The state of passkey in 2025

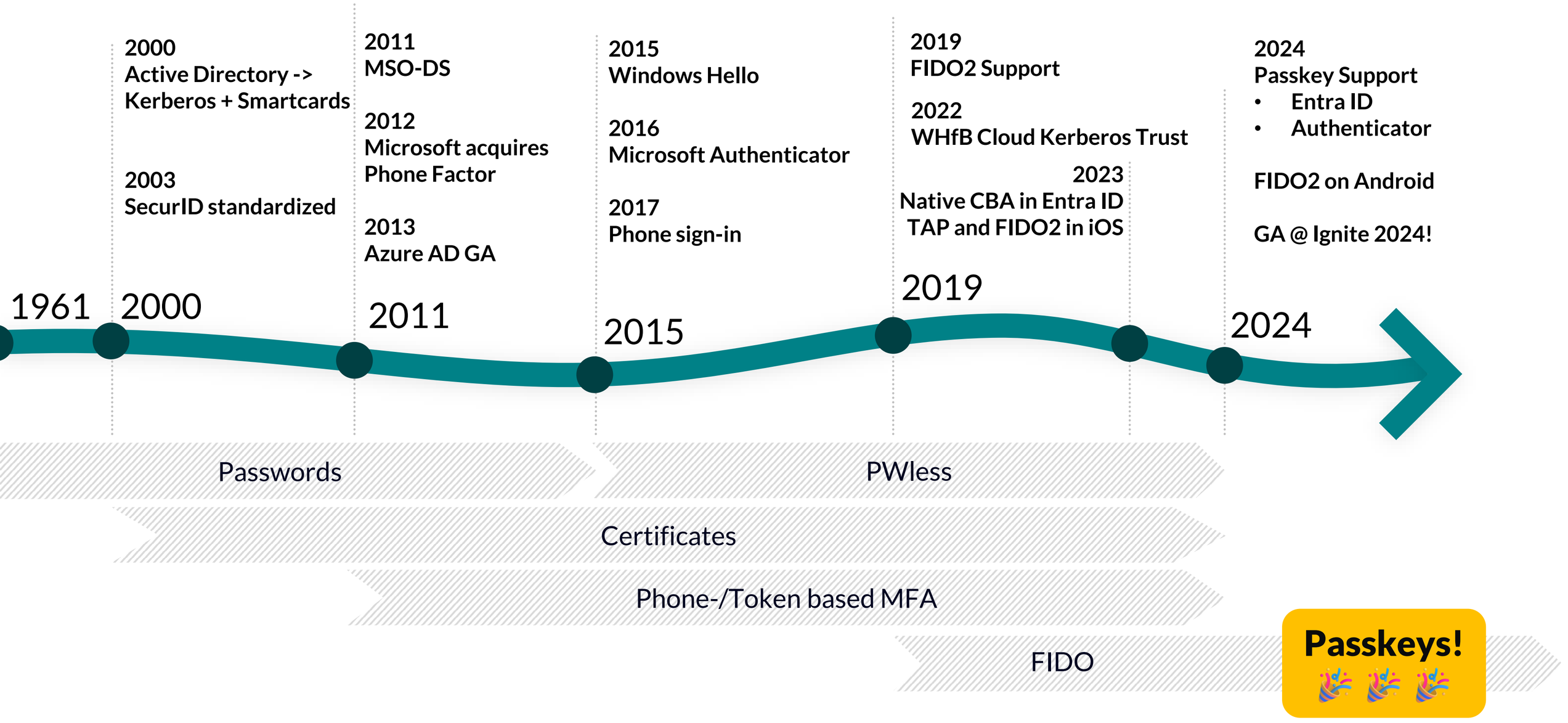
Fabian Bader & Christopher Brumm
Cyber Security Architects @ glueck kanja

About us…

Fabian Bader		Chris Brumm
old		very old
MVP		CISSP (and now also MVP)
@fabian_bader		@cbrhh
/in/fabianbader		/in/christopherbrumm
cloudbrothers.info		chris-brumm.com

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

Evolution of Authentication at Microsoft



Evolution of Authentication at Microsoft

2000
Active D
Kerberc

2003
SecurID

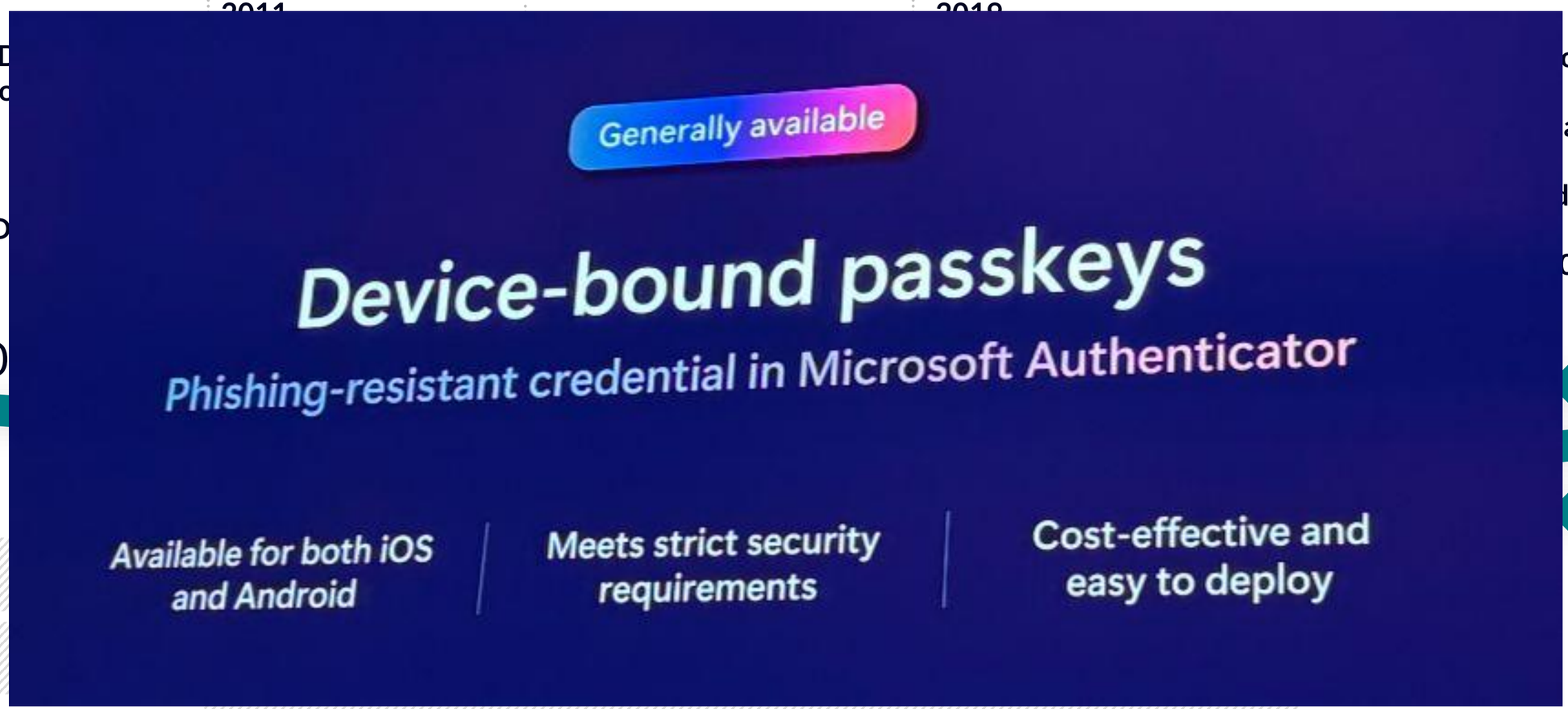
ort

ator

droid

024!

