



The state of passkey in 2025

Fabian Bader & Christopher Brumm
Cyber Security Architects @ **glueckkanja**



About us...



Fabian Bader

old
MVP
@fabian_bader
/in/fabianbader
cludbrothers.info

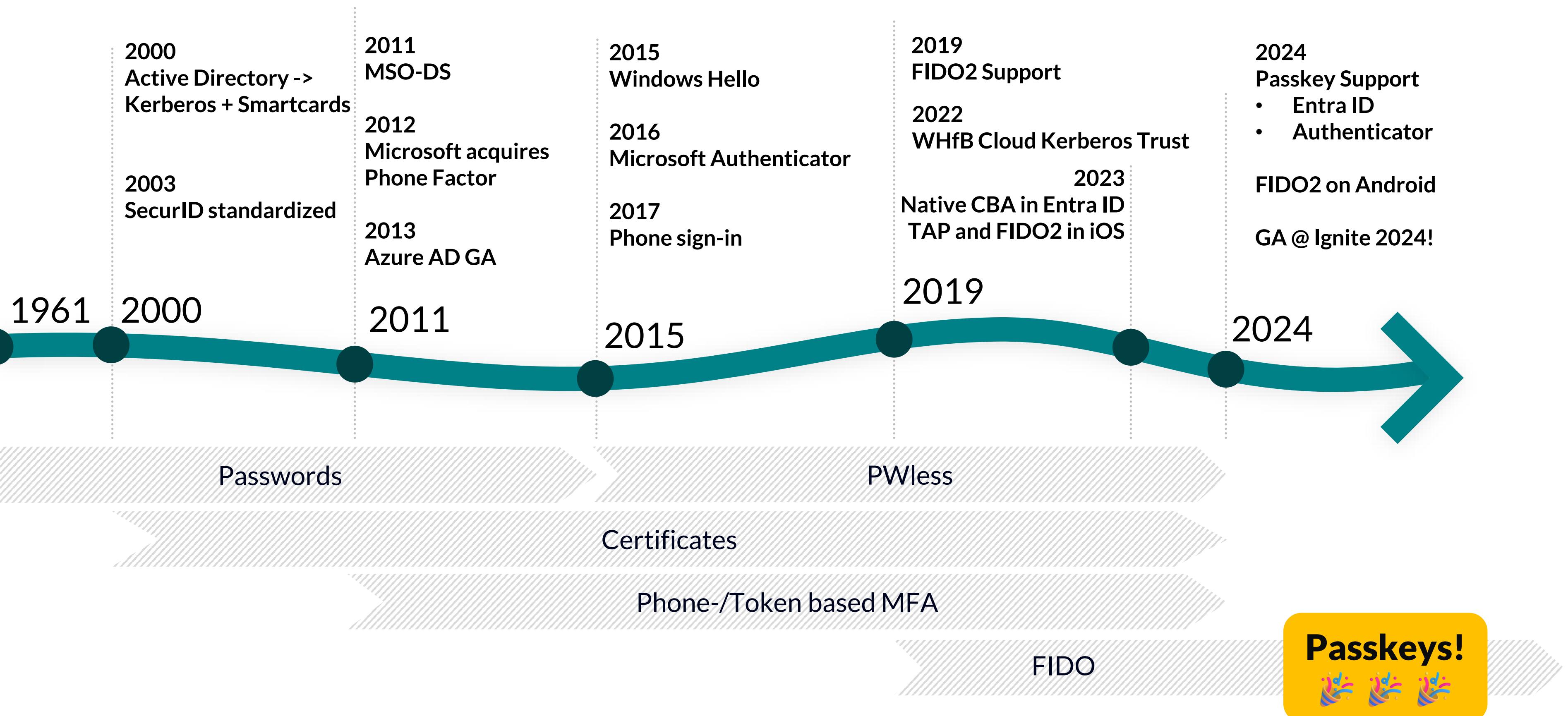
very old
CISSP (and now also MVP)
@cbrhh
/in/christopherbrumm
chris-brumm.com



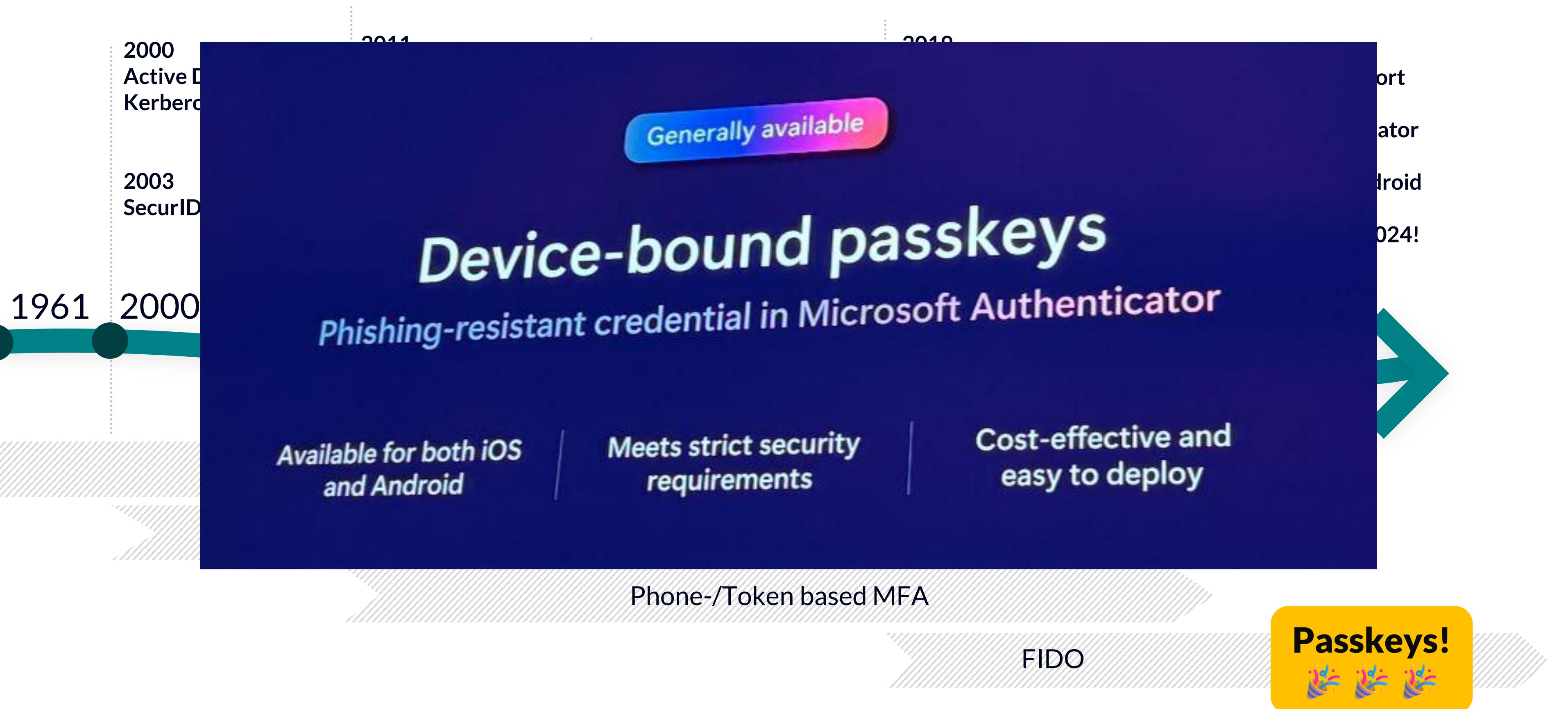
Chris Brumm

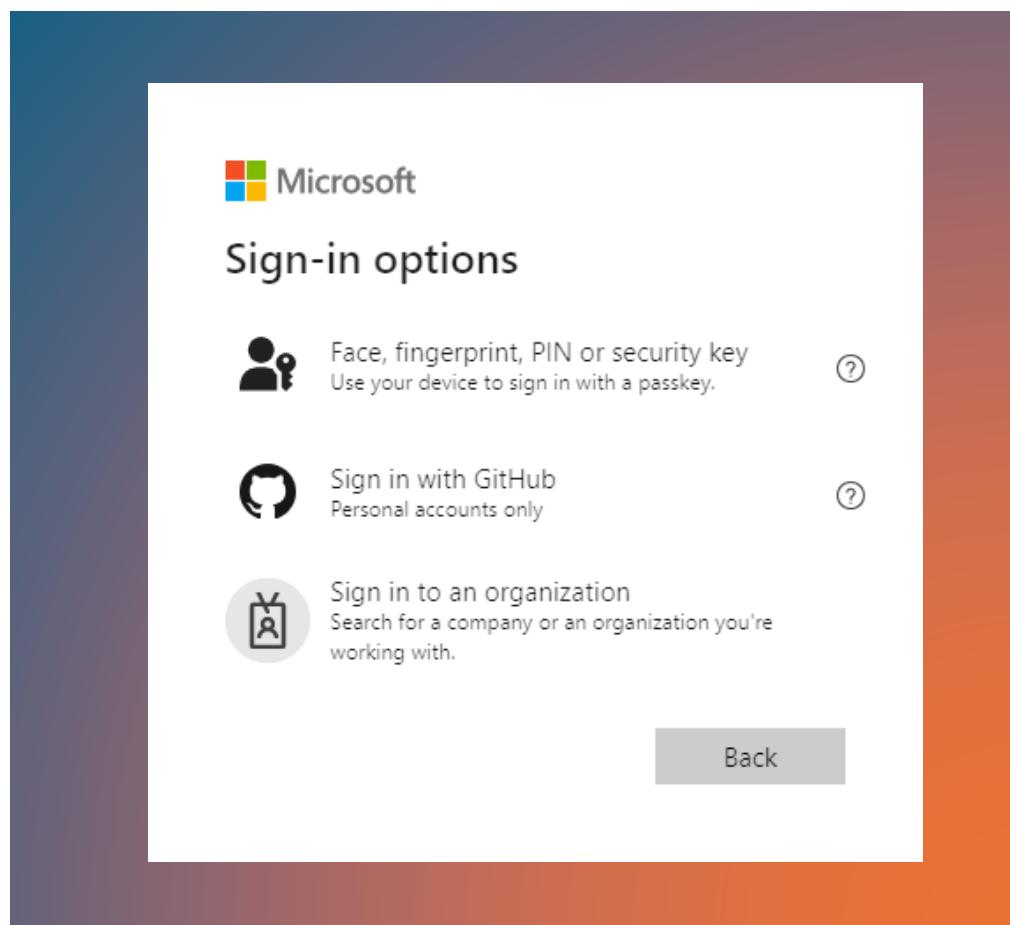
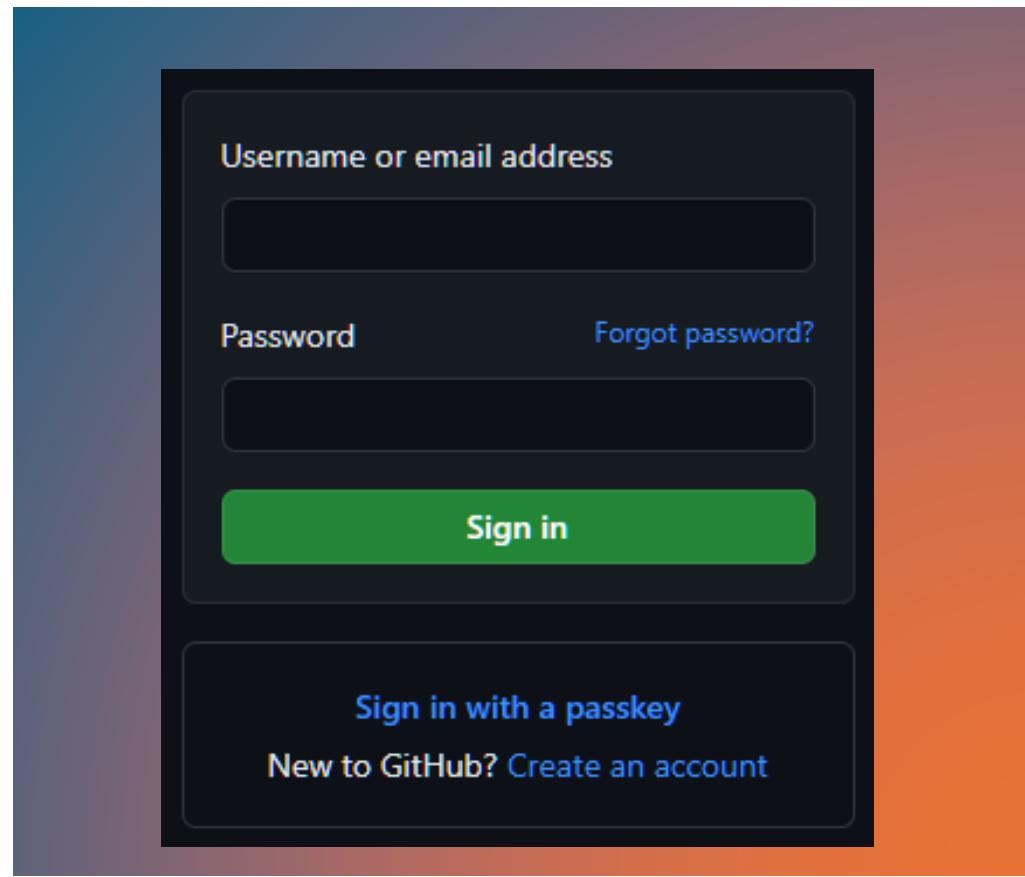
working at **glueck■kanja**
as Cyber Security Architect
living in Hamburg, Germany

Evolution of Authentication at Microsoft



Evolution of Authentication at Microsoft





What's a passkey?

- A passkey is a FIDO2/WebAuthn Discoverable Credential
- “Discoverable Credential” means you don’t have to enter your username
- Password-less
- Phishing resistant
- Based on cryptographic public and private keys

 Erstelle einen Passkey, um deine nächste Anmeldung einfacher zu machen

Dein Passkey bietet eine sichere und einfache Möglichkeit, um dich wieder bei deinem Konto anzumelden.

Verwende deinen Passkey mit deinem Fingerabdruck, der Gesichtserkennung oder der Displaysperre.

 Google Passwortmanager

Passkey zur Anmeldung in WhatsApp erstellen?

 *****5910 Passkey

Anders speichern Weiter

Dieser Passkey wird im Google Passwortmanager für cbrrh0@googlemail.com gespeichert. Du kannst ihn auch auf anderen Geräten verwenden. Die Daten werden über die Displaysperre verschlüsselt.

Mein Konto > Anmeldung & Sicherheit > Passkey

Passkey

Teilst du dieses Konto mit jemandem, der sich mit einem Schlüsselbund anmelden möchte? Diese Person muss sich ihren eigenen einrichten.

2 Passkeys bei amazon.de

 Windows Hello Einrichten: 16.08.2024	
 Google-Passwort-Manager Einrichten: 16.08.2024	

Passkey hinzufügen

💡 Wenn du einen Schlüsselbund hinzufügen möchtest, verwende ein anderes Cloud-Servicekonto (z. B.: Apple-ID oder Google-Konto).

DU HAST NUN ALLES EINGERICHTET

Nun kannst du diesen Passkey jedes Mal nutzen, wenn du dich auf diesem Gerät bei X anmeldest.

Fertig

E-Mail-Adresse oder Handynummer

Passwort

 Use a passkey

Passwort vergessen?

Einloggen

oder

Neu anmelden



Nintendo Account

Passkey Sign-In

Use a passkey to sign in to your account.

