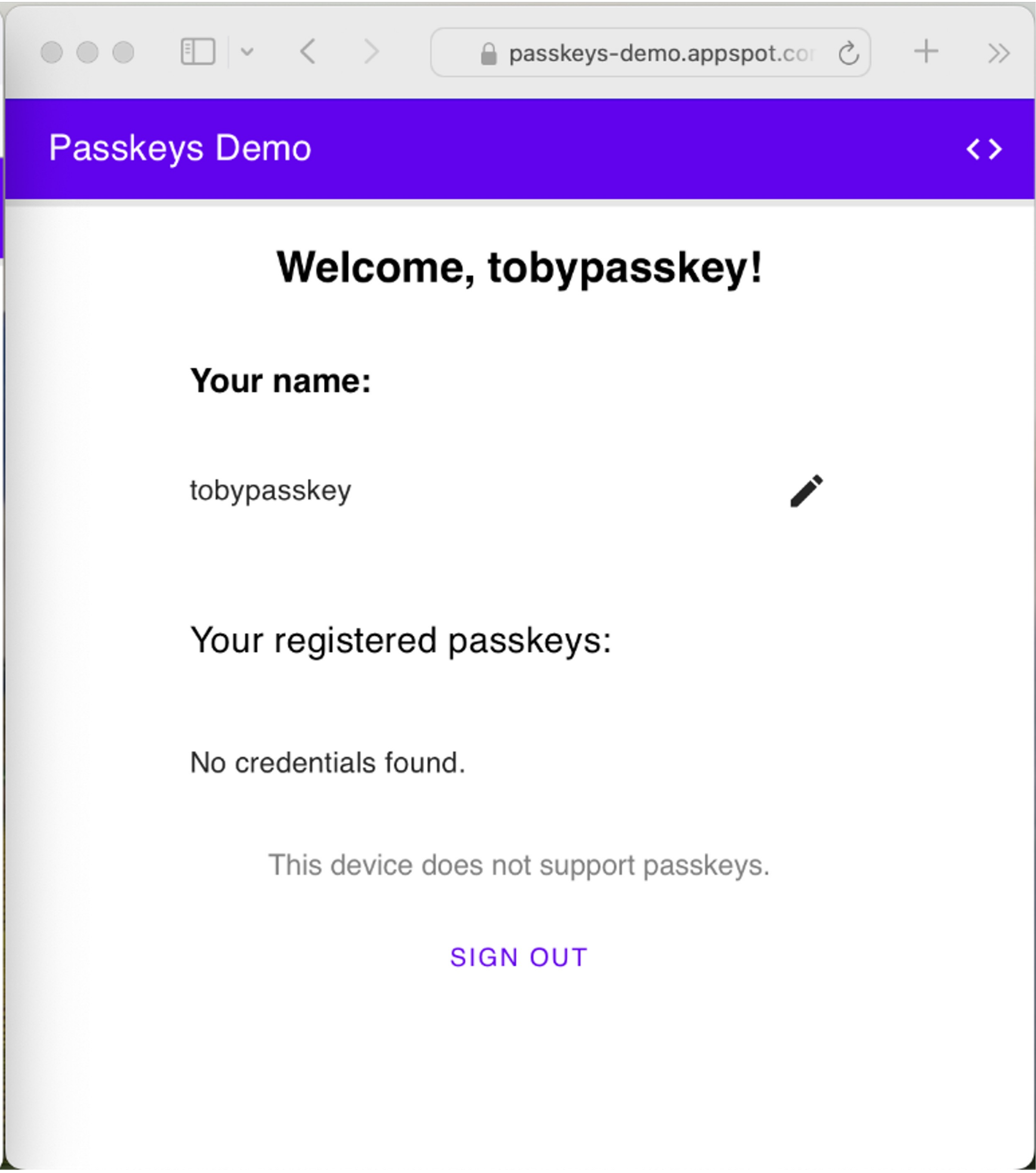
Welcome, tobypasskey!

Your name:

tobypasskey

Your registered passkeys:

No credentials found.



Welcome, tobypasskey!

Your name:

tobypasskey

Your registered passkeys:

No credentials found.

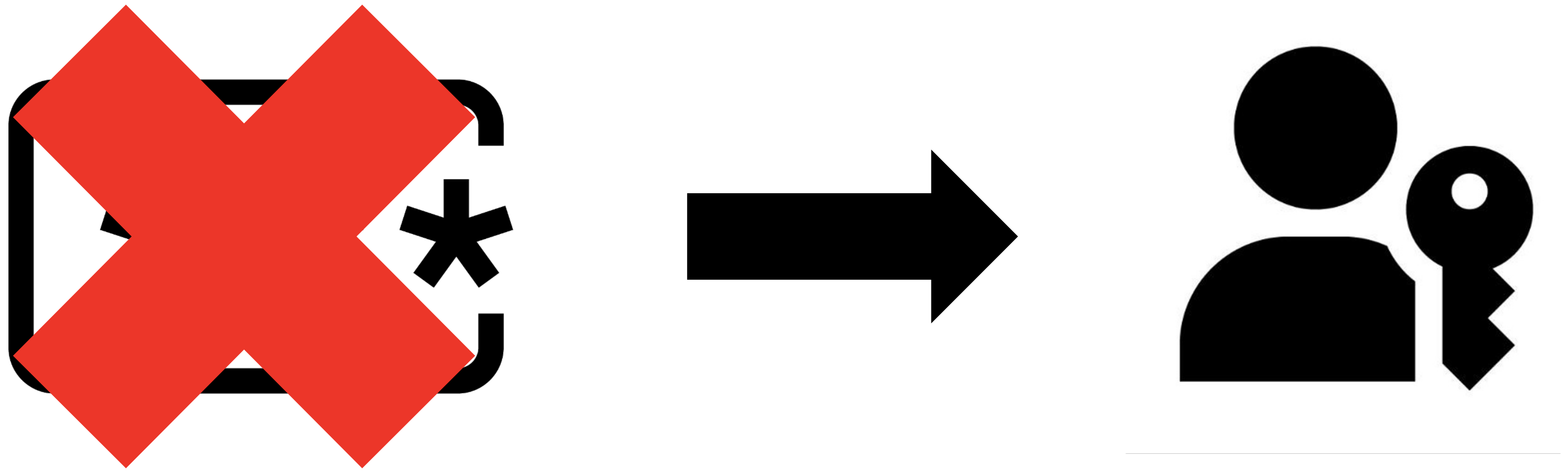
This device does not support passkeys.

Cross Ecosystem Challenges

- Offer Cross Device Authentication WITH follow up option to create another passkey

- Offer selfservice Passkey & Session Management options in your application.
  - Revoke a devices Session
  - Revoke a Passkey

Final Thoughts



Passkeys **WILL** replace passwords and it will happen quicker than we expect.

Learn More

learnpasskeys.io

Contact

Toby Allen

iamse.blog

@tobes@infosec.exchange

linkedin.com/in/tobyallen11

@tobyallen