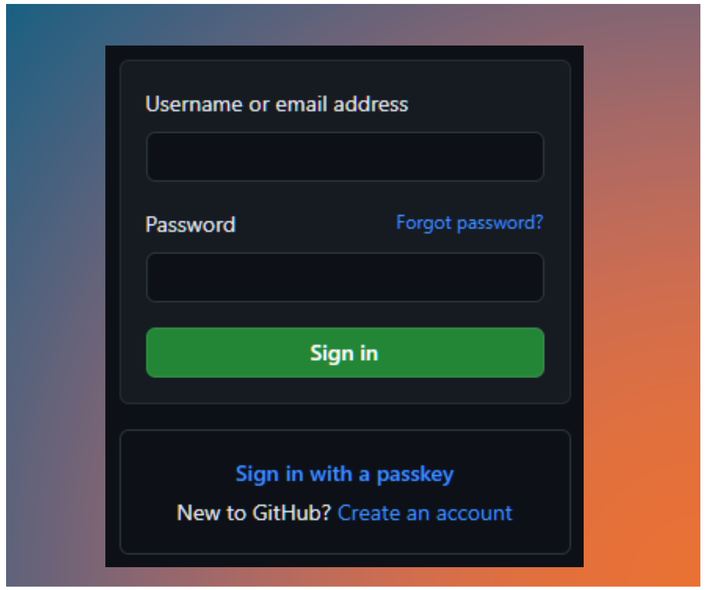
1961 2000

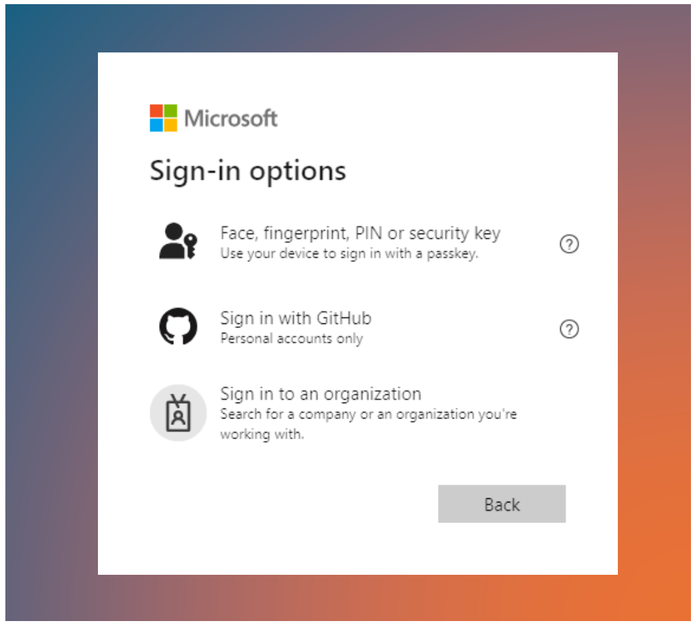


Phone-/Token based MFA

FIDO

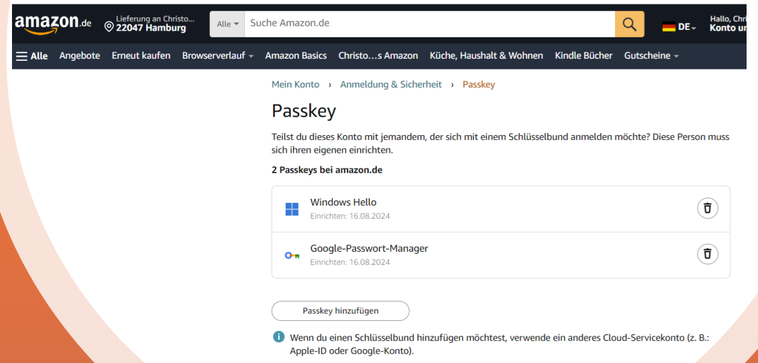
Passkeys! 🎉 🎉 🎉

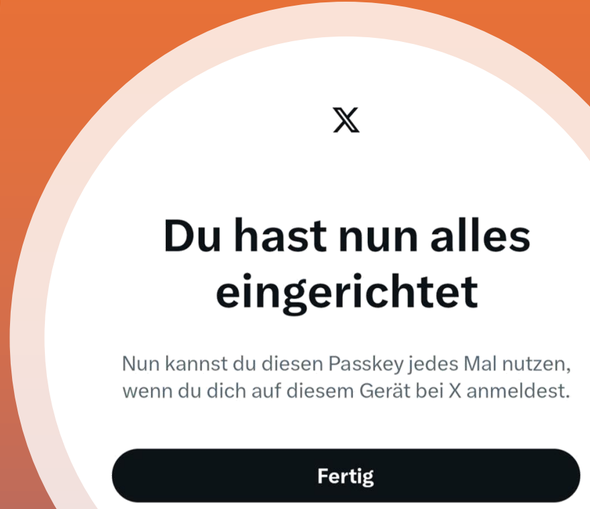


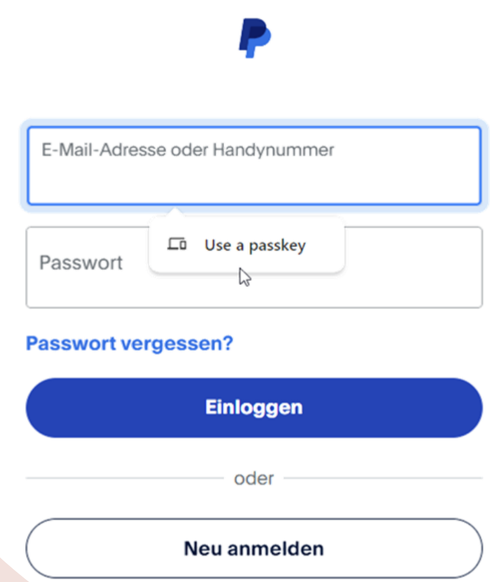


What's a passkey?

- 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

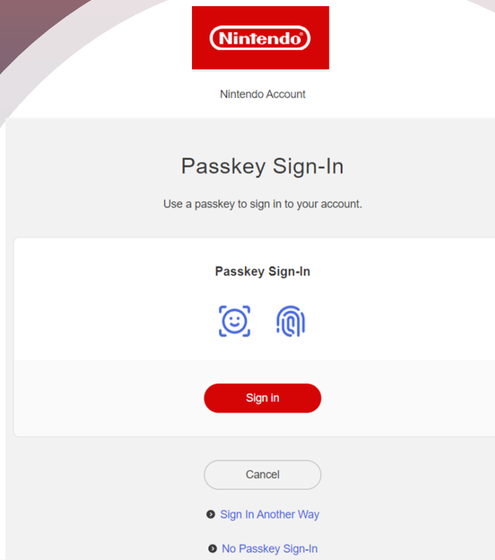






Passkeys used by Chris' family

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



Consumer want **easy** passkeys!

Synced Keys 🤗

Easy Recovery

Easy Setup

Phishing-resistance

Easy usage

Enterprises want **secure** passkeys!