Passkey Sign-In



Sign in

Cancel

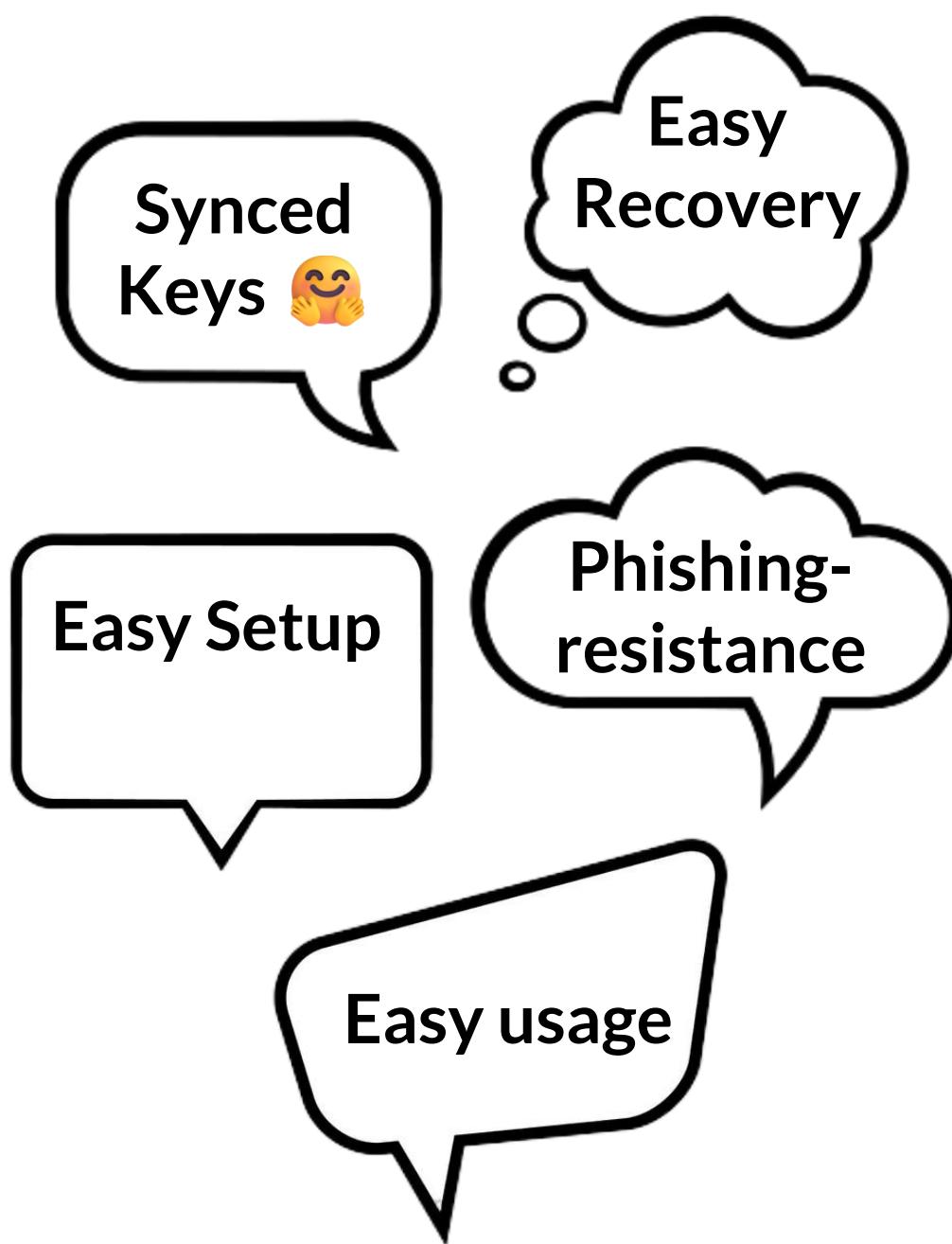
Sign in Another Way

No Passkey Sign-in

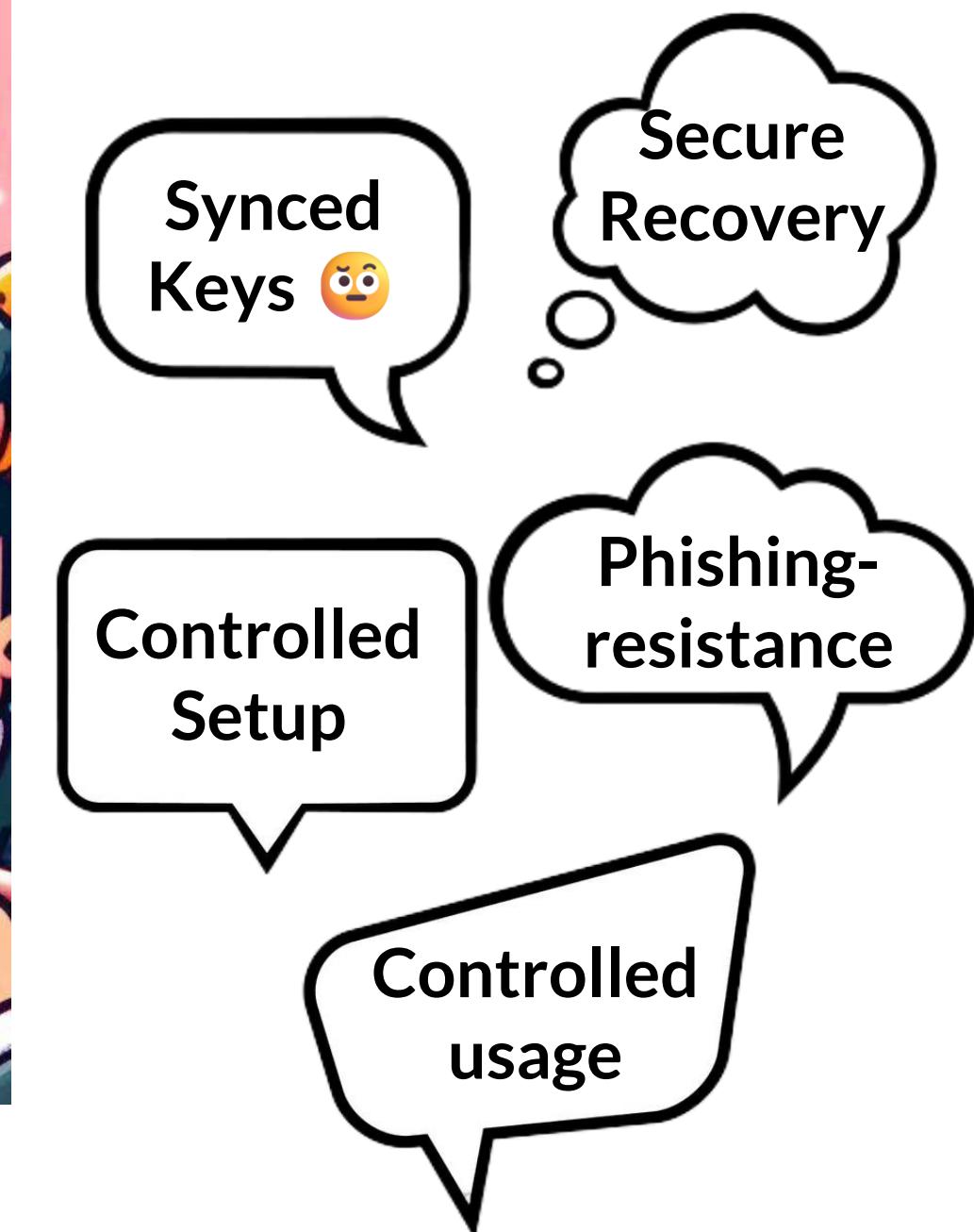
Passkeys used by Chris' family

<https://www.passkeys.io/who-supports-passkeys>

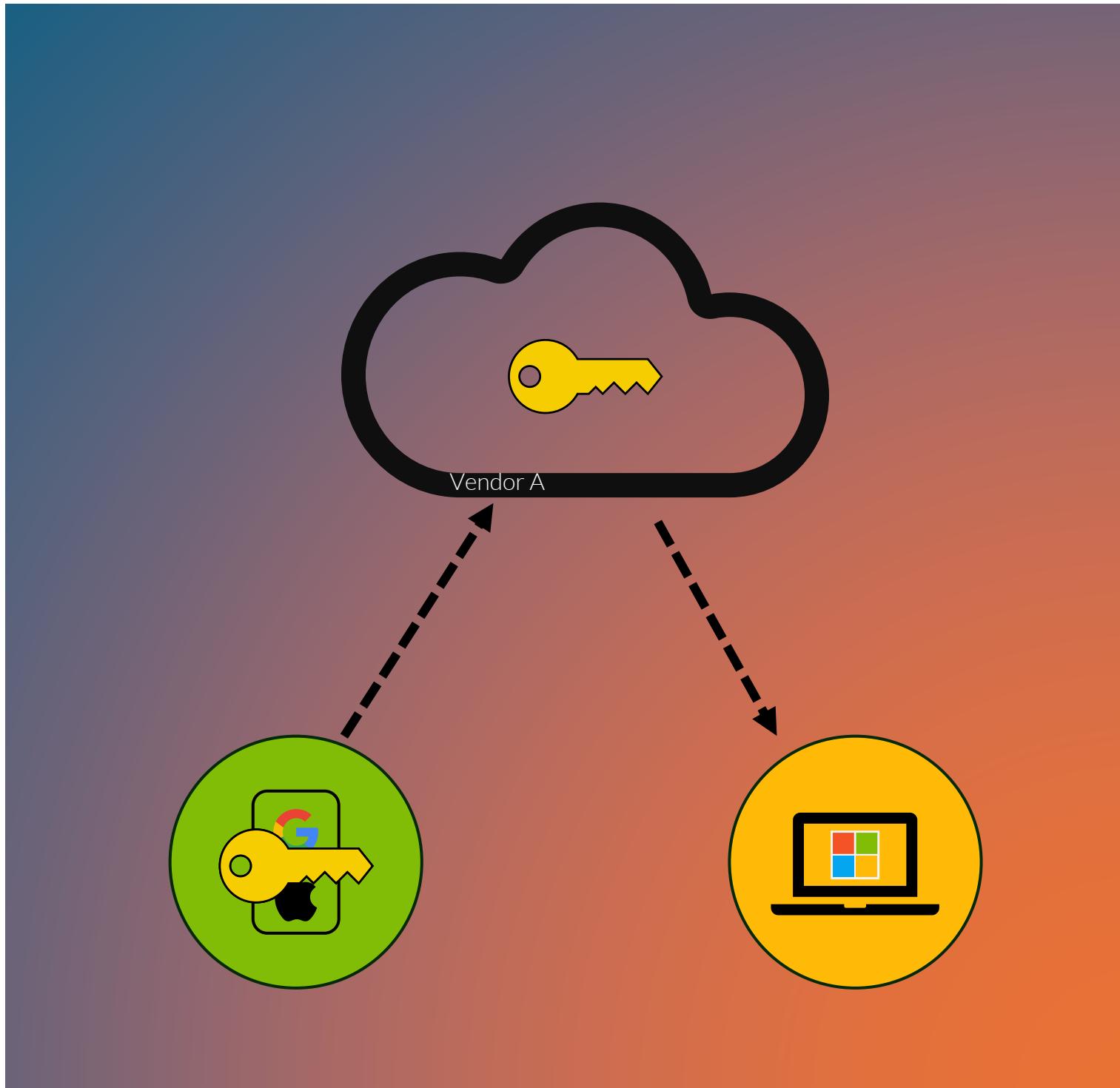
Consumer want easy passkeys!



Enterprises want secure passkeys!

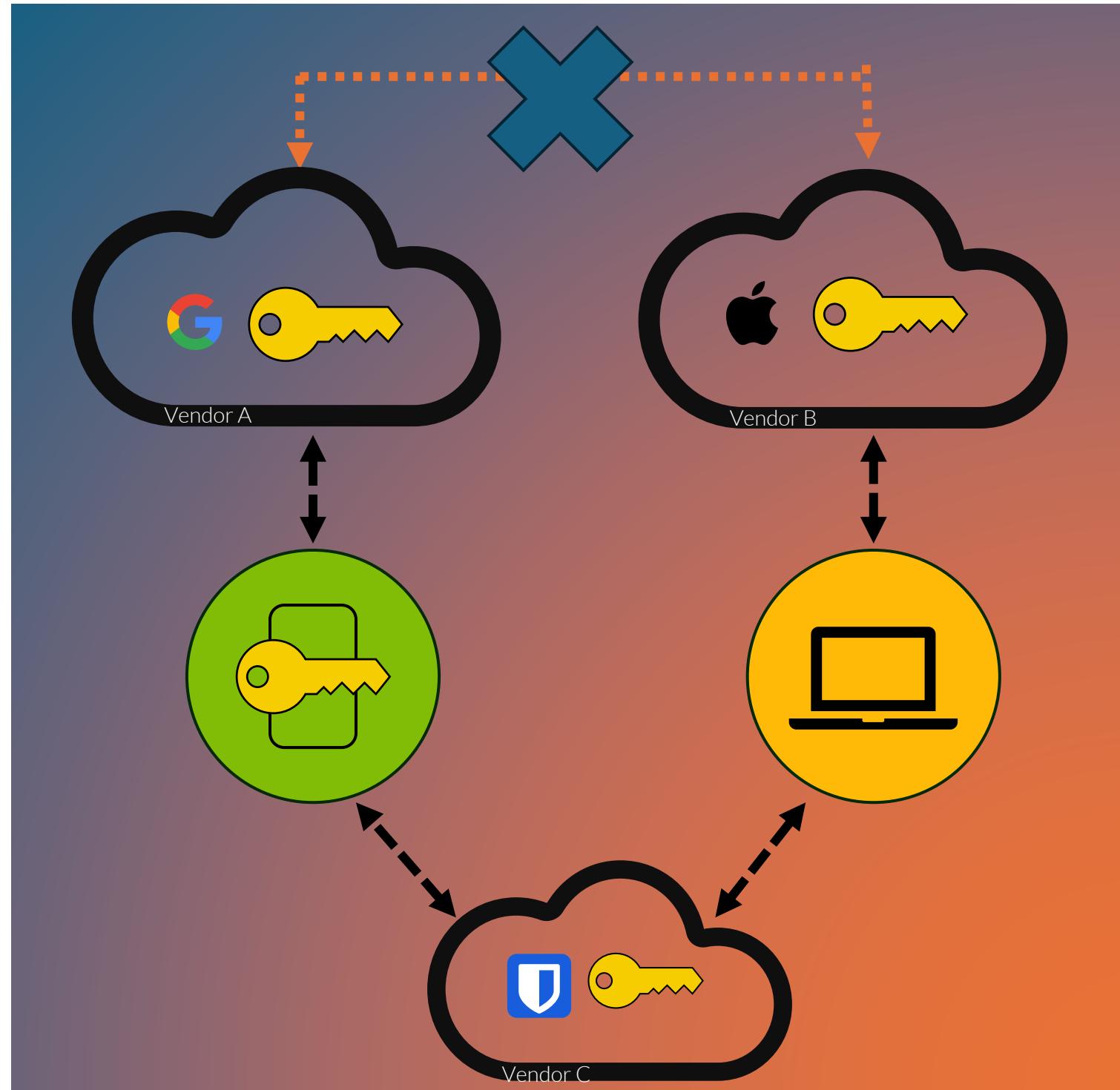


Synced vs. Device-bound passkeys



- Passkeys are synced by default
- Private key is sent to your provider
- Restore security is based on the account recovery mechanism of the provider
- Hard to track or secure for enterprises
- Backup to vendor or third-party passkey provider

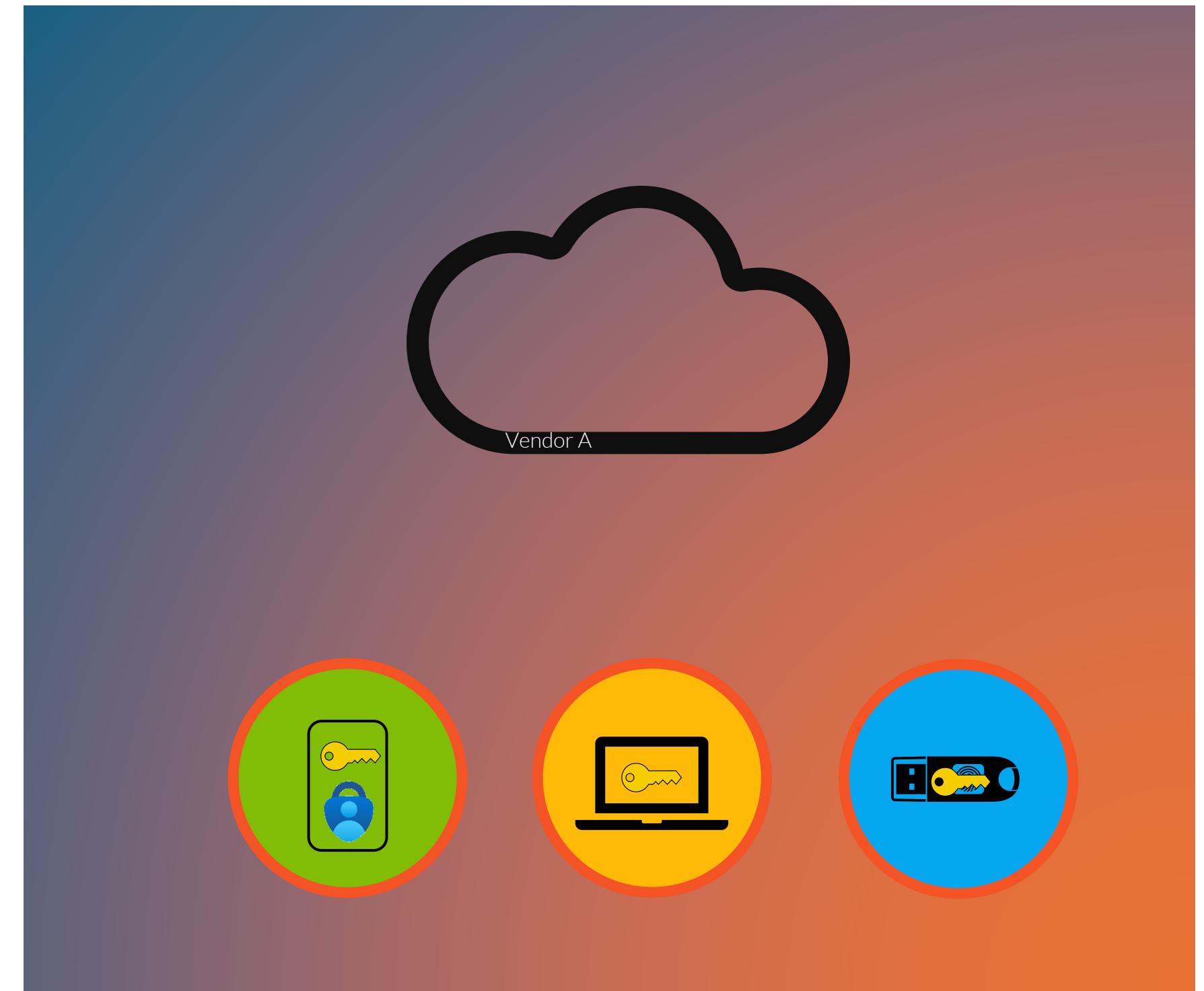
Synced vs. Device-bound passkeys



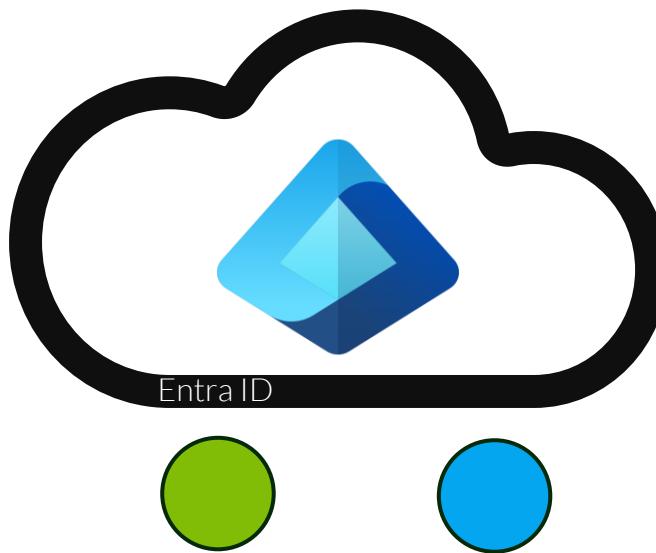
- Native cross vendor sync is not possible
- Workarounds
 - Cross-Device Authentication
 - Third-party passkey provider
 - Credential Exchange Protocol (CXP)