Synced Keys 🧐

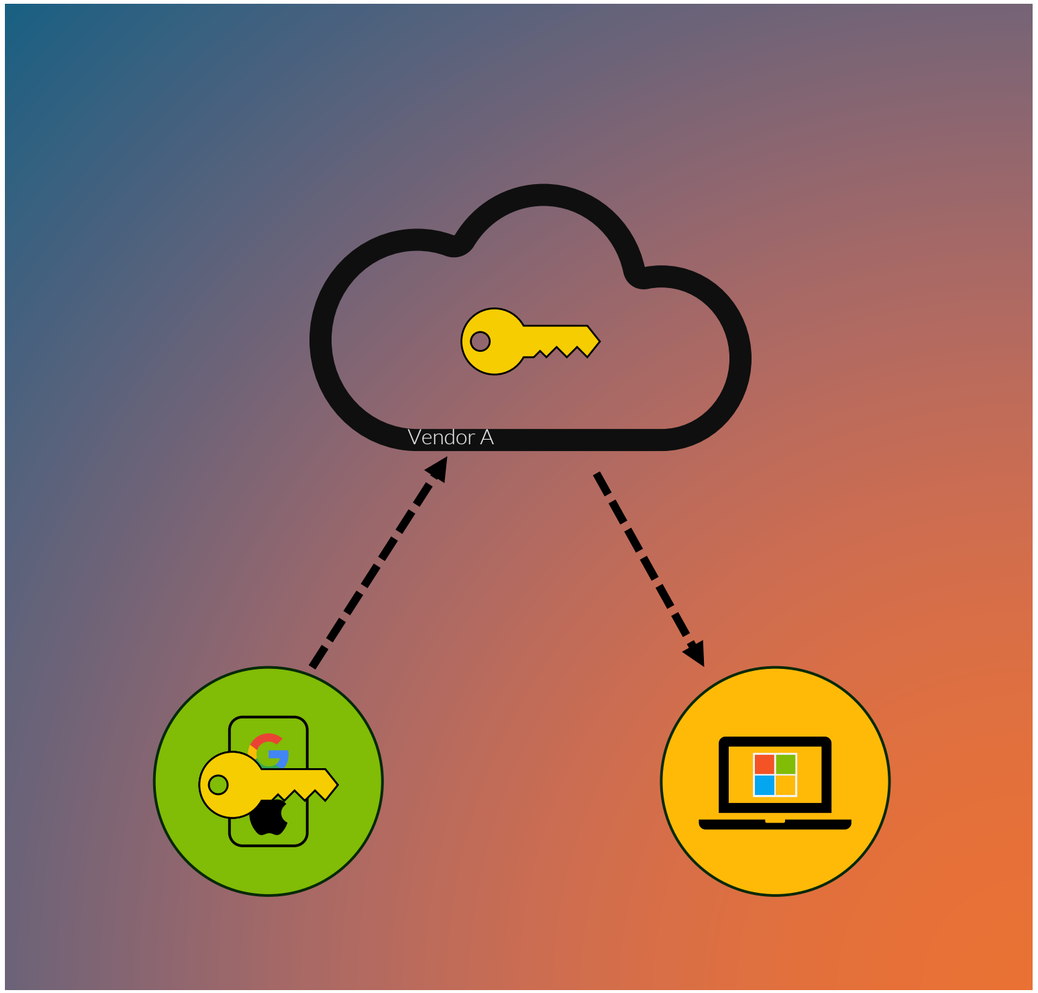
Secure Recovery

Controlled Setup

Phishing-resistance

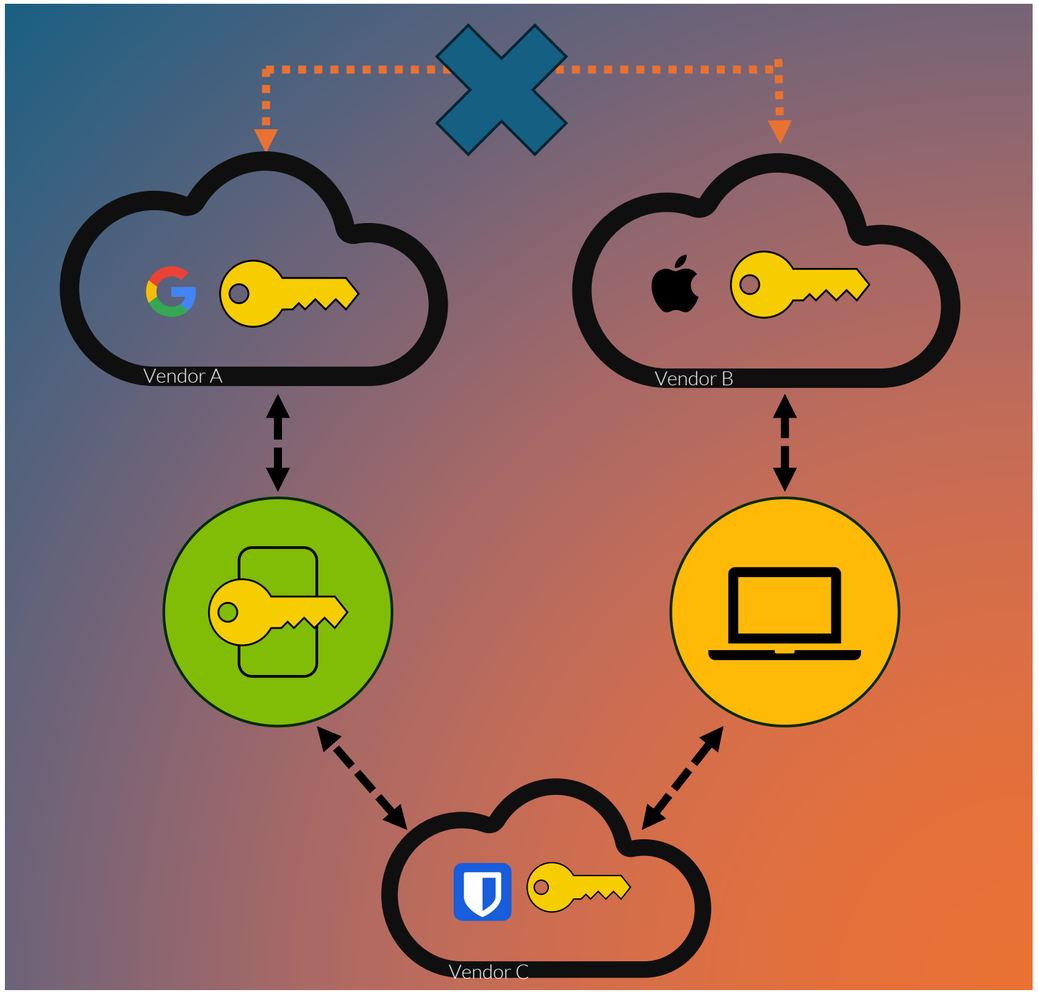
Controlled usage

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

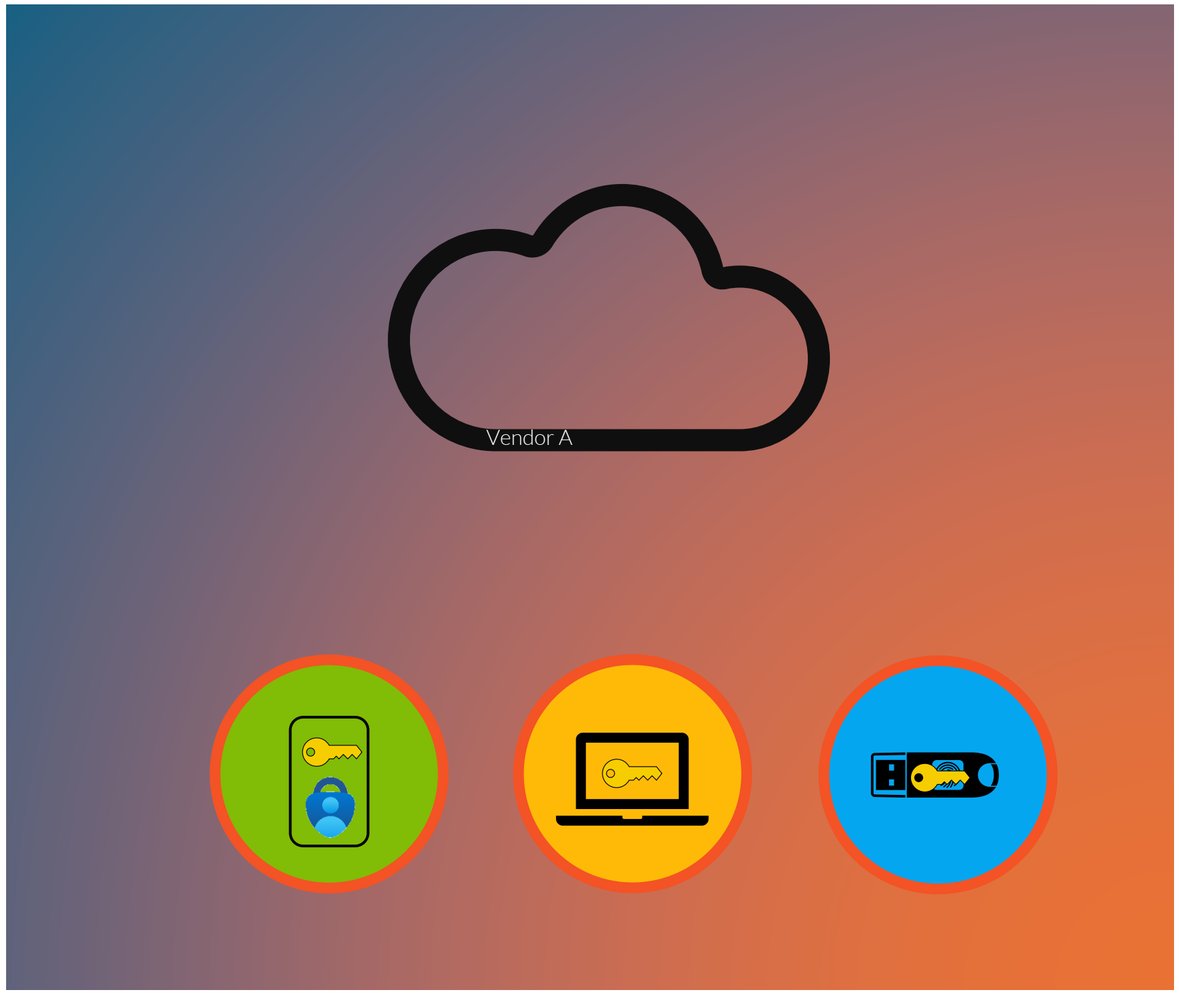
Synced vs. Device-bound passkeys



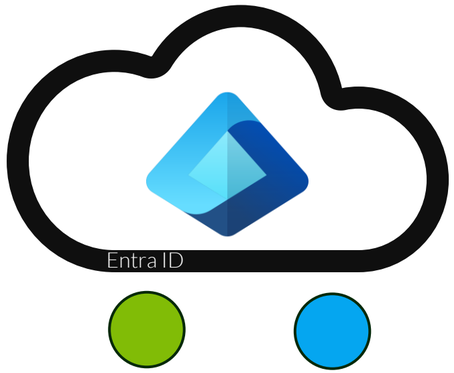
- Native cross vendor sync is not possible
- Workarounds
  - Cross-Device Authentication
  - Third-party passkey provider
  - Credential Exchange Protocol (CXP)

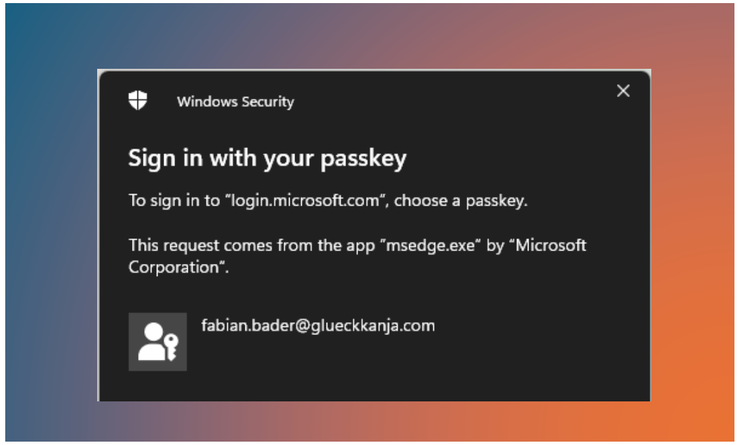
Synced vs. Device-bound passkeys

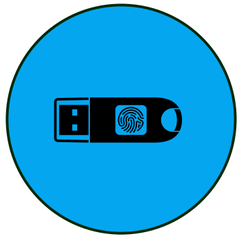
- The private key cannot leave the device
- FIDO2 security keys are device-bound passkeys
- Microsoft Authenticator creates a device-bound passkey
- Recovery = New Setup



Microsofts current implementation







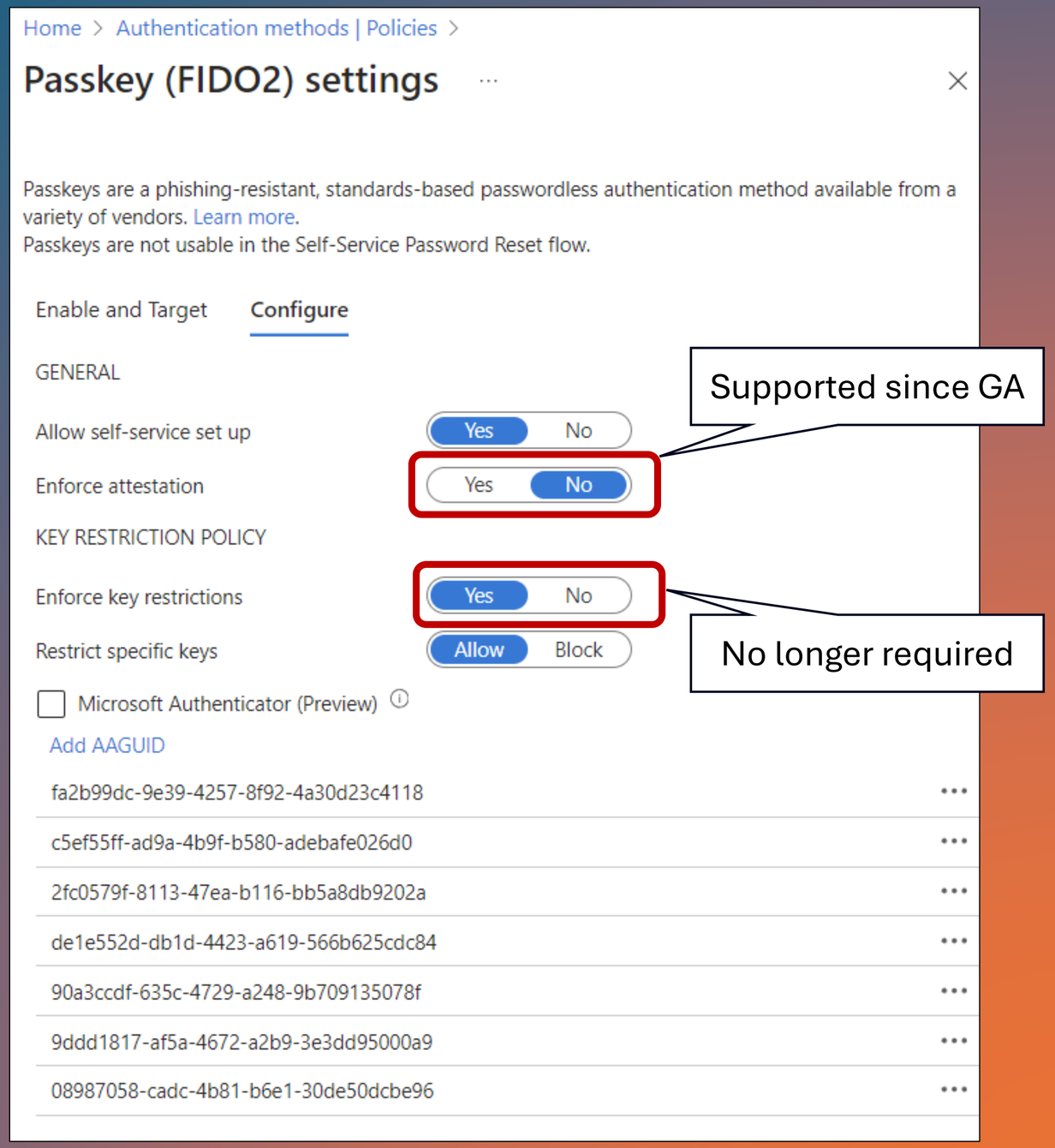
Auth Funnel - Thanks @merill

Authentication Methods available

Authentication Methods allowed for the user
Configured through Authentication Policies

Authentication methods registered by the user

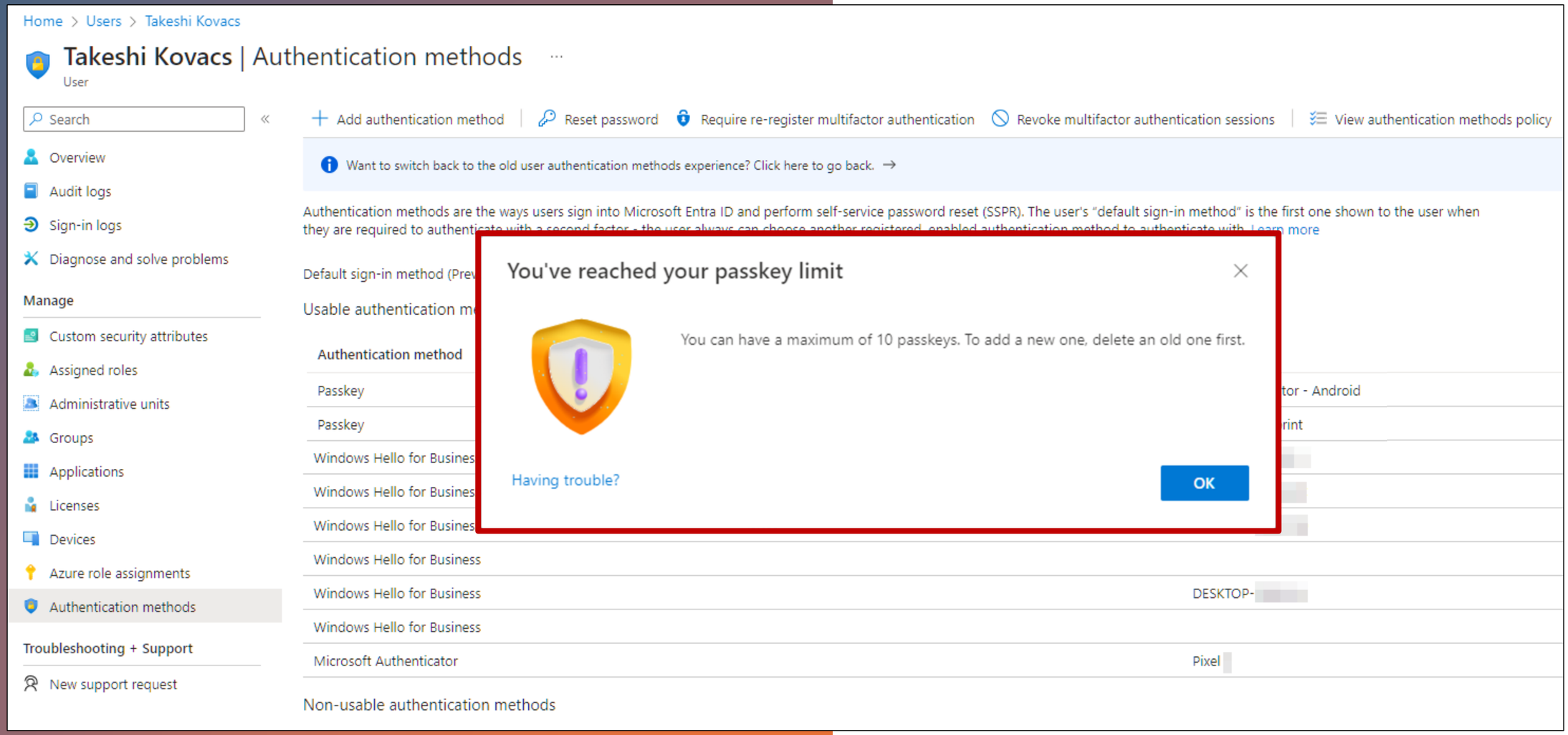
Authentication methods the user must use
Configured through authentication strengths