Synced vs. Device-bound passkeys

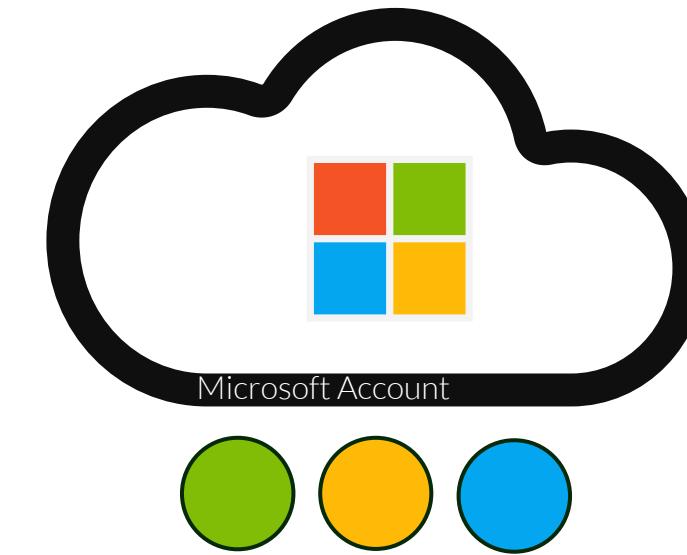
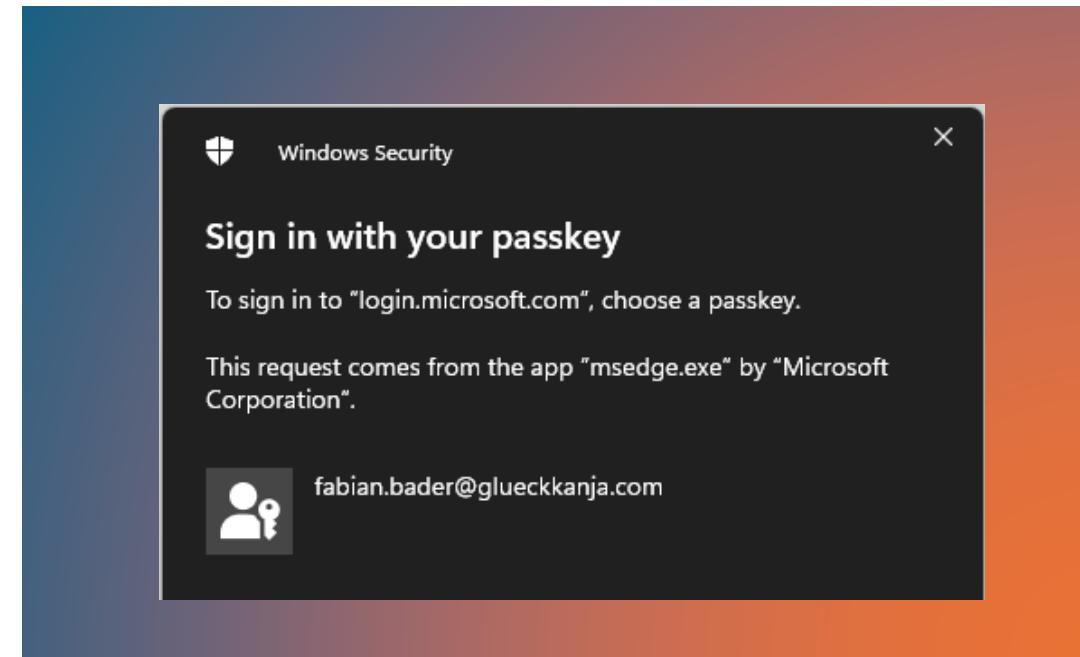
- The private key cannot leave the device
- FIDO2 security keys are device-bound passkeys
- Microsoft Authenticator creates a device-bound passkey
- Recovery = New Setup



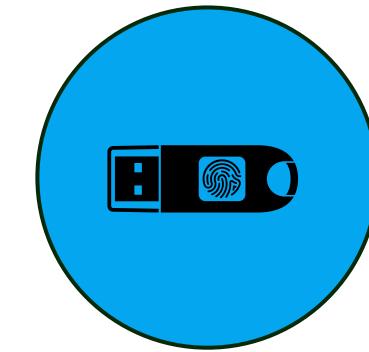
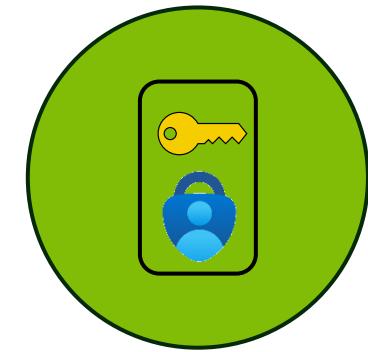
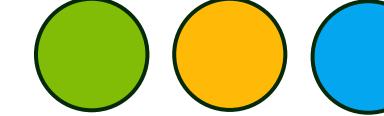
Microsoft's current implementation



Entra ID



Microsoft Account



Auth Funnel - Thanks @merill



Authentication Methods available

Authentication Methods allowed for the user
Configured through Authentication Policies

Authentication methods registered by the user

Authentication methods the user must use
Configured through authentication strengths



Passkey (FIDO2) settings

Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more.](#)

Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target [Configure](#)

GENERAL

Allow self-service set up

Yes No

Supported since GA

Enforce attestation

Yes No

KEY RESTRICTION POLICY

Enforce key restrictions

Yes No

No longer required

Restrict specific keys

Allow Block

Microsoft Authenticator (Preview) ^①

[Add AAGUID](#)

fa2b99dc-9e39-4257-8f92-4a30d23c4118

...

c5ef55ff-ad9a-4b9f-b580-adebafe026d0

...

2fc0579f-8113-47ea-b116-bb5a8db9202a

...

de1e552d-db1d-4423-a619-566b625cdc84

...

90a3ccdf-635c-4729-a248-9b709135078f

...

9ddd1817-af5a-4672-a2b9-3e3dd95000a9

...

08987058-cadc-4b81-b6e1-30de50dcbe96

...

Authentication Methods allowed for the user
Configured through Authentication Policies

**Define which Passkeys
can be registered
by your users**

Authentication methods registered by the user

Home > Users > Takeshi Kovacs

Takeshi Kovacs | Authentication methods

User

Search Add authentication method Reset password Require re-register multifactor authentication Revoke multifactor authentication sessions View authentication methods policy

Want to switch back to the old user authentication methods experience? Click here to go back.

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Prev)

You've reached your passkey limit

OK

Manage

- Custom security attributes
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Usable authentication methods

Authentication method
Passkey
Passkey
Windows Hello for Business
Microsoft Authenticator

Non-usable authentication methods

DESKTOP- Pixel

Home >

EPA 1 - Require YubiKey for Admin Access

Conditional Access policy

Delete View policy information

Name *

Assignments

Users or workload identities

Specific users included and specific users excluded

Target resources

1 app included

Network

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Enable policy

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access
 Grant access

Require multifactor authentication

"Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require authentication strength
YubiKey Only

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more](#)

View Authentication Strength	
Name	YubiKey Only
Type	Custom
Description	
Creation Date	7/28/2024, 2:05 PM
Modified Date	7/28/2024, 2:05 PM
Authentication Flows	Passkeys (FIDO2)
c5ef55ff-ad9a-4b9f-b580-adebaf026d0	
fa2b99dc-9e39-4257-8f92-4a30d23c4118	
2f-0E70f-8113-47ea-b116-bbfa8dh0202a	

Authentication methods the user must use
Configured through authentication strengths

Define which Passkeys can be used in specific situations

Auth Funnel - Thanks @merill



Authentication Methods available

Authentication Methods allowed for the user
Configured through Authentication Policies

Authentication methods registered by the user

Authentication methods the user must use
Configured through authentication strengths



1. Credential key pair generated
2. Sign public with attestation private key



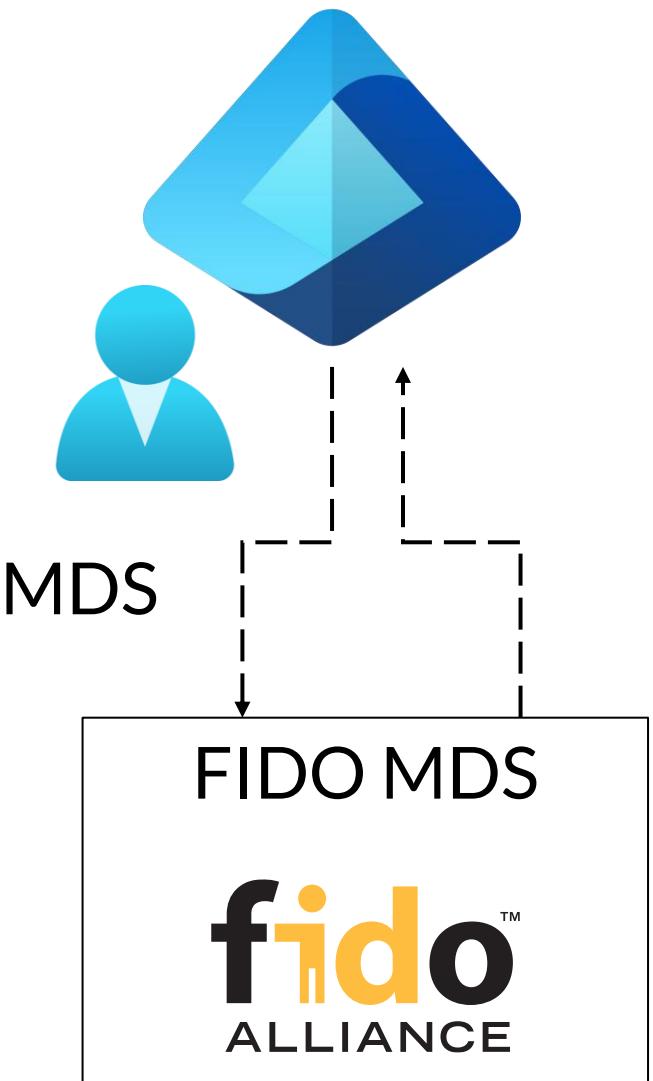
Attestation? AAGUID?

Authenticator Attestation GUID = AAGUID

3. Send signed public key to Entra ID

AAGUID: dd86a2da-86a0-4cbe-b462-4bd31f57bc6f
Vendor: Yubikey
Product: YubiKey Bio - FIDO Edition
Firmware: 5.7

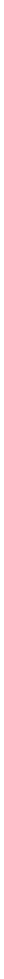
4. Request Certificate information from MDS
5. Validate signed public key
6. Store public key with user object