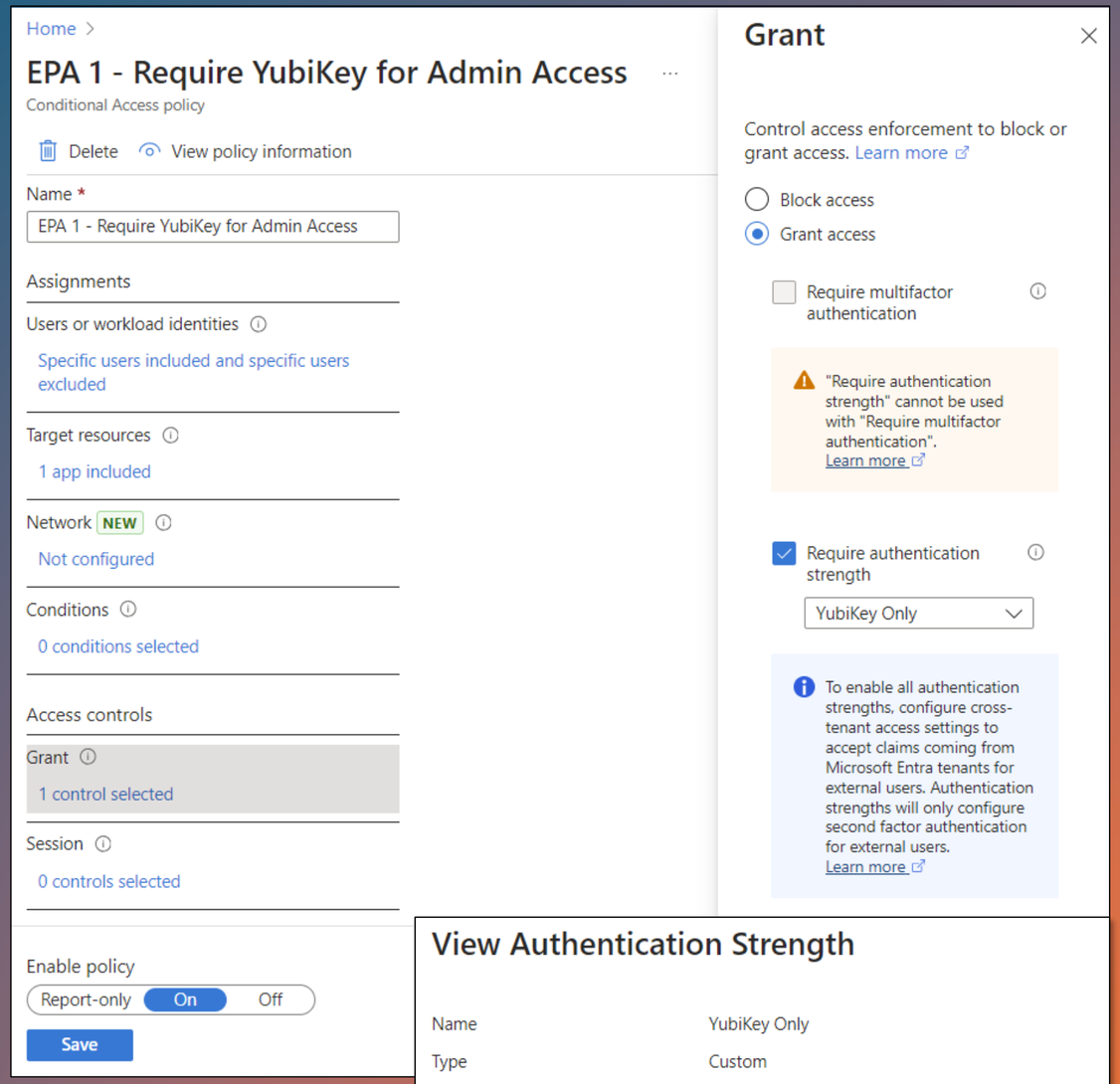


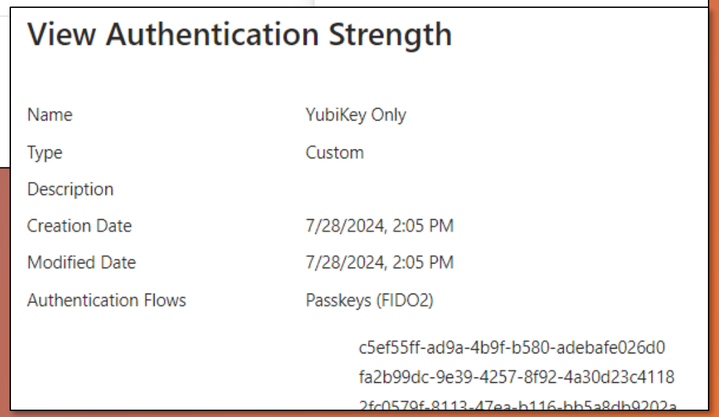
Authentication Methods allowed for the user
Configured through Authentication Policies

Define which Passkeys can be registered by your users

Authentication methods registered by the user







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

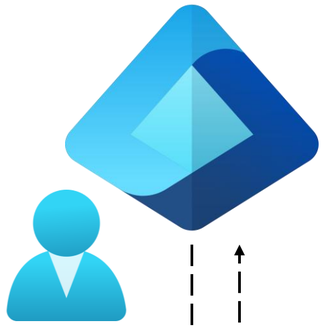
Attestion? AAGUID?

Authenticator Attestation GUID = AAGUID

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

3. Send signed public key to Entra ID

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



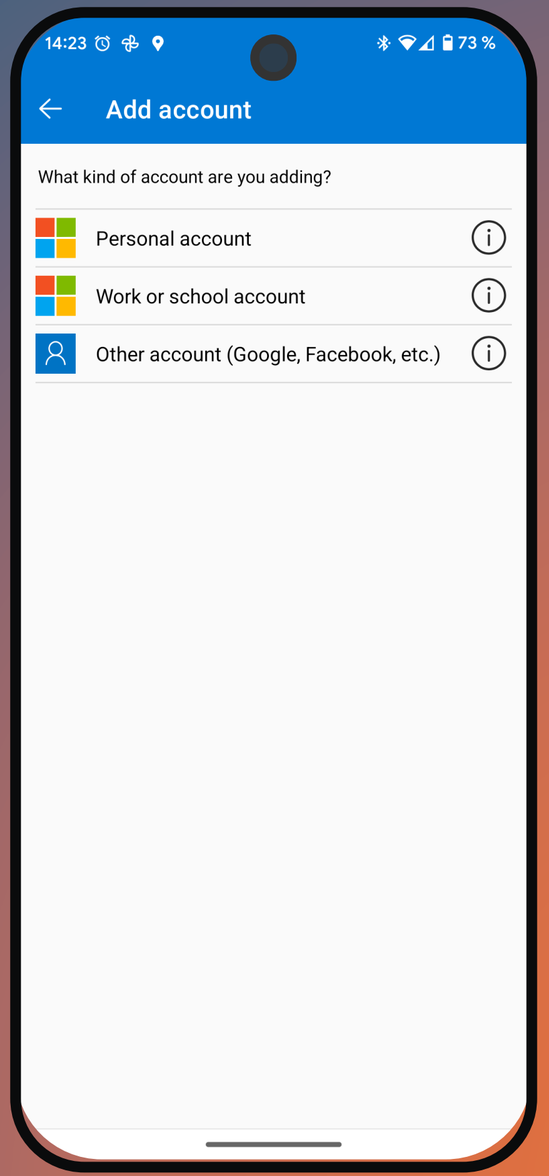
4. Request Certificate information from MDS
5. Validate signed public key
6. Store public key with user object

FIDO MDS

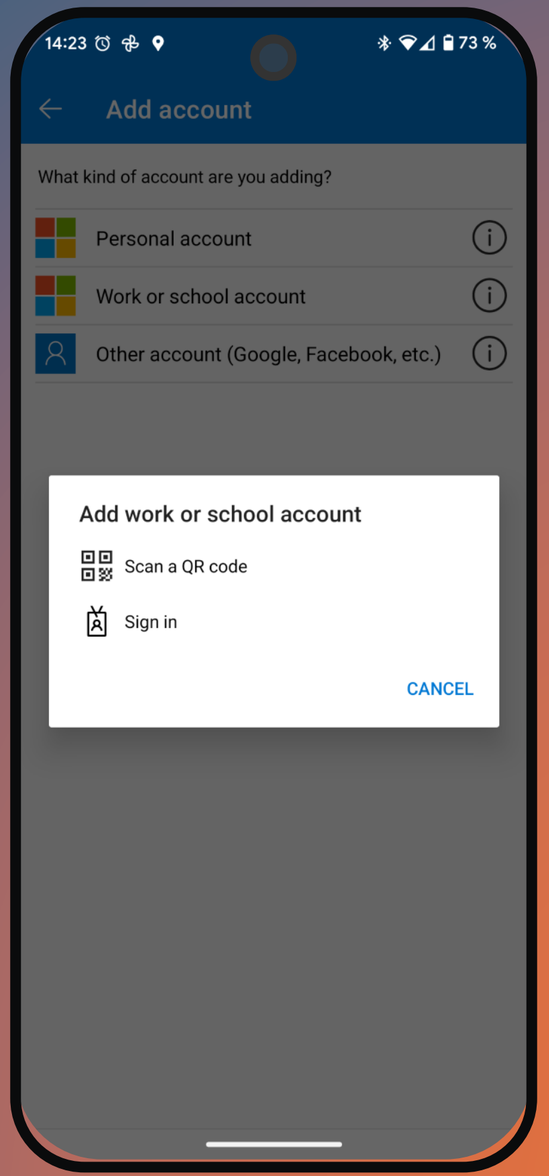
https://aaguid.nicolasuter.ch/
https://fidoalliance.org/fido-technotes-the-truth-about-attestation/