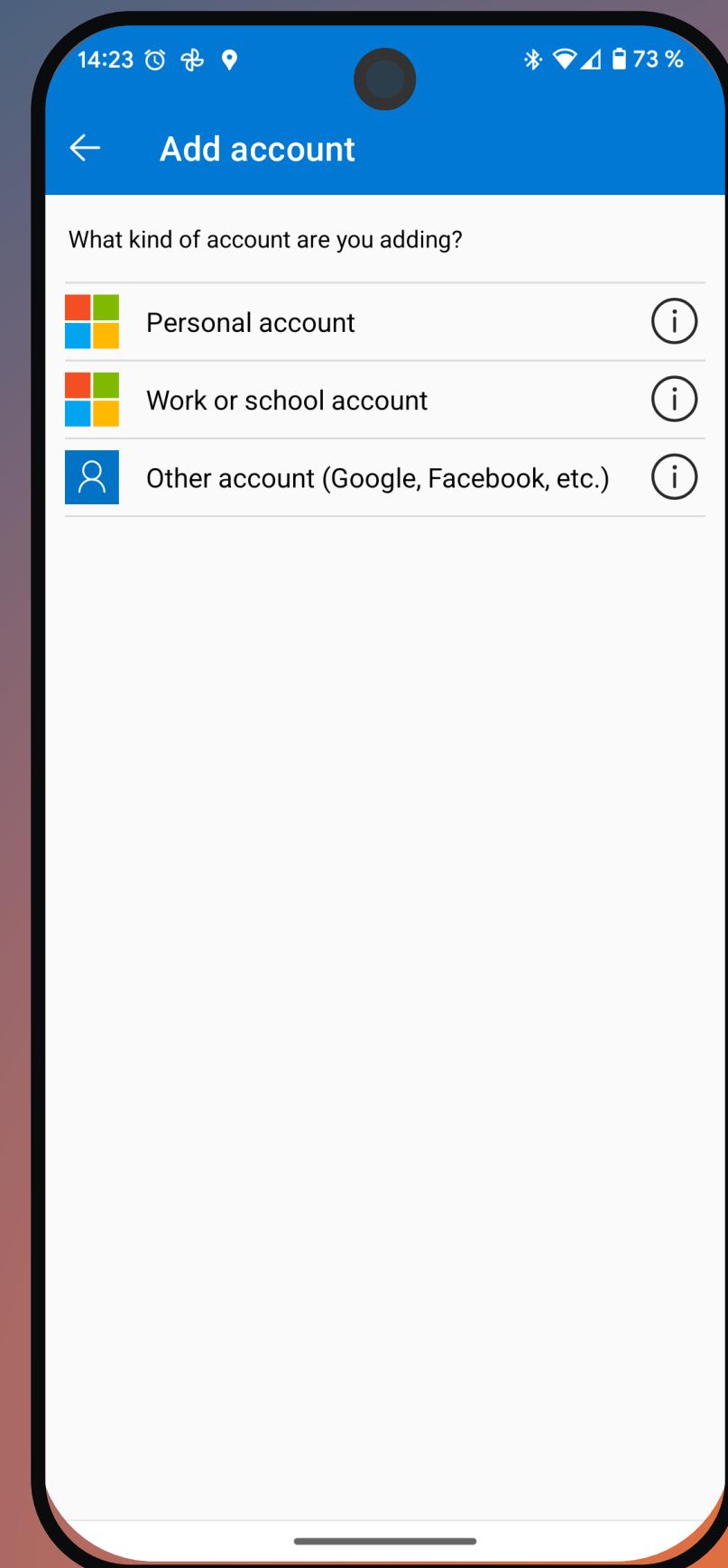
<https://aaguid.nicolasuter.ch/>

<https://fidoalliance.org/fido-technotes-the-truth-about-attestation/>

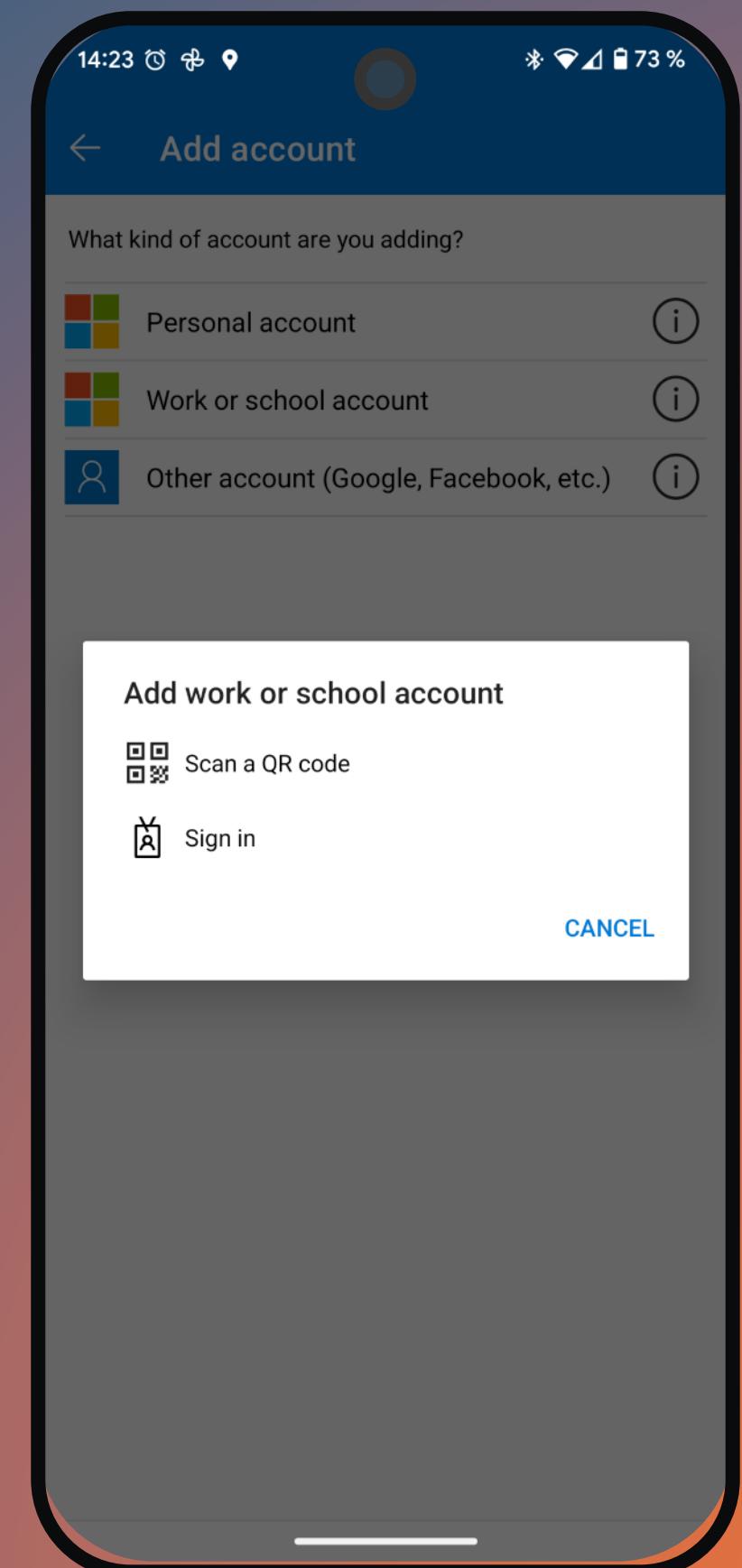
User experience in the lab



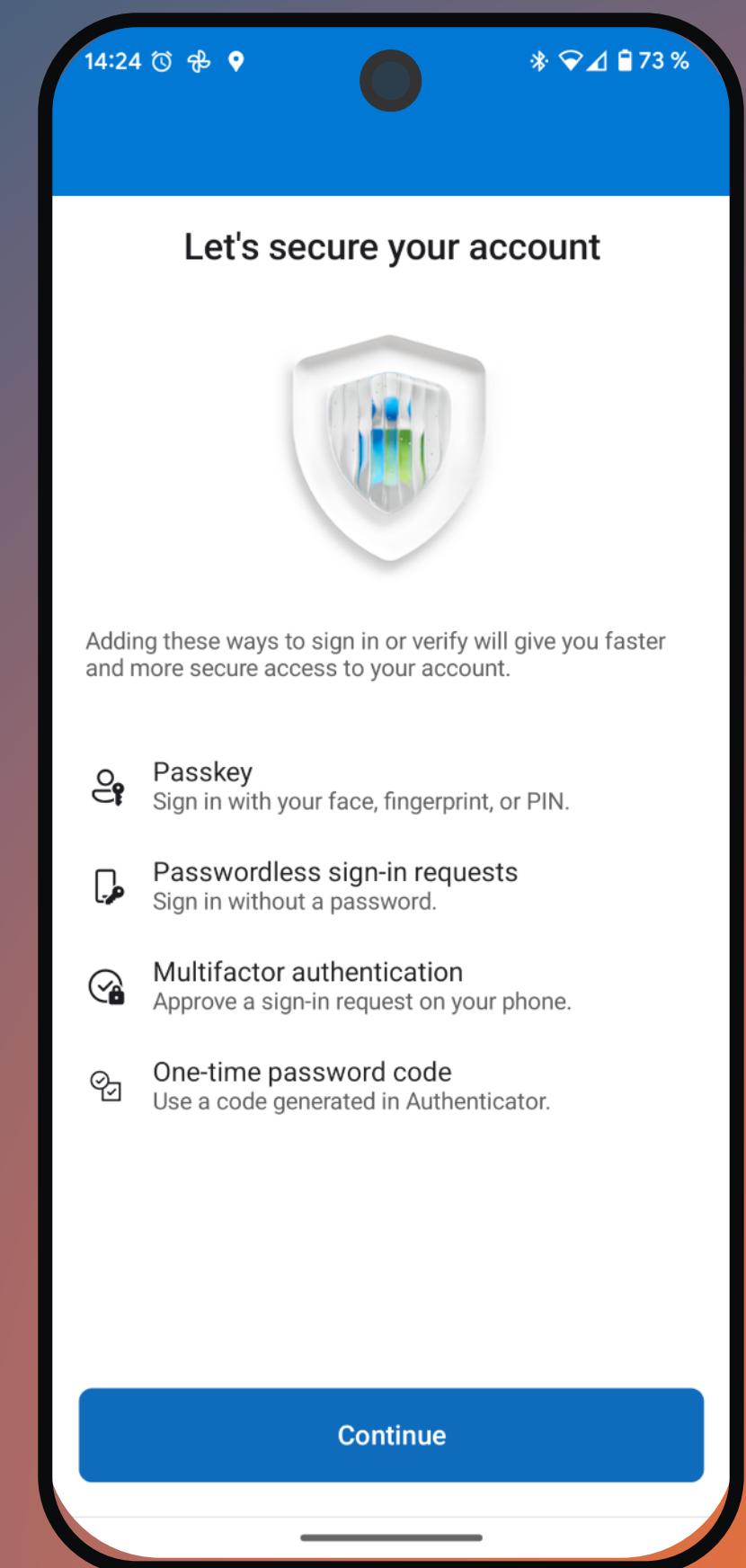
User experience in the lab



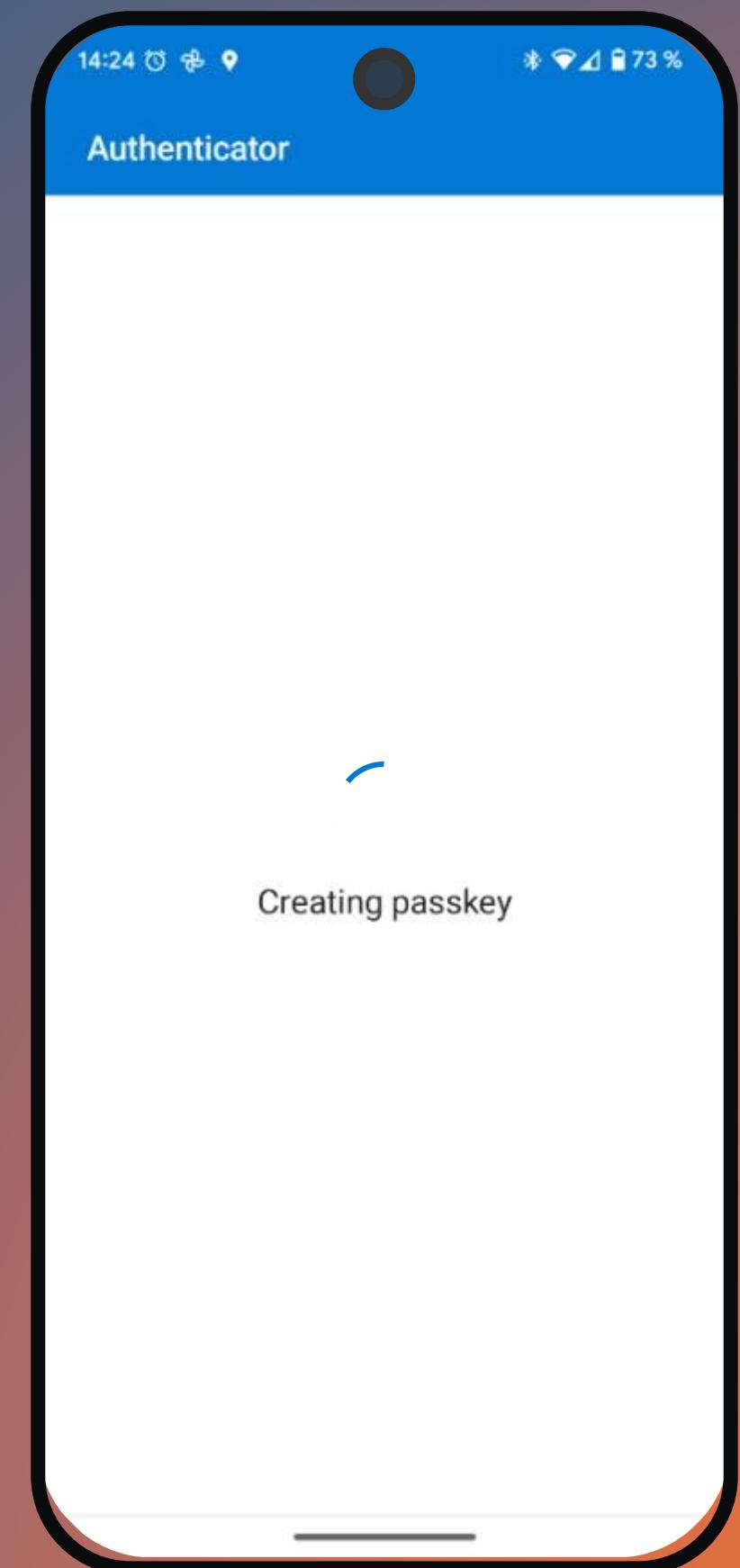
User experience in the lab



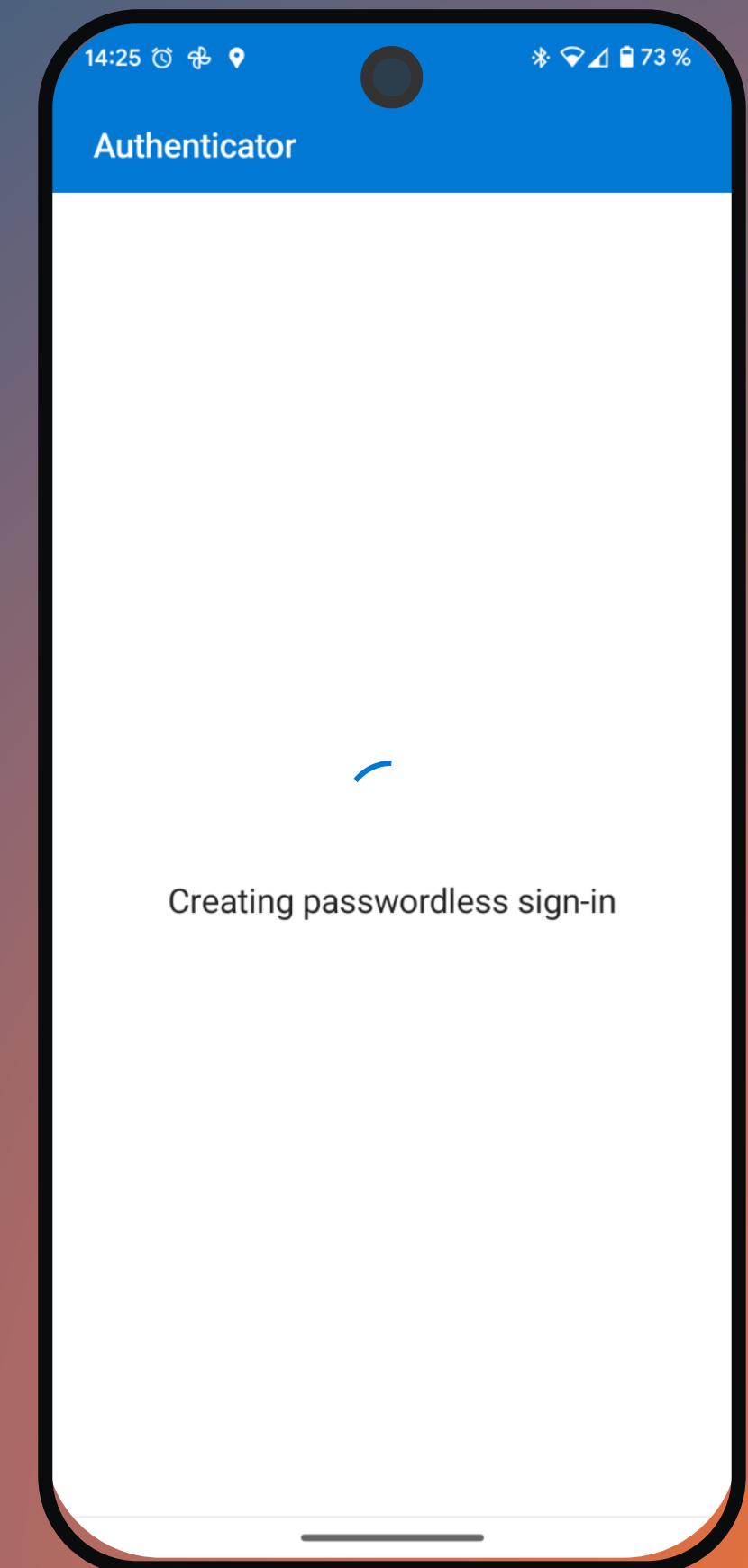
User experience in the lab



User experience in the lab

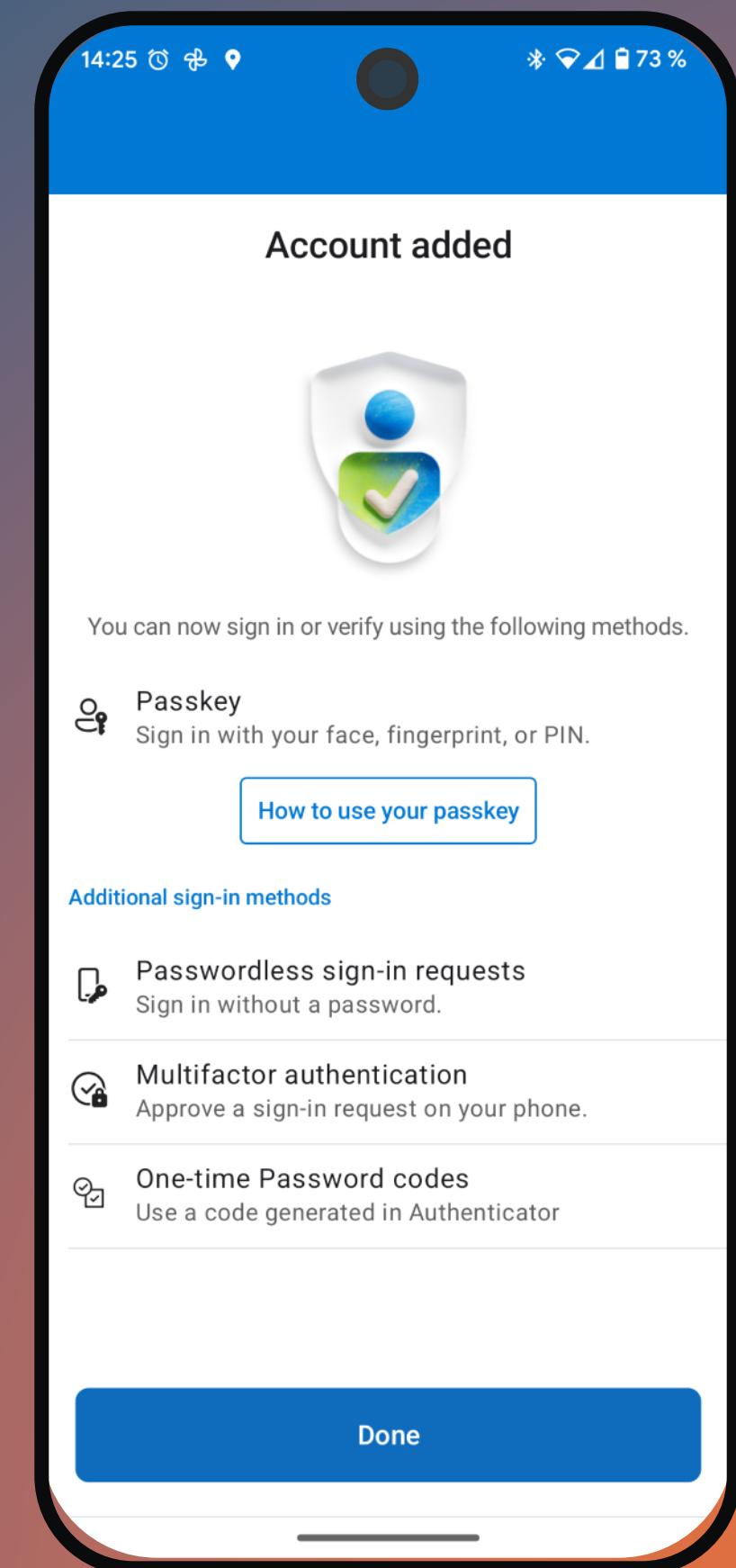


User experience in the lab

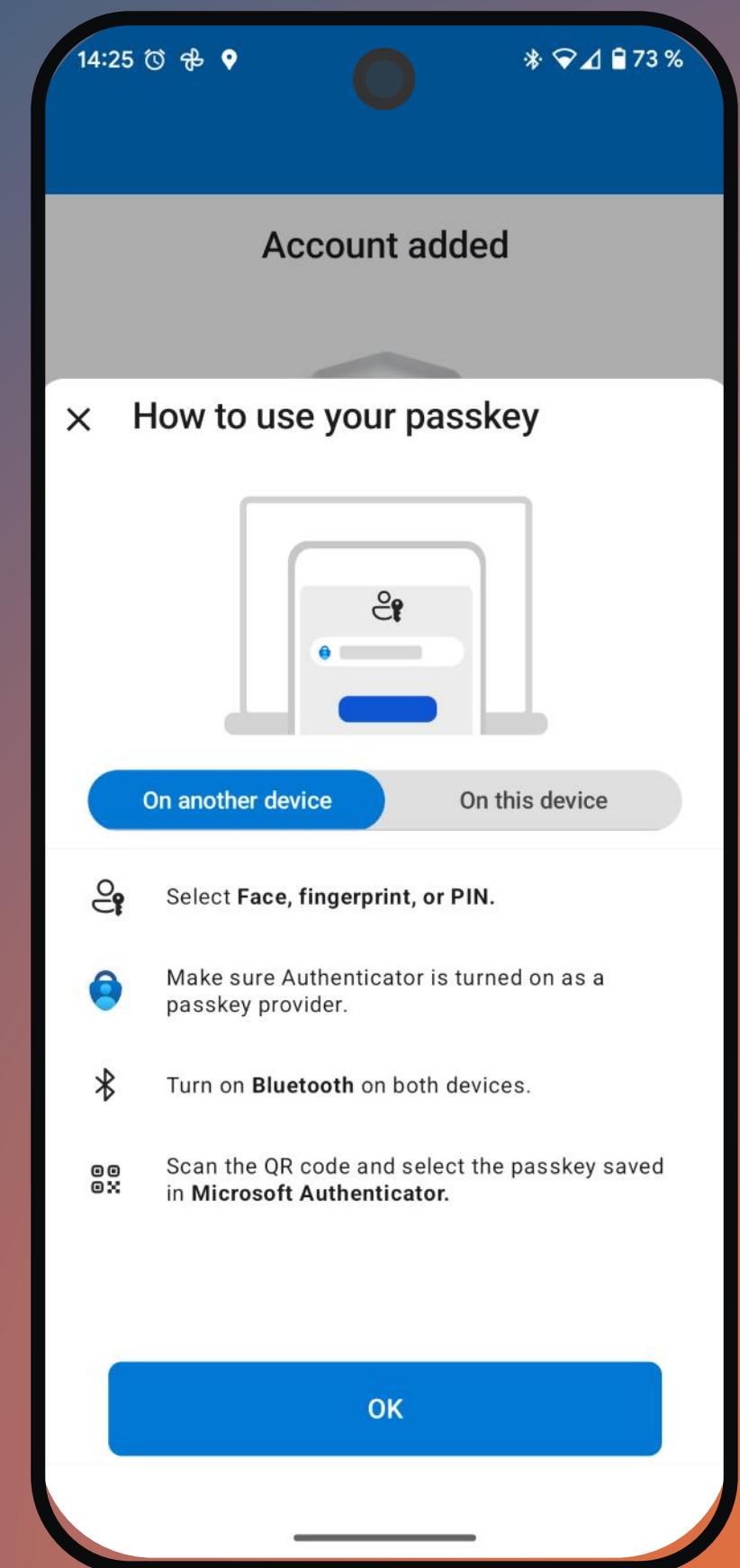


Creating passwordless sign-in

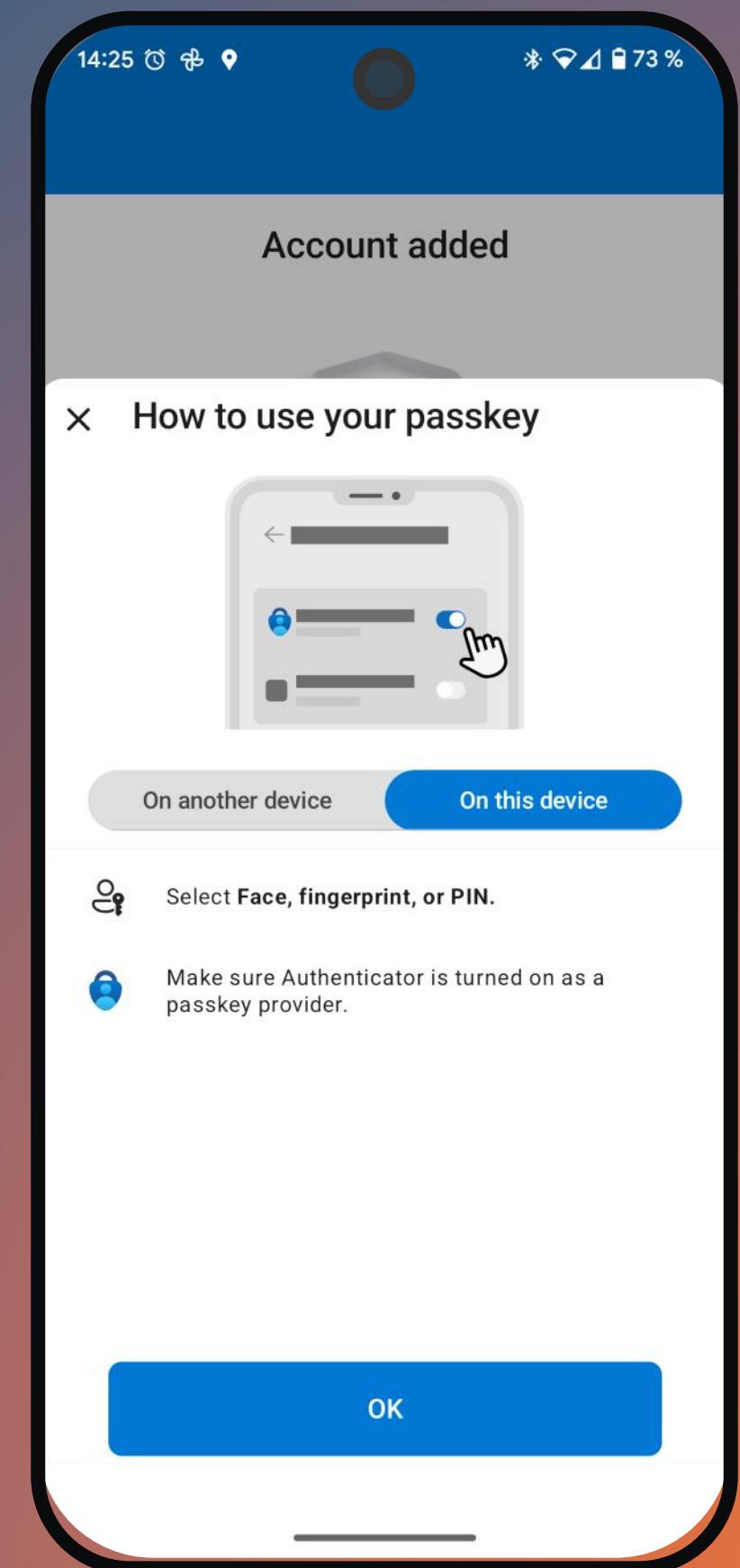