User experience in the lab

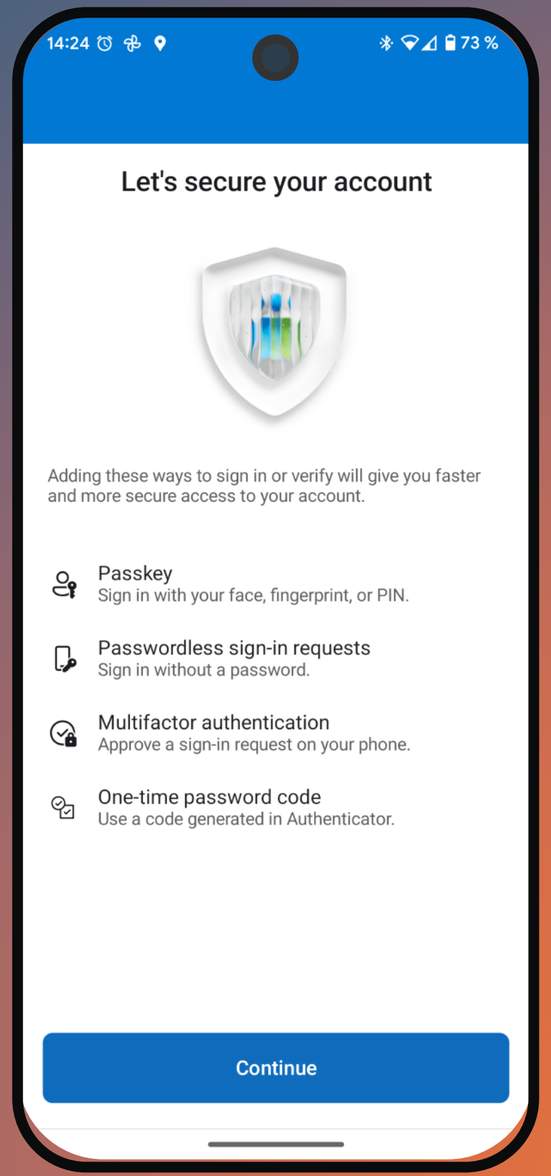
User experience in the lab



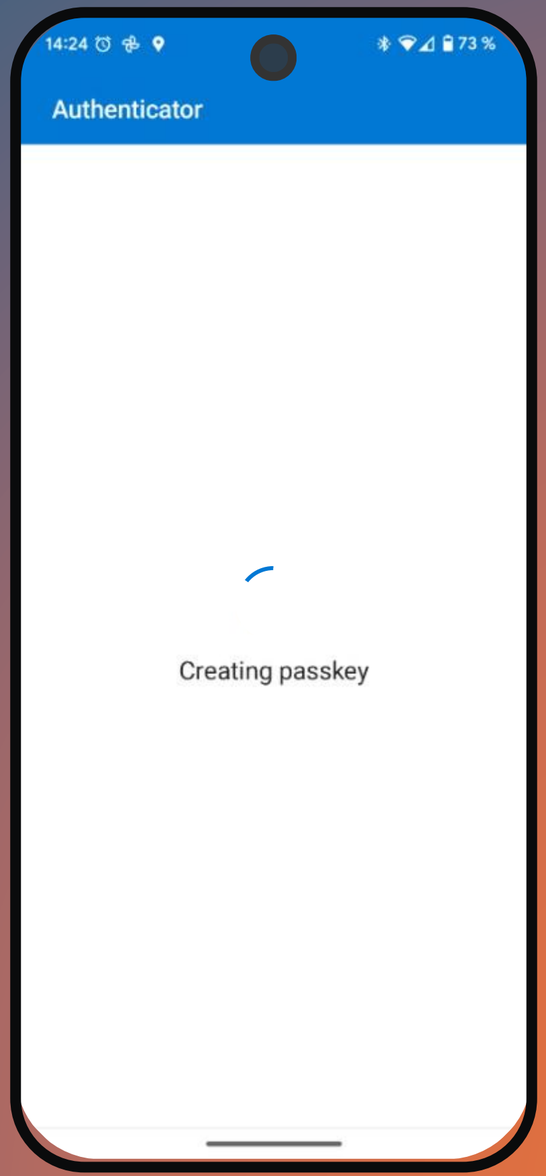
User experience in the lab



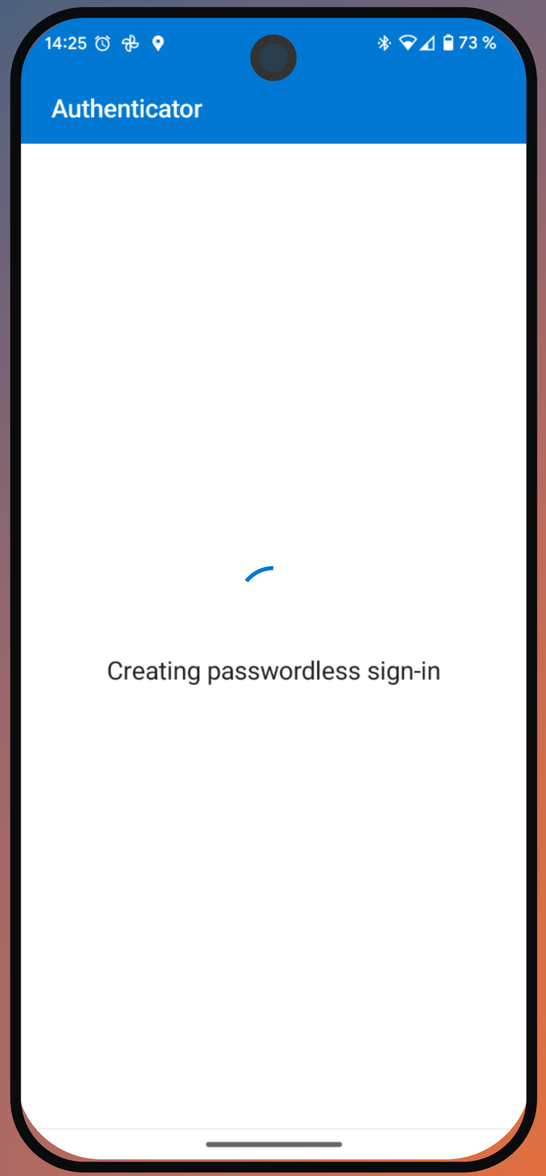
User experience in the lab



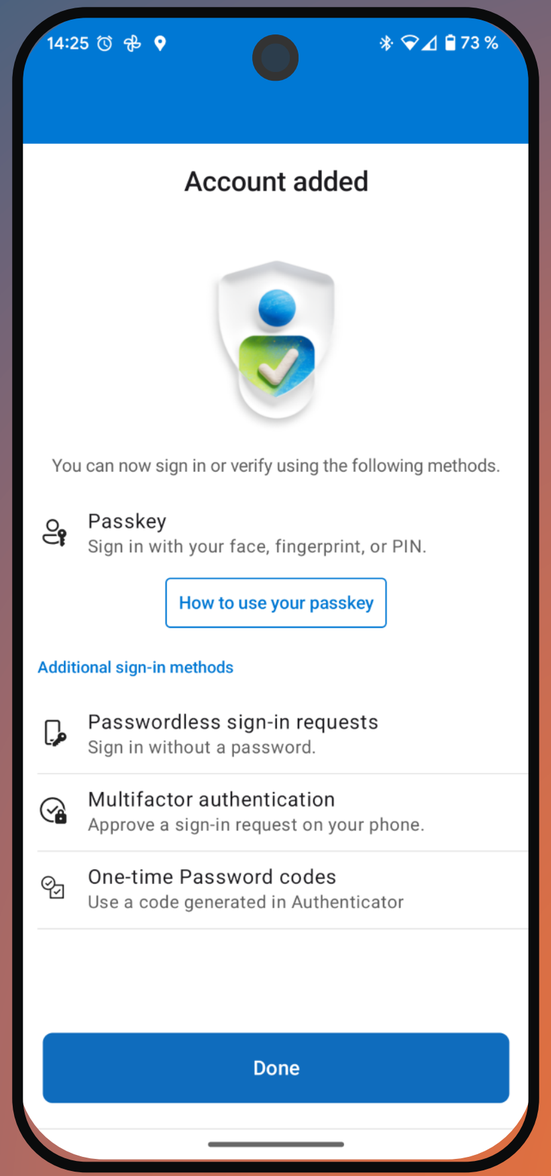
User experience in the lab



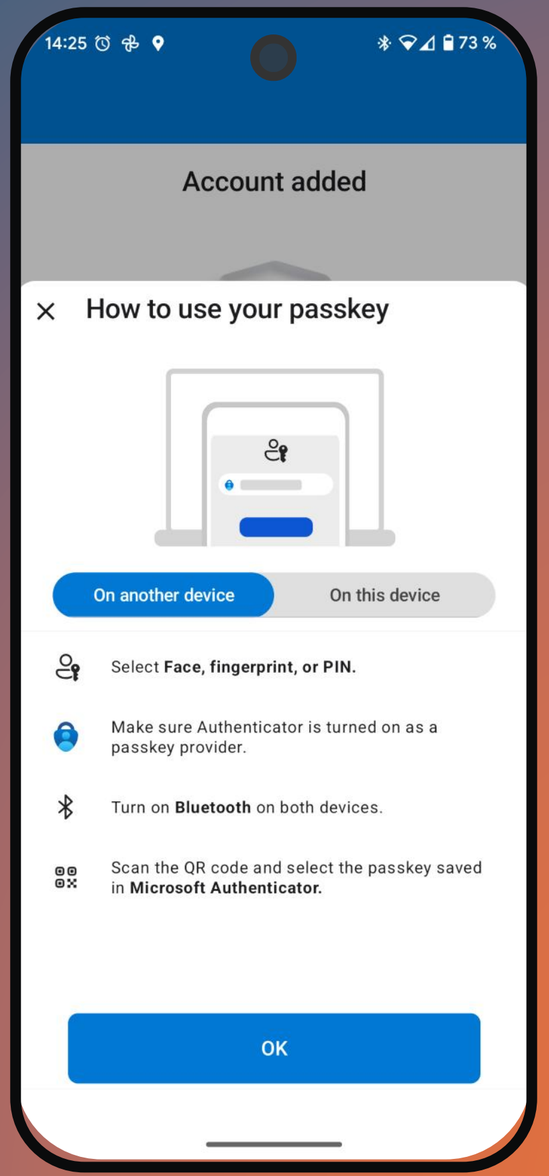
User experience in the lab



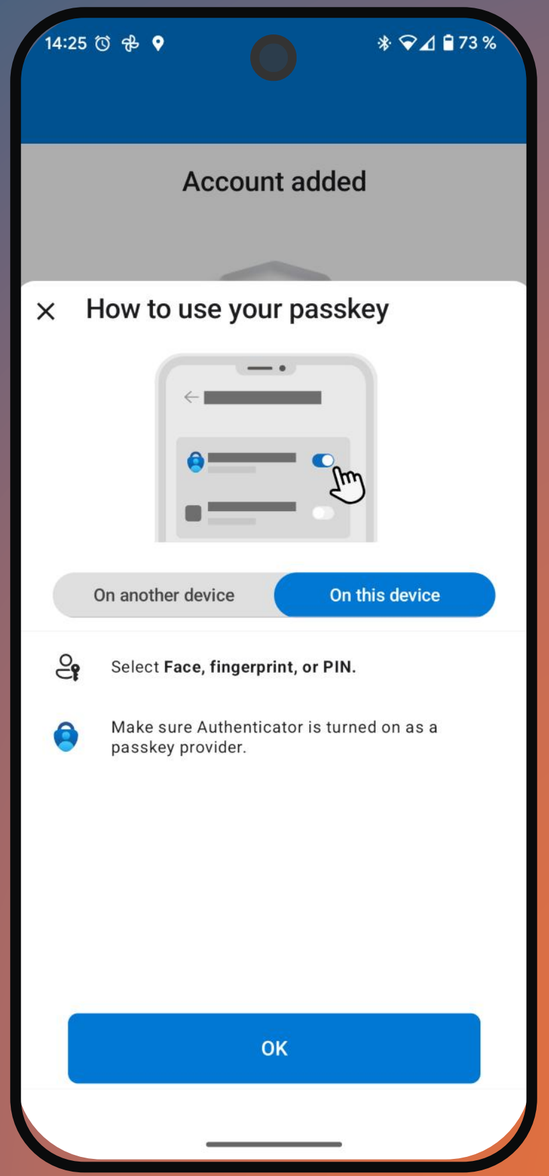
User experience in the lab