User experience in the lab



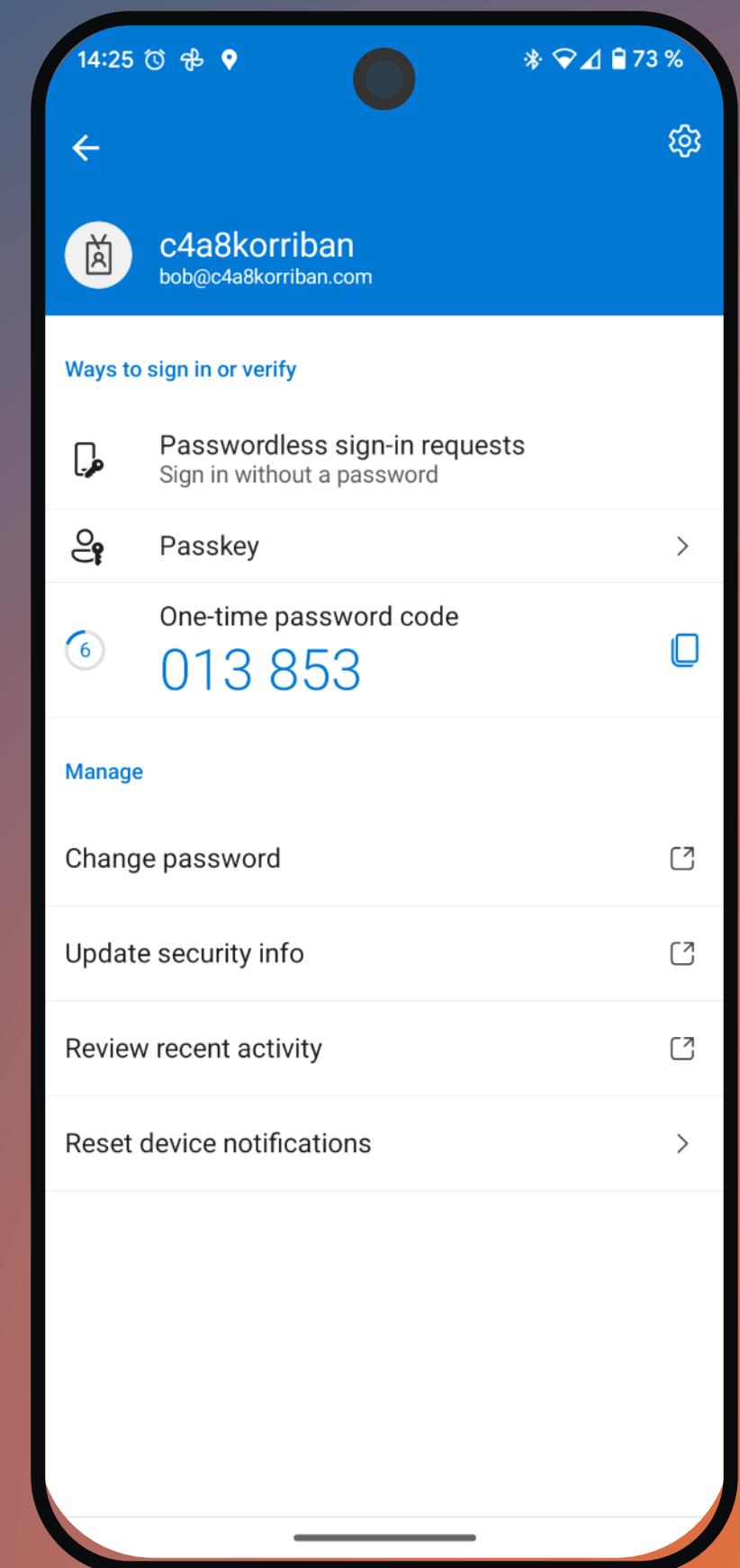
User experience in the lab



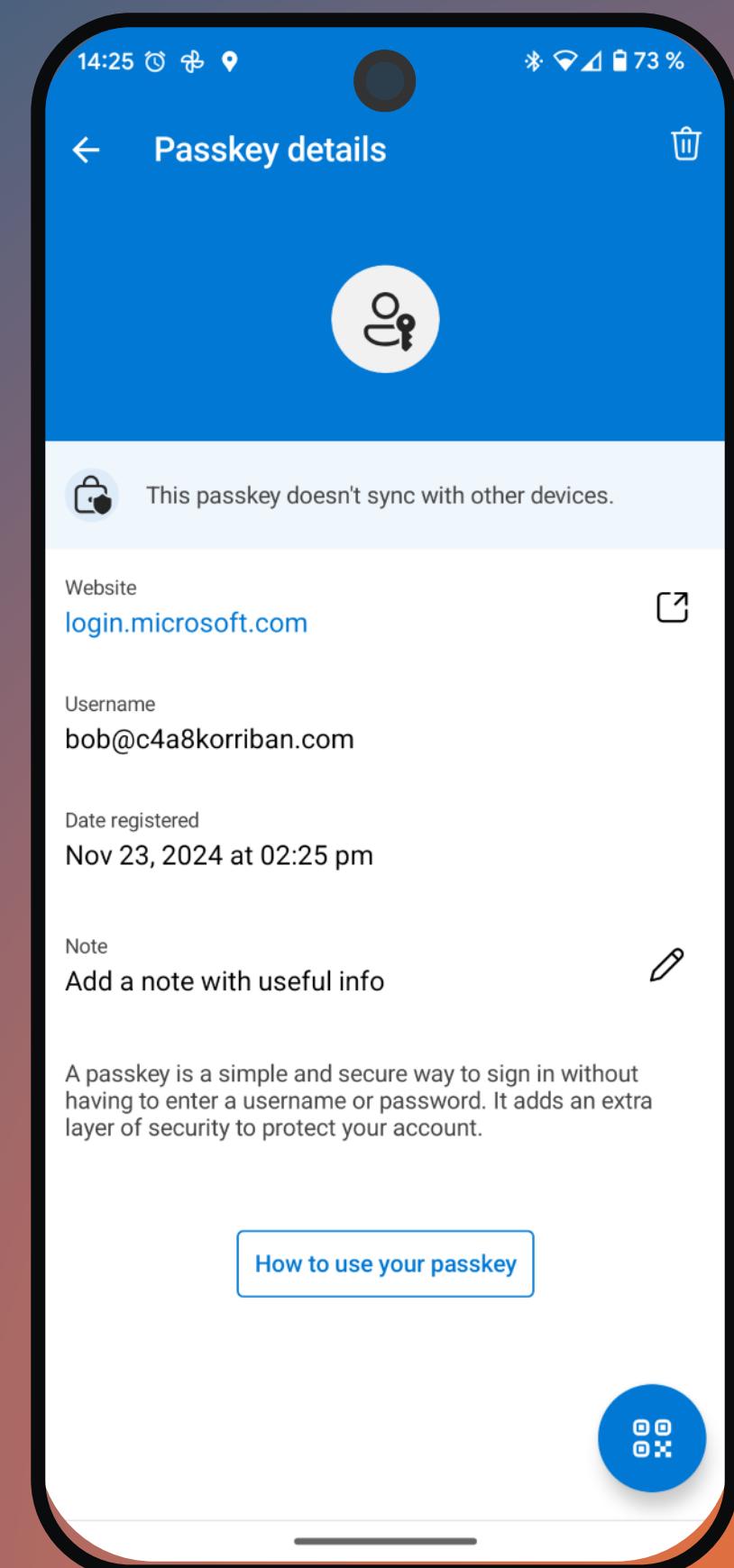
User experience in the lab



User experience in the lab



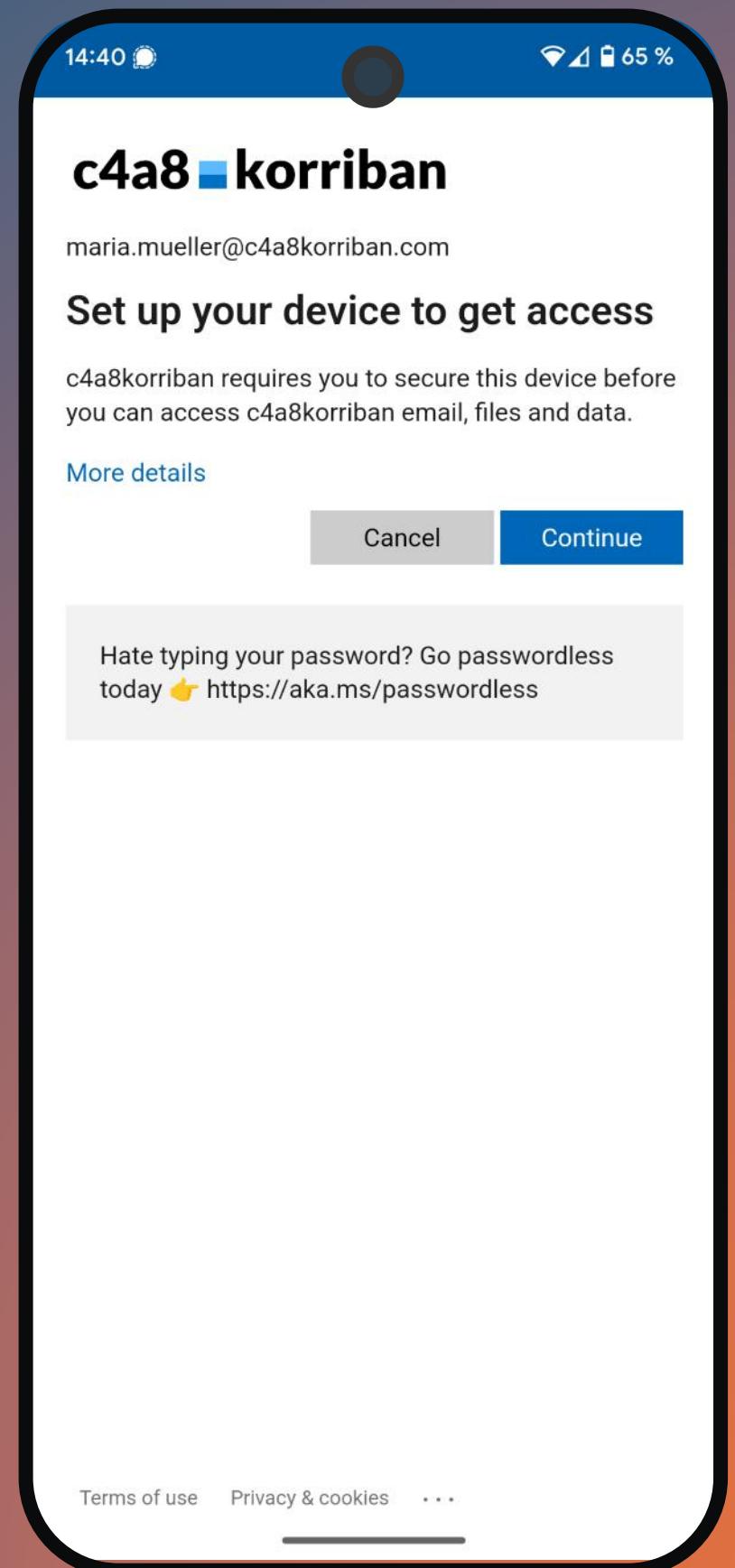
User experience in the lab



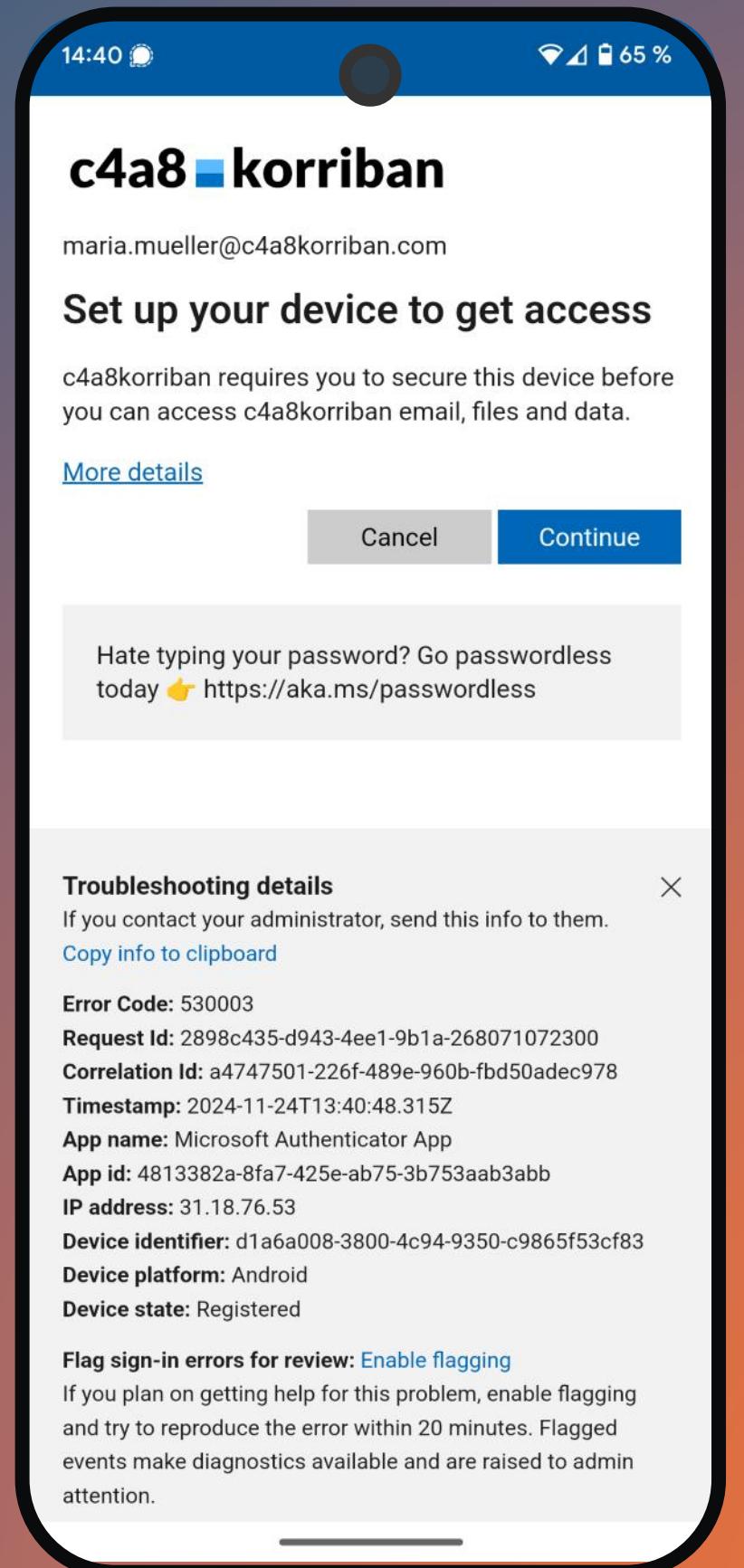


Experience in the
real world

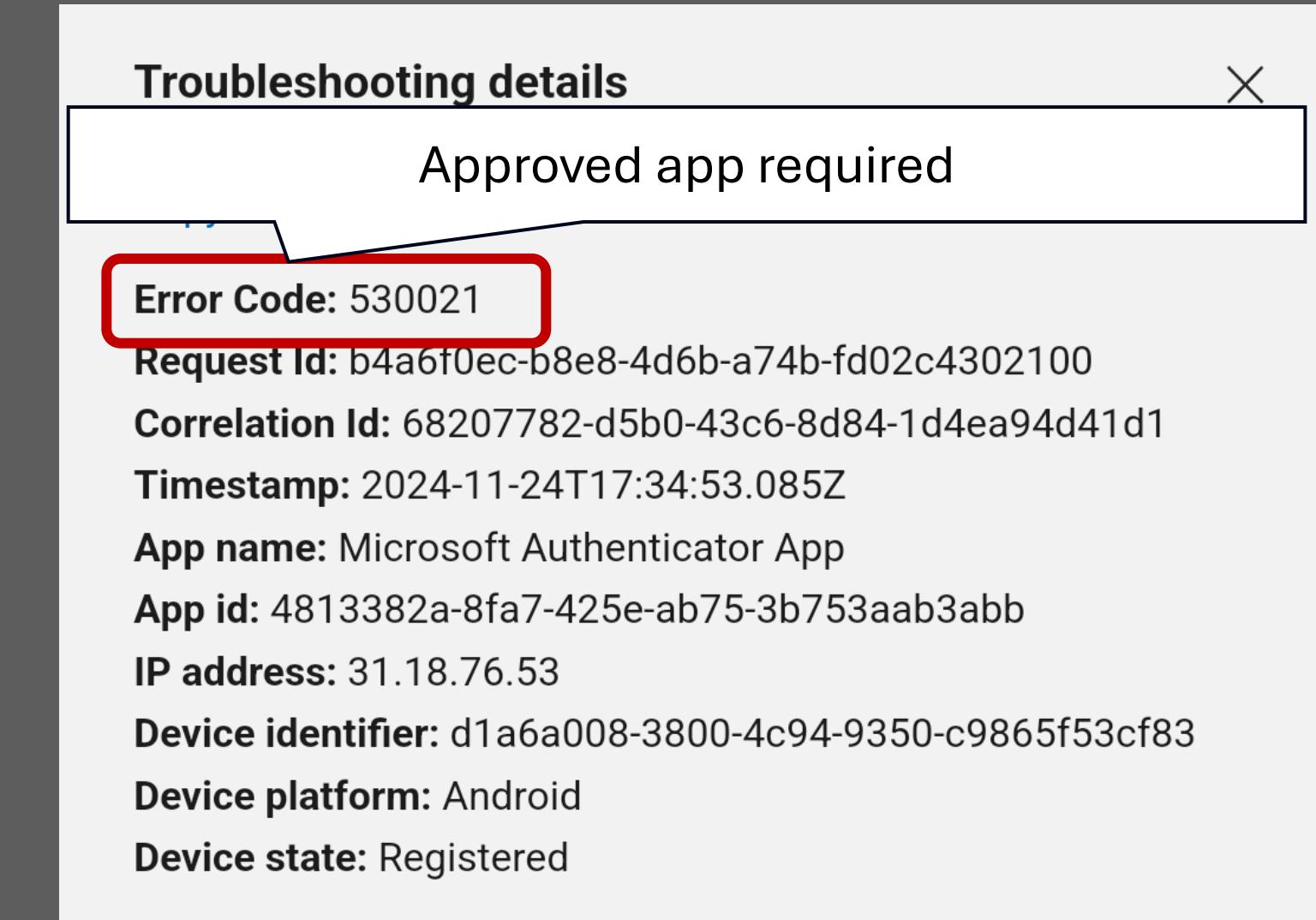
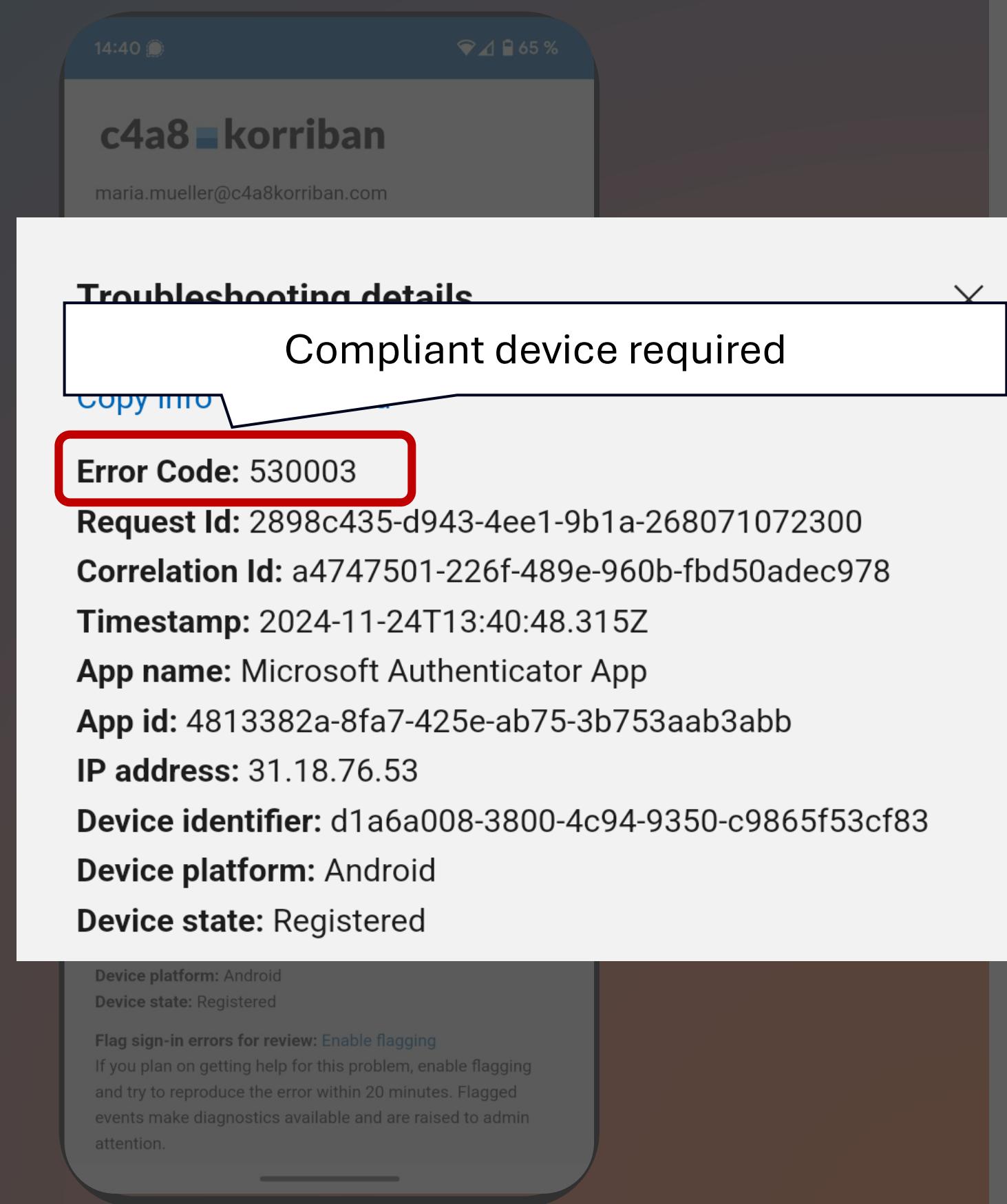




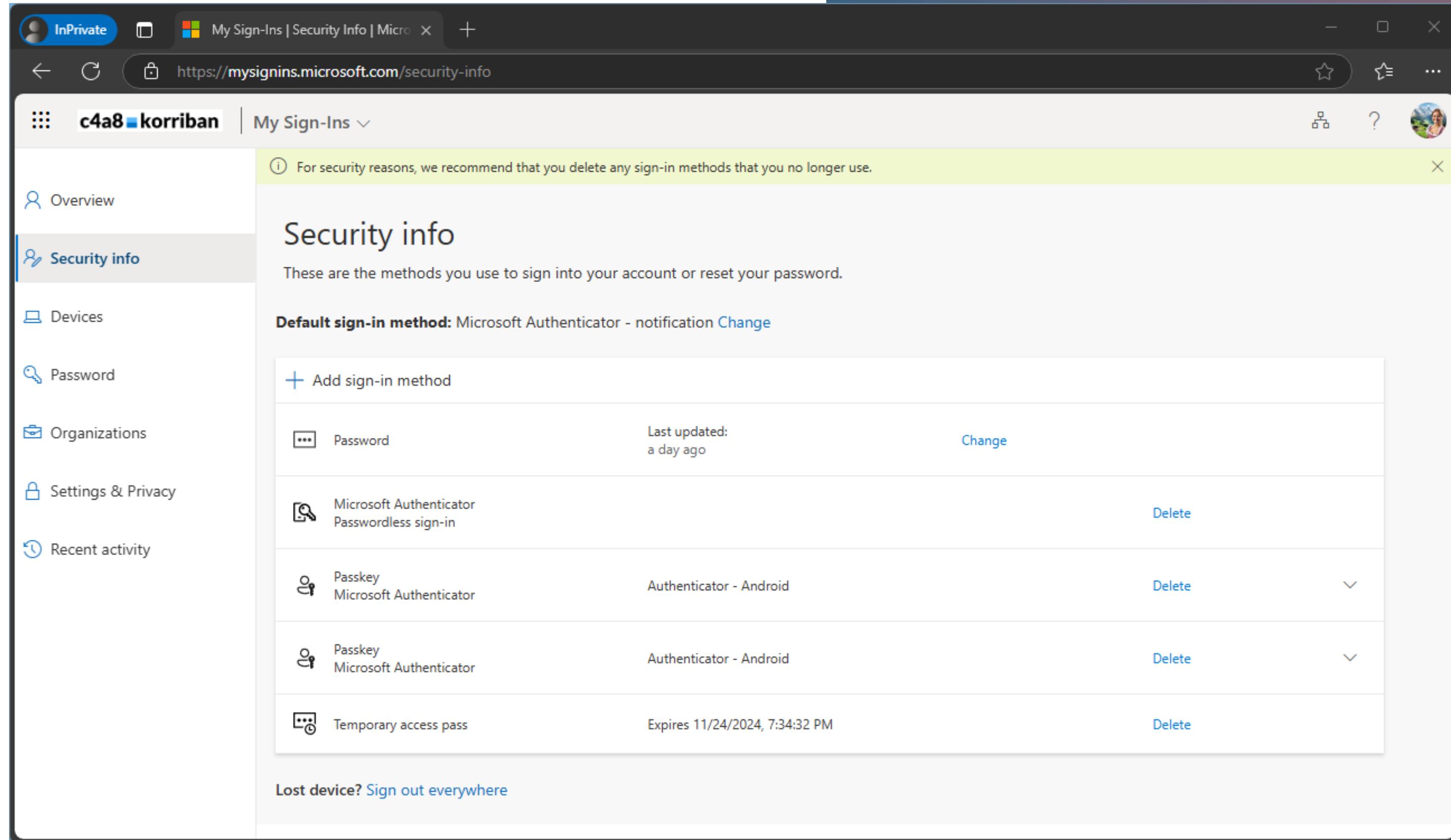
Experience in the real world



Experience in the real world



Cross Device Flow



The screenshot shows the Microsoft My Sign-Ins Security Info page. The user is signed in as **c4a8korriban**. The left sidebar has links for Overview, Security info (which is selected), Devices, Password, Organizations, Settings & Privacy, and Recent activity. The main content area displays a list of sign-in methods:

Method	Description	Actions
>Password	Last updated: a day ago	Change
Microsoft Authenticator Passwordless sign-in		Delete
Passkey Microsoft Authenticator	Authenticator - Android	Delete
Passkey Microsoft Authenticator	Authenticator - Android	Delete
Temporary access pass	Expires 11/24/2024, 7:34:32 PM	Delete

At the bottom, there is a link for [Lost device? Sign out everywhere](#).

Cross Device Flow

The screenshot shows a Microsoft Edge browser window in InPrivate mode. The URL is <https://mysignins.microsoft.com/security-info>. The main page displays 'Security info' with a note about deleting unused sign-in methods. A modal window titled 'Add a sign-in method' is open, listing four options: 'Passkey in Microsoft Authenticator', 'Security key or passkey', 'Security key', and 'Microsoft Authenticator'. Each option has a description and a 'Delete' link to its right.

InPrivate

My Sign-Ins | Security Info | Micro x

https://mysignins.microsoft.com/security-info

c4a8 koriban | My Sign-Ins

Overview

Security info

Devices

Password

Organizations

Settings & Privacy

Recent activity

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

These are the methods you can use to sign in to your account.

Default sign-in method: Microsoft Authenticator

Add sign-in method

Passkey in Microsoft Authenticator
Sign in with your face, fingerprint, PIN

Security key or passkey
Sign in with your face, fingerprint, PIN or security key

Security key
Sign in using a USB, Bluetooth, or NFC device

Microsoft Authenticator
Approve sign-in requests or use one-time codes

Temporary access pass
Expires 11/24/2024, 7:34:32 PM

Lost device? Sign out everywhere

Cross Device Flow

The screenshot shows a Microsoft Edge browser window in InPrivate mode. The URL is <https://mysignins.microsoft.com/security-info>. The main page is titled "Security info" and displays a list of sign-in methods. A modal window titled "Create your passkey in Microsoft Authenticator" is overlaid on the page. The modal contains instructions about passkeys, a note about device requirements, and a link to add the account to the Authenticator app. It also has "Back" and "Next" buttons. The background page lists a "Passkey Microsoft Authenticator" method and a "Temporary access pass".

InPrivate

My Sign-Ins | Security Info | Micro x

https://mysignins.microsoft.com/security-info

c4a8 koriban | My Sign-Ins

Overview

Security info

Devices

Password

Organizations

Settings & Privacy

Recent activity

Having trouble?

Create your passkey in Microsoft Authenticator

A passkey lets you sign in more easily and securely with your face, fingerprint, or PIN.

Make sure your device has at least Android 14 or iOS 17, and that Authenticator is updated to the latest version.

Need to add your account in Authenticator? [Add it now](#)

Back Next

Passkey Microsoft Authenticator

Authenticator - Android

Temporary access pass

Expires 11/24/2024, 7:34:32 PM

Lost device? [Sign out everywhere](#)

Cross Device Flow

The screenshot shows a Microsoft Edge browser window in InPrivate mode. The address bar displays <https://mysignins.microsoft.com/security-info>. The main content area is titled "Security info" and lists various sign-in methods. A modal window titled "Having Trouble?" provides instructions for troubleshooting Microsoft Authenticator sign-in issues using a browser and mobile device.

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

These are the methods you use to sign into your account or reset your password.

Default

Having Trouble?

Can't sign in to Microsoft Authenticator? You can still [create your passkey a different way](#) using your browser and mobile device. This requires Bluetooth on both devices.

For more information, go to our [support page](#). If you still need help, contact your admin.

Close

Method	Details	Action
Passkey Microsoft Authenticator	Authenticator - Android	Delete
Temporary access pass	Expires 11/24/2024, 7:34:32 PM	Delete

Lost device? [Sign out everywhere](#)

Cross Device Flow

The screenshot shows a Microsoft Edge browser window in InPrivate mode. The URL is <https://mysignins.microsoft.com/security-info>. The main page is titled "Security info" and displays a list of sign-in methods. A modal window titled "Which device do you want to use?" is open, listing "Android" and "iPhone or iPad".

My Sign-Ins | Security info

c4a8 koriban

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification [Change](#)

Add sign-in method

- ... Password
- Microsoft Authenticator - Passwordless sign-in
- Passkey - Microsoft Authenticator
- Temporary access pass

Which device do you want to use?

- Android**
Passkeys require at least Android 14
- iPhone or iPad**
Passkeys require at least iOS 17 or iPad OS 17

Lost device? [Sign out everywhere](#)

Cross Device Flow

The screenshot shows a Microsoft Edge browser window in InPrivate mode. The URL is <https://mysignins.microsoft.com/security-info>. The main page is titled "Security info" and displays a list of sign-in methods. A modal window is open, titled "Step 1 of 3 Turn on Microsoft Authenticator as a passkey provider". The modal contains instructions: "1. On your Android device, open **Settings**
2. Search for **Passkeys** or **Passwords and accounts**
3. Turn on Authenticator as a **passkey provider**
4. Once done, come back here." It also features a blue padlock icon and a "Having trouble?" link. At the bottom of the modal are "Back" and "Continue" buttons. The background shows a list of devices: "Passkey Microsoft Authenticator" (Authenticator - Android, Expires 11/24/2024, 7:34:32 PM), "Temporary access pass" (Expires 11/24/2024, 7:34:32 PM), and a "Lost device? Sign out everywhere" link.

InPrivate

My Sign-Ins | Security Info | Micro x

c4a8 koriban | My Sign-Ins

Overview

Security info

Devices

Password

Organizations

Settings & Privacy

Recent activity

Having trouble?

Passkey Microsoft Authenticator

Authenticator - Android

Temporary access pass

Expires 11/24/2024, 7:34:32 PM

Lost device? Sign out everywhere

Step 1 of 3

Turn on Microsoft Authenticator as a passkey provider

1. On your Android device, open **Settings**
2. Search for **Passkeys** or **Passwords and accounts**
3. Turn on Authenticator as a **passkey provider**
4. Once done, come back here.

Back Continue

Cross Device Flow

InPrivate My Sign-Ins | Security Info | Micro ...

https://mysignins.microsoft.com/security-info

c4a8 koriban | My Sign-Ins

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

These are the methods you use to sign into your account or reset your password.

Default Step 2 of 3

Get your devices ready

Make sure **Bluetooth** is on for both devices. When you're ready, a new browser window will open with the following steps:

- Select **iPhone, iPad or Android device**.
- Scan the QR code to connect your mobile device.
- Choose **Save another way**.
- Save your passkey in Authenticator.

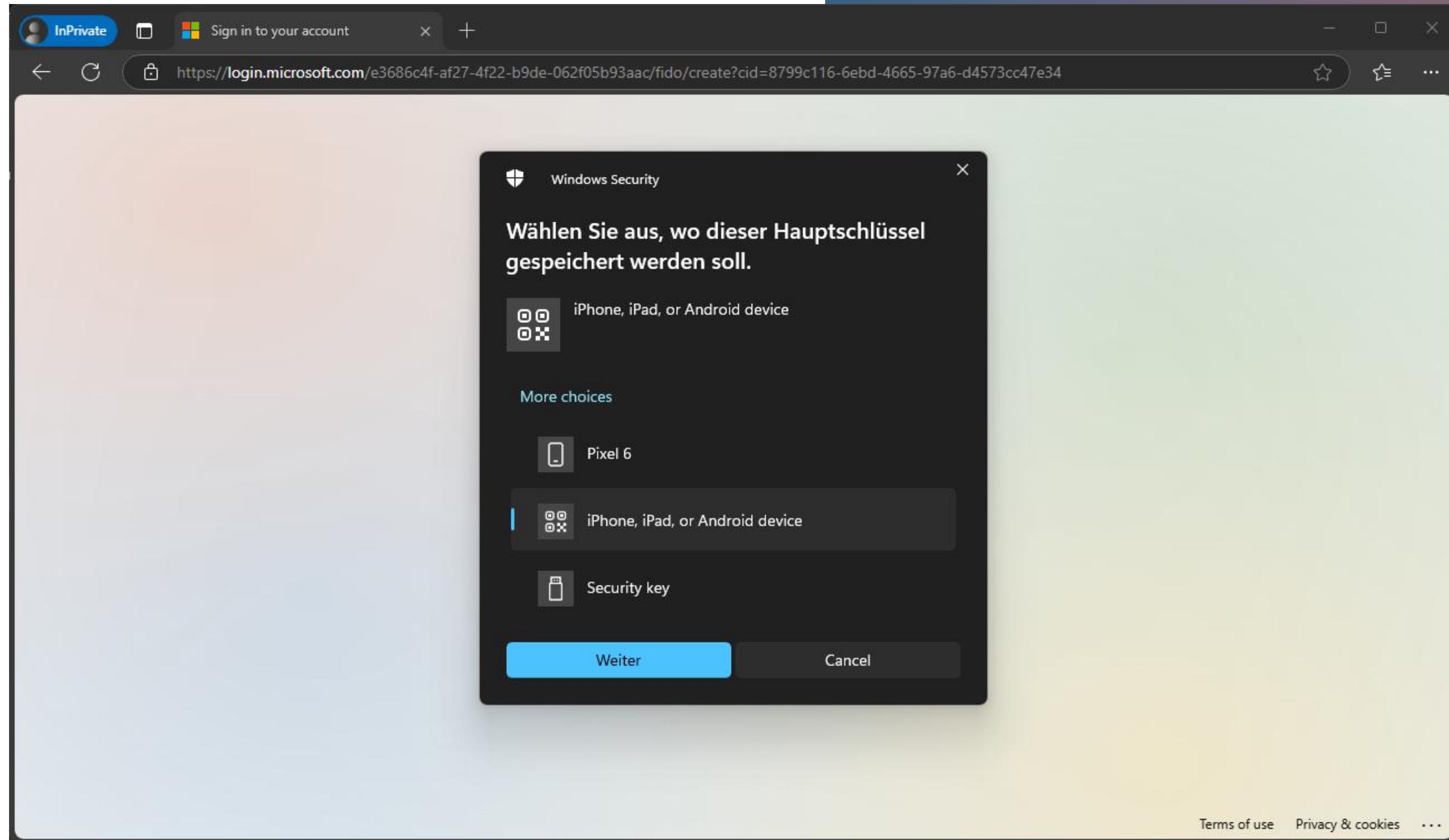
Having trouble?

Back I'm ready

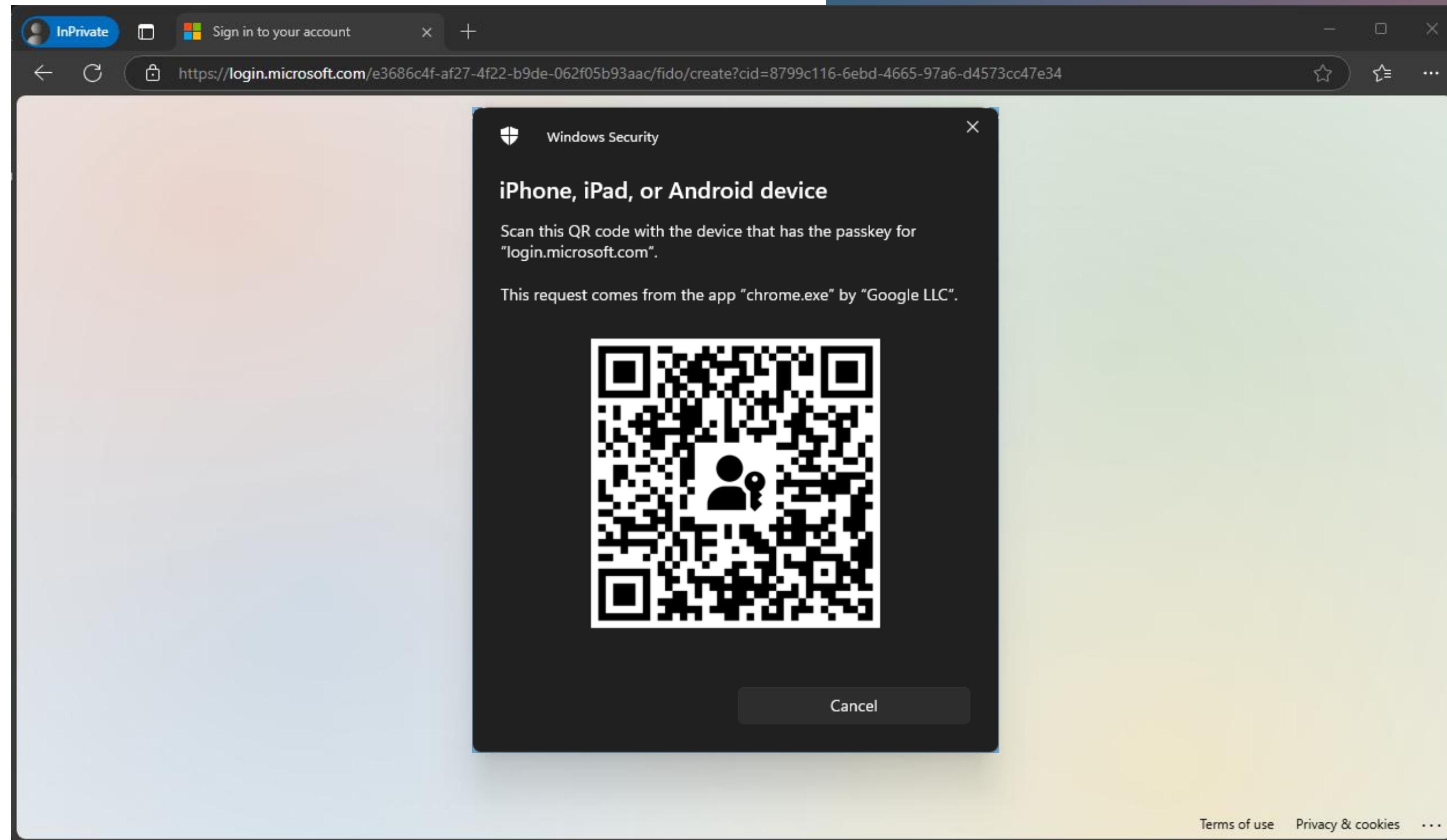
Passkey Microsoft Authenticator	Authenticator - Android	Delete
Temporary access pass	Expires 11/24/2024, 7:34:32 PM	Delete

Lost device? Sign out everywhere

Cross Device Flow



Cross Device Flow



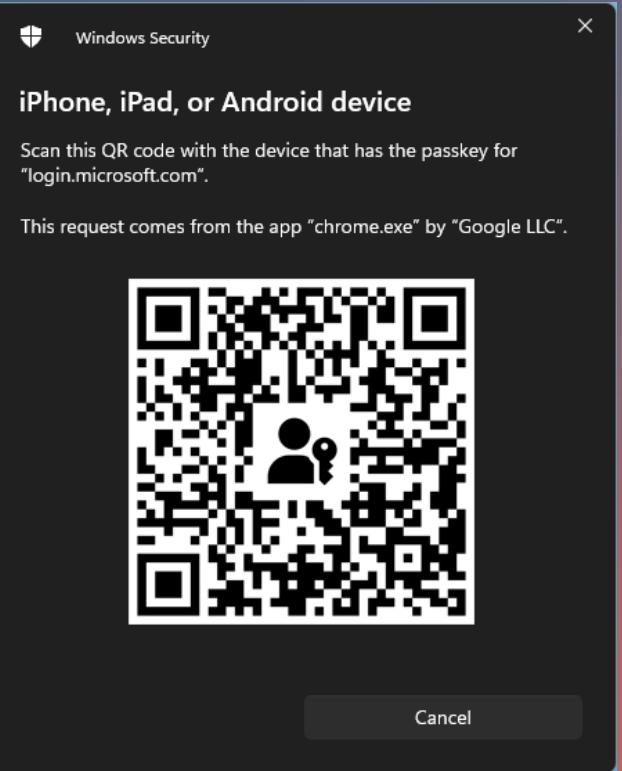


Maybe Cross-Device is
not the answer...