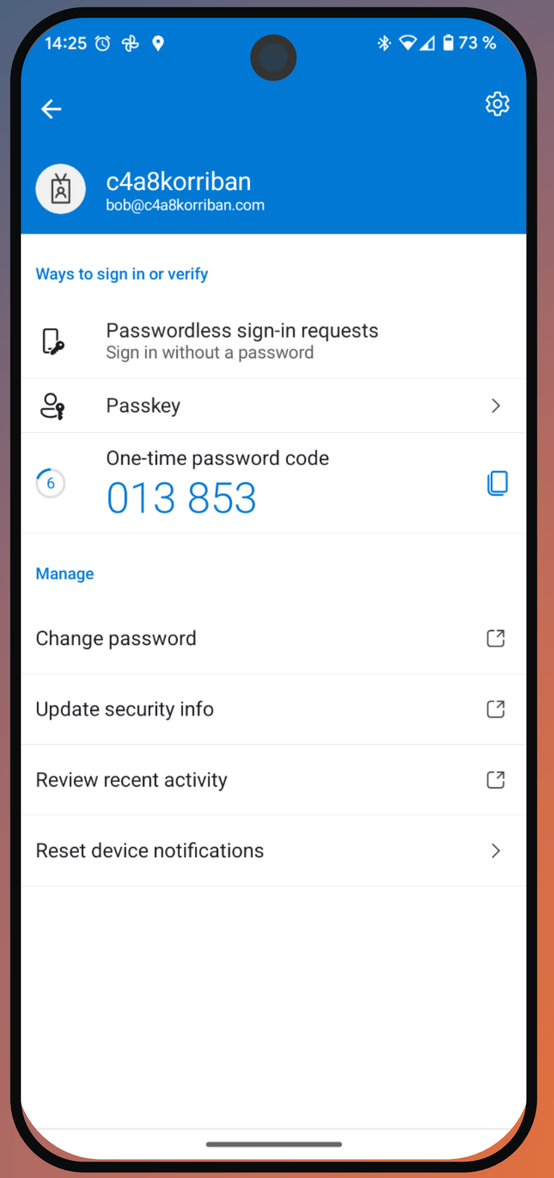
User experience in the lab



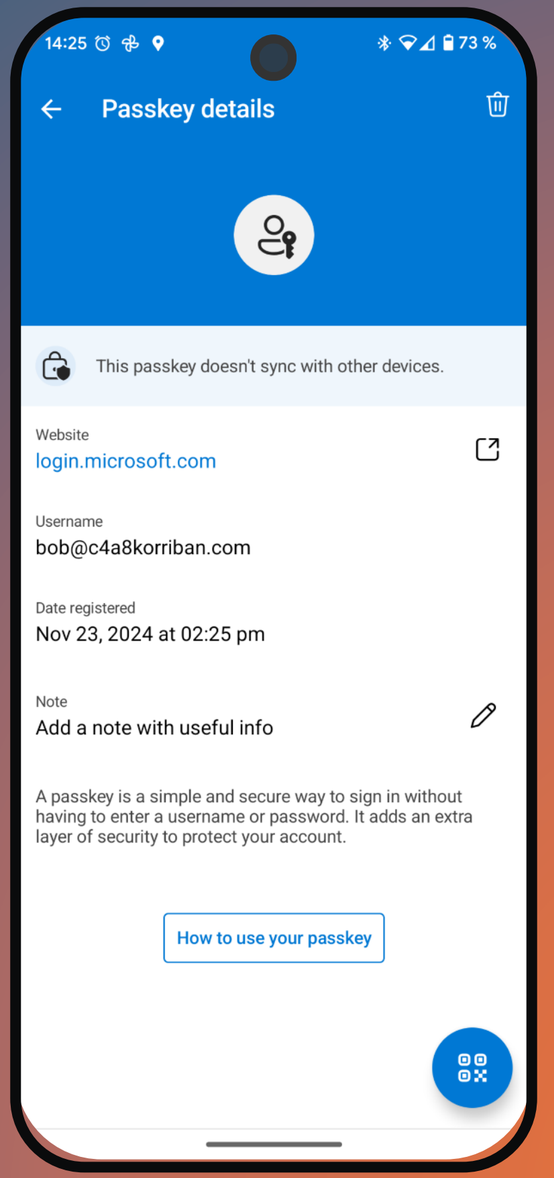
User experience in the lab



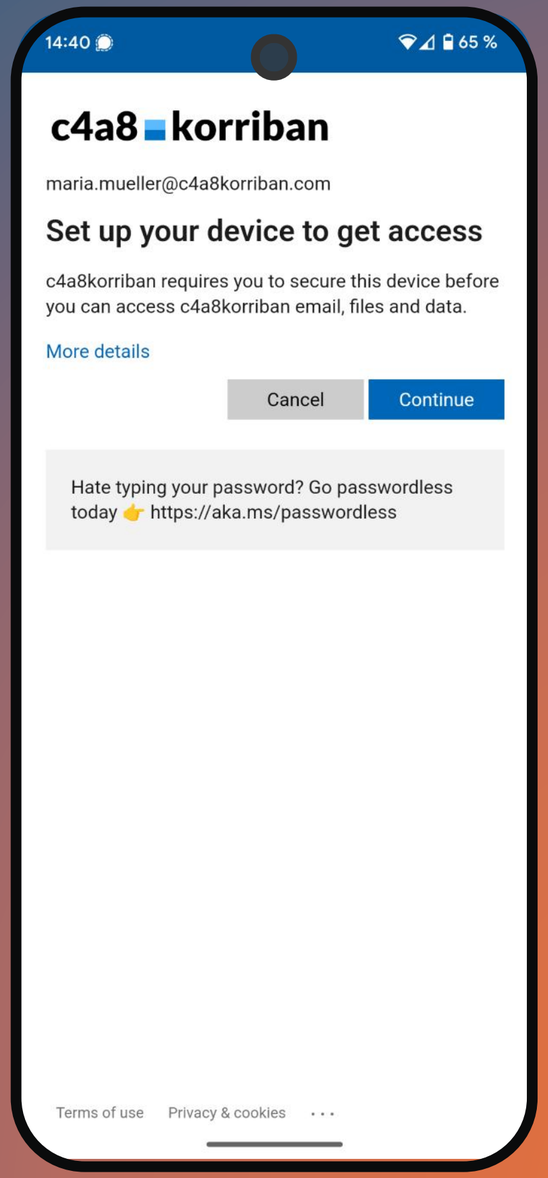
User experience in the lab



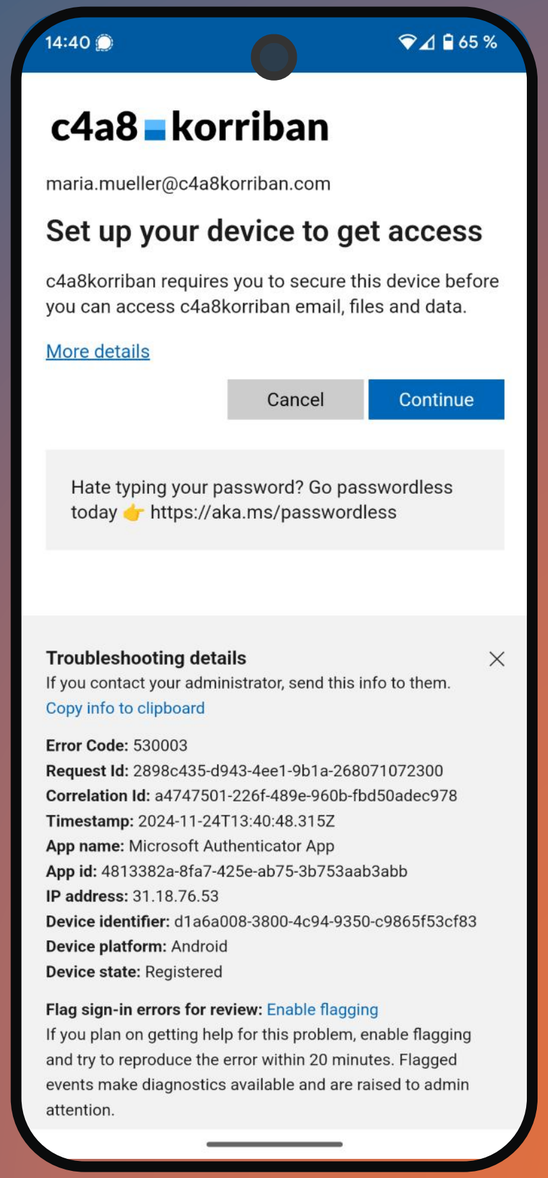
User experience in the lab



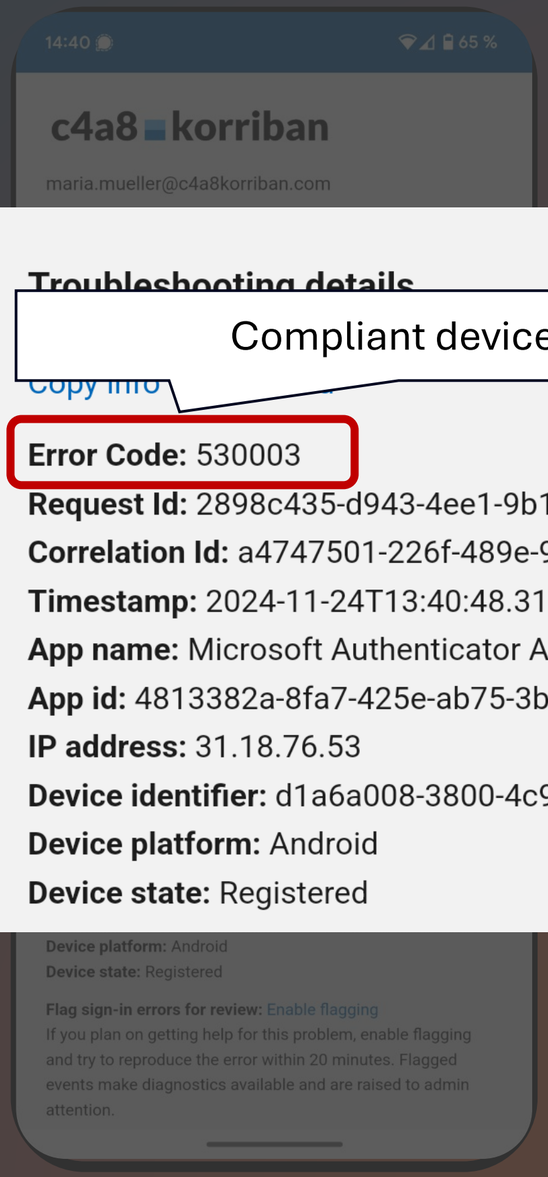
Experience in the real world



Experience in the real world



Experience in the real world

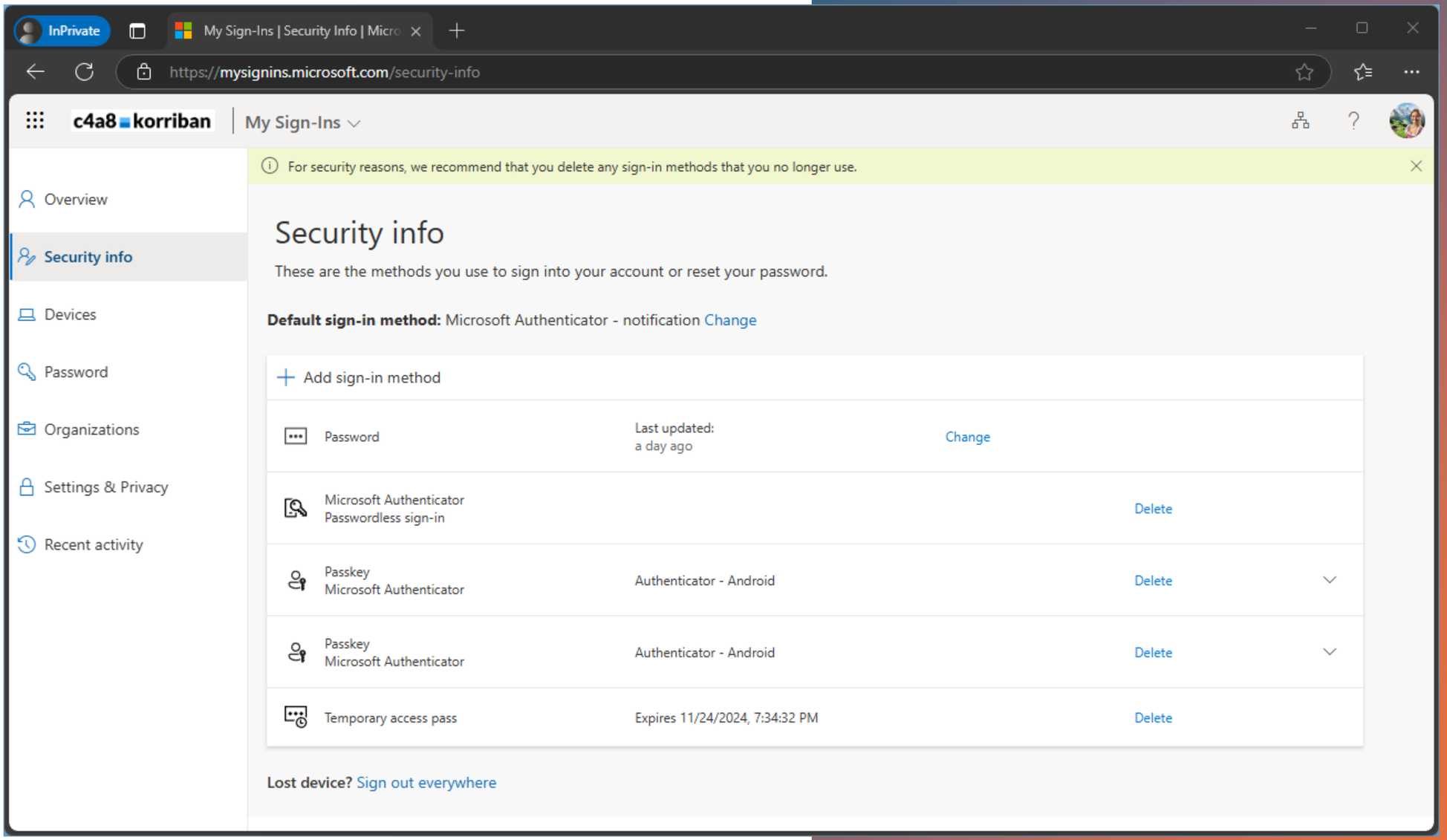


Troubleshooting details

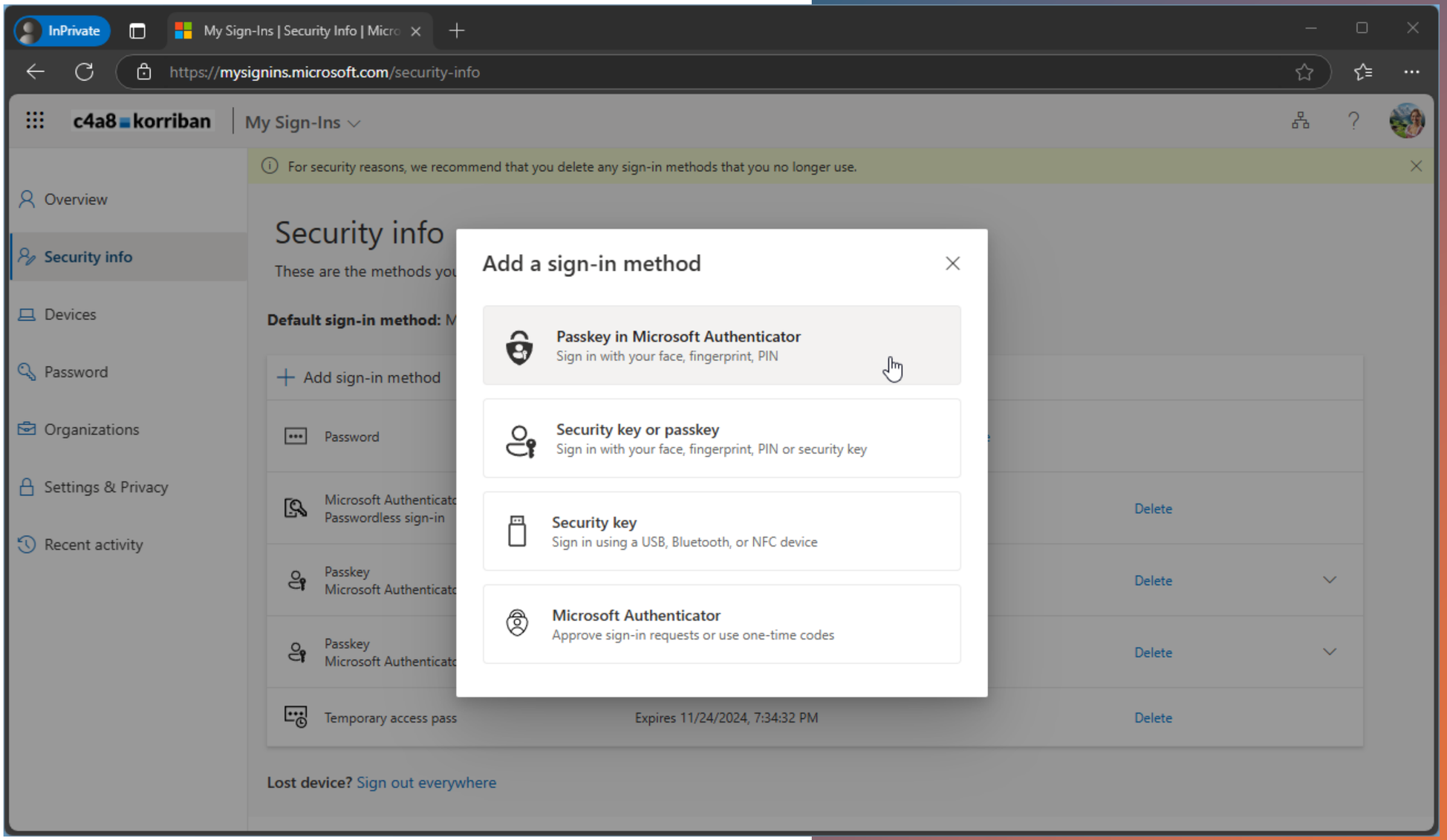
Approved app required

Error Code: 530021
Request Id: b4a6f0ec-b8e8-4d6b-a74b-fd02c4302100
Correlation Id: 68207782-d5b0-43c6-8d84-1d4ea94d41d1
Timestamp: 2024-11-24T17:34:53.085Z
App name: Microsoft Authenticator App
App id: 4813382a-8fa7-425e-ab75-3b753aab3abb
IP address: 31.18.76.53
Device identifier: d1a6a008-3800-4c94-9350-c9865f53cf83
Device platform: Android
Device state: Registered