Cross Device

- Requires Bluetooth on both devices for proximity check
- Requires internet access
 - <https://cable.ua5v.com> (Android)
 - <https://cable.auth.com> (Apple)



FIDO: /088521772645746
304256629196898023805
213791974887885159969
946751928771388701793
485401070923423366366
303159168738737767290
060661159865120837177

QR Code Deep Dive

FIDO:/088521772645746
304256629196898023805
213791974887885159969
946751928771388701793
485401070923423366366
303159168738737767290
060661159865120837177
011010667266107096654
083332

- Base10 encoded string
- Concise Binary Object Representation (CBOR) data format

QR Code Deep Dive

FIDO:/088521772645746
304256629196898023805
213791974887885159969
946751928771388701793
485401070923423366366
303159168738737767290
060661159865120837177
011010667266107096654
083332

- Base10 encoded string
- Concise Binary Object Representation (CBOR) data format

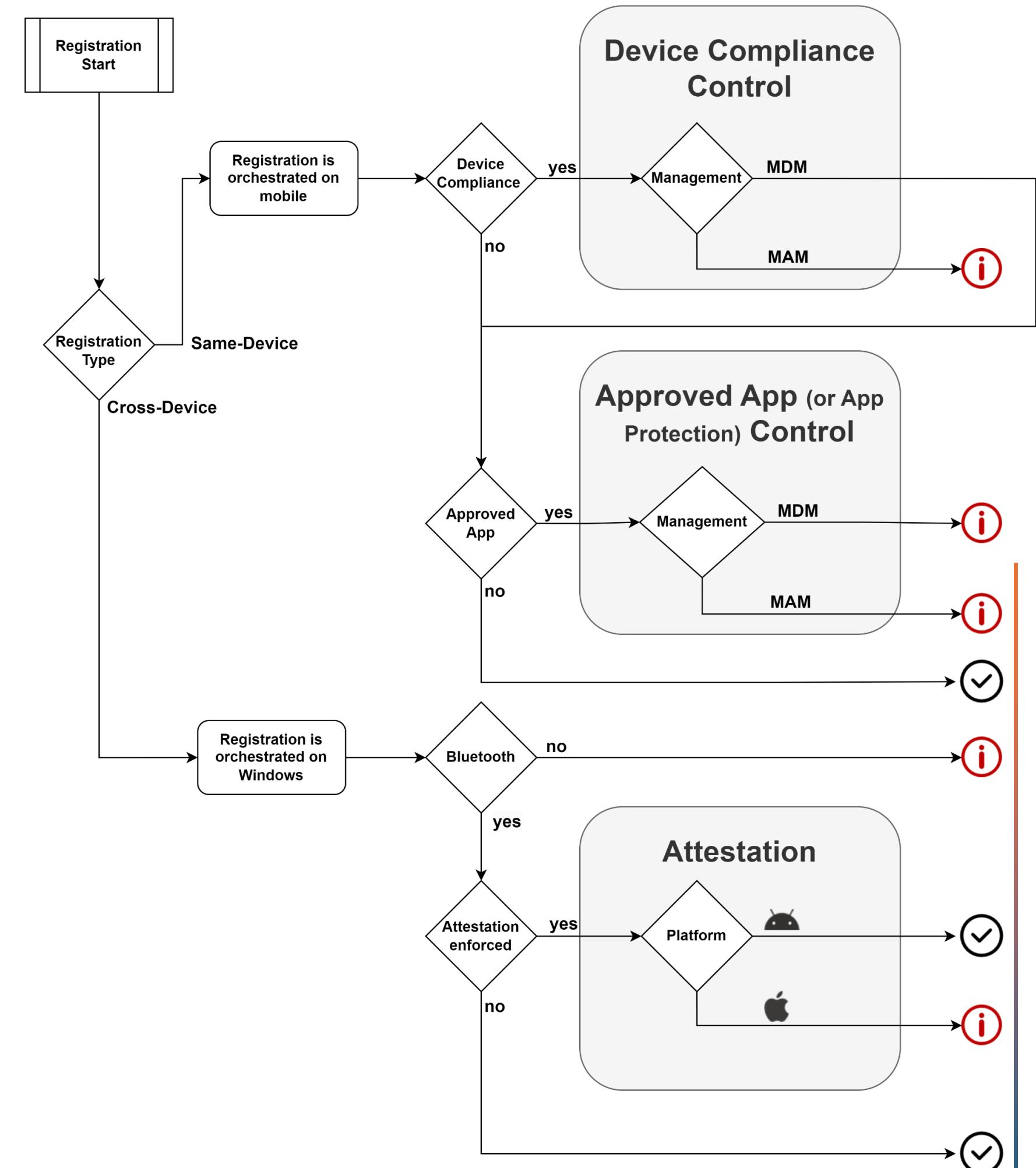
A6	00	58	21	02	73	1F
00	0E	75	37	28	D1	39
97	00	CD	91	98	8A	EA
85	12	00	2D	B4	16	91
2E	D5	38	00	7A	17	FF
52	2B	56	31	00	5F	C4
01	50	7A	F8	FB	00	59
60	2E	FD	4F	8C	38	00
48	AF	DA	C4	B5	27	02
00	02	03	1A	67	4B	14
84	00	04	F5	05	62	67
61	00	00				

QR Code Deep Dive

```
// Compressed public key
0: h'02731F0E7537[...]315FC4'
// Random QR Code secret
1: h'7AF8FB59602E[...]C4B527'
// decodeTunnelServerDomain
2: 2
// Current epoch time
3: 1732973700
// State-assisted transactions
4: true
// getAssertion or makeCredential
5: "ga"
```

Passkey "support" matrix

- Conditional Access controls apply to the device orchestrating the registration
 - Same-Device -> Authenticator App
 - Cross-Device -> Browser on Windows
 - Cross-Device requires Bluetooth
 - No attestation for iOS at Cross-Device registration



Passkey "support" matrix

Management	Conditional Access	BT	Method	Attestation	Result
MAM	Compliant device: All resources		Same-Device	Yes/No	
MAM	Compliant device: All resources		Cross-Device	Yes	
MAM	Compliant device: All resources		Cross-Device	No	
All	Approved apps: All resources		Same-Device	Yes/No	
MAM	Approved apps: All resources		Cross-Device	Yes	
MAM	Approved apps: All resources		Cross-Device	No	
Work Profile/MDM	Compliant device: All resources		Same-Device	Yes/No	
All	n/a		Cross-Device	Yes	

Passkey "support" matrix caveats

- Update to the latest OS version
- On Android also update the Play Service
Settings → About phone → Android version → Google play system update
- On Android 14 the device vendor third party passkeys are optional
 - Not supported by e.g. Motorola, Fairphone, Oppo, Oneplus, Sony*

*List based on forums entries and responses to social media outreach.

Workaround

Require approved client apps and app protection ...

Conditional Access policy

[Delete](#) [View policy information](#)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

Users or workload identities [\(1\)](#)

Specific users included and specific users excluded

Target resources [\(1\)](#)

2 resources included

Network [\(NEW\)](#) [\(1\)](#)

Not configured

Conditions [\(1\)](#)

1 condition selected

Access controls

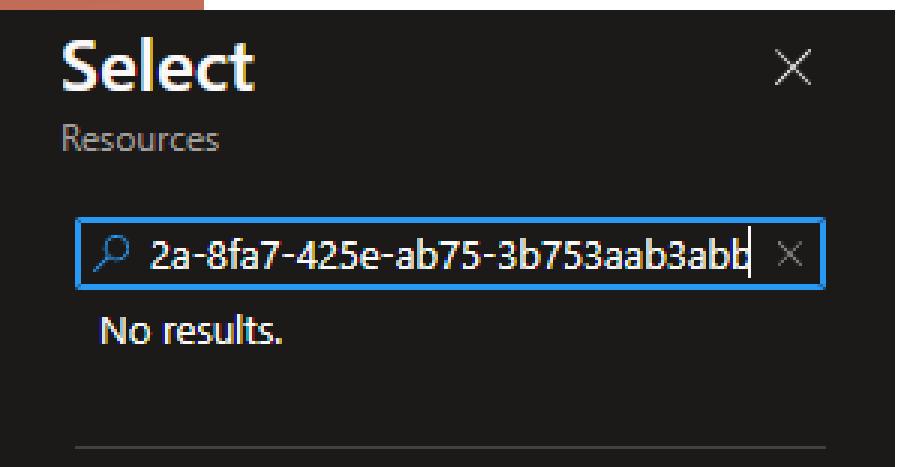
Grant [\(1\)](#)

2 controls selected

Session [\(1\)](#)

0 controls selected

To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. [Learn more](#)



Control access based on all or specific apps, internet resources, actions, or authentication context. [Learn more](#)

Select what this policy applies to [Resources \(formerly cloud apps\)](#)

Include [Exclude](#)

None

All internet resources with Global Secure Access

All resources (formerly 'All cloud apps')

Select resources

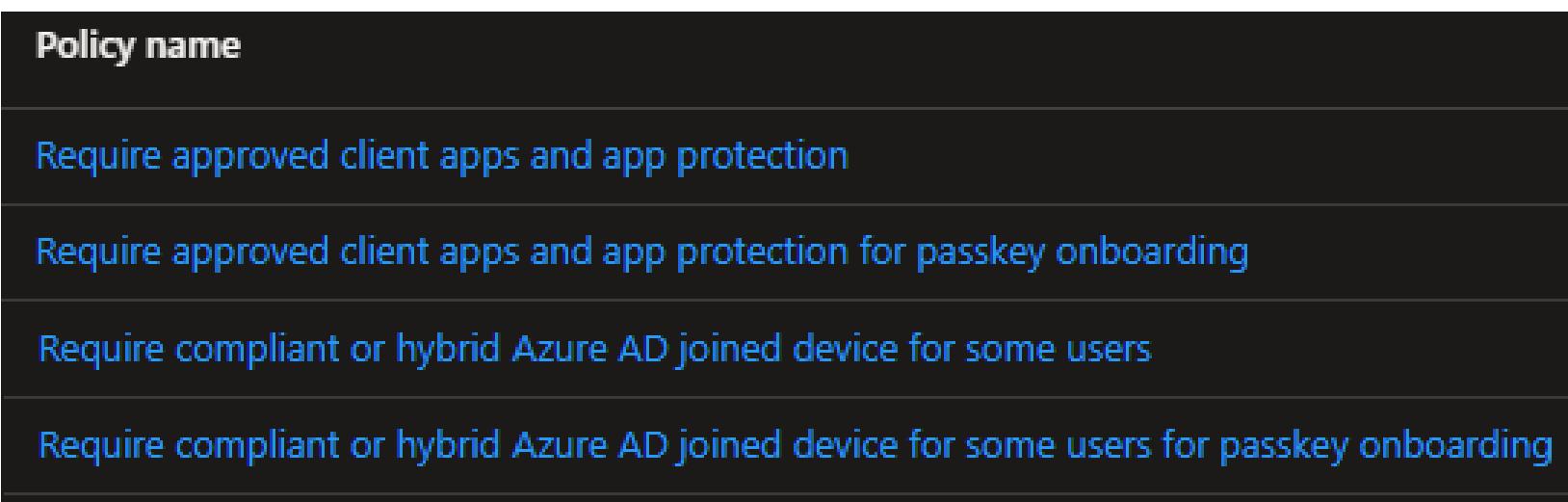
Edit filter [None](#)

Select [Office 365 and 1 more](#)

Microsoft Admin Portals [\(1\)](#) [...](#)

Office 365 [\(1\)](#) [...](#)

Workaround



My Access

c4a8korriban | My Access | Search packages by name, description or resources

Cloud Admin
cloudadmin@c4a8korriban...

Overview

Access packages

Available (3) Active (0) Expired (0)

Name ↑	Description	Resources	Actions
Advanced Protection	sec - Advanced Protection Programm		Request
Passkeys onboarding	cfg - Passkey Onboarding		Request
Verified App			Request

Passkeys onboarding

Request details Resources

Temporarily changes the access requirements to allow for passkey onboarding in the Authenticator app

Share a link to this access package:

Copy link

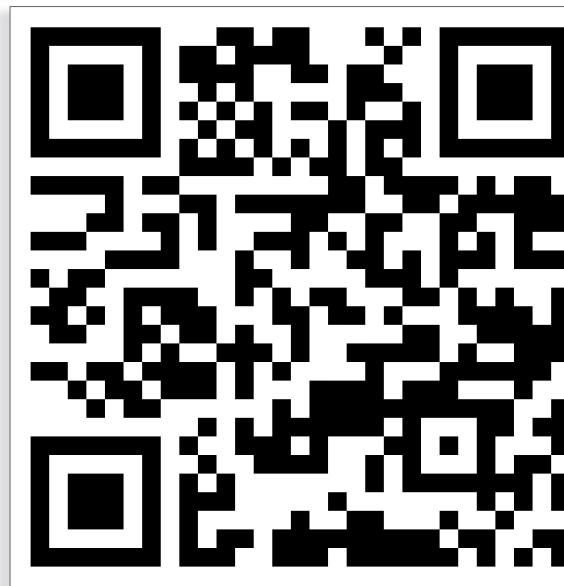
Continue

OUR BEST PRACTICES AND TIPS

- Use TAP and same device registration for initial onboarding
- On Windows devices use WHfB & Cloud Kerberos Trust
- Enable attestation (after GA)
- Restrict Security Info Registration via Conditional Access
- Enforce phishing resistant using Authentication Strength to prevent downgrade AiTM attacks
- No synced passkeys for privileged users
- Every passkey is better than a password even with MFA!**

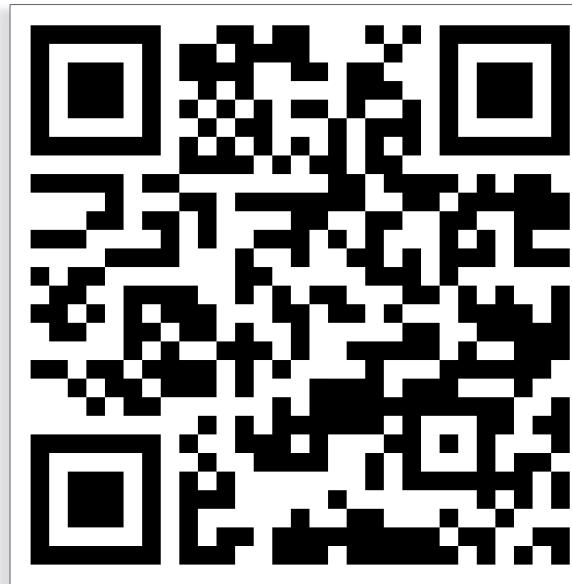


Bootstrap your
Passkey rollout with
a TAP self service

The image shows the myWorkID self-service portal and a mobile application side-by-side. Both interfaces feature a light gray header with the myWorkID logo and a sun icon. The main content area displays a user profile for "Dr Jane Doe" with a risk state of "NONE". Below the profile are four large blue buttons: "Reset Password", "Create Temporary Access Password", "Validate Identity", and "Dismiss User Risk". Each button has a small icon above it. At the bottom of both screens, the text "powered by glueck^{kanja}" is visible. The mobile app interface is a smaller version of the portal, also showing the user profile and the same four buttons.



Bootstrap your
Passkey rollout with
a TAP self service



A screenshot of a Microsoft sign-in page from a web browser. The URL in the address bar is `login.microsoftonline.com/0f642f1e-8030-465d-91cf-5252c6ca581b/oauth2/v2.0/authorize?client_id=492b3fcf-56a2-4718-97db-1c89f4762351&scop...`. The page features a dark blue background with a white sign-in form on the right. The form includes the 'glueckkanja' logo, a 'Sign in' field, a 'Next' button, and a 'Sign-in options' link. To the left of the form, there is a graphic of a smartphone with a circular trackball or fingerprint sensor on its back, and a blue arrow pointing towards the phone. The browser interface shows tabs for 'Sign in to your account' and 'glueckkanja AG'.

Big Thank You to Our Sponsors





Thank you!

MyWorkId





Next up

Next session with Bert-Jan Pals:

**Let us summarize
these logs for you**

In this session we will dive into the Microsoft Graph Activity Logs and show the benefits of Microsoft Sentinel summary rules for your wallet.

@ 14:20 / Room 4 / Floor 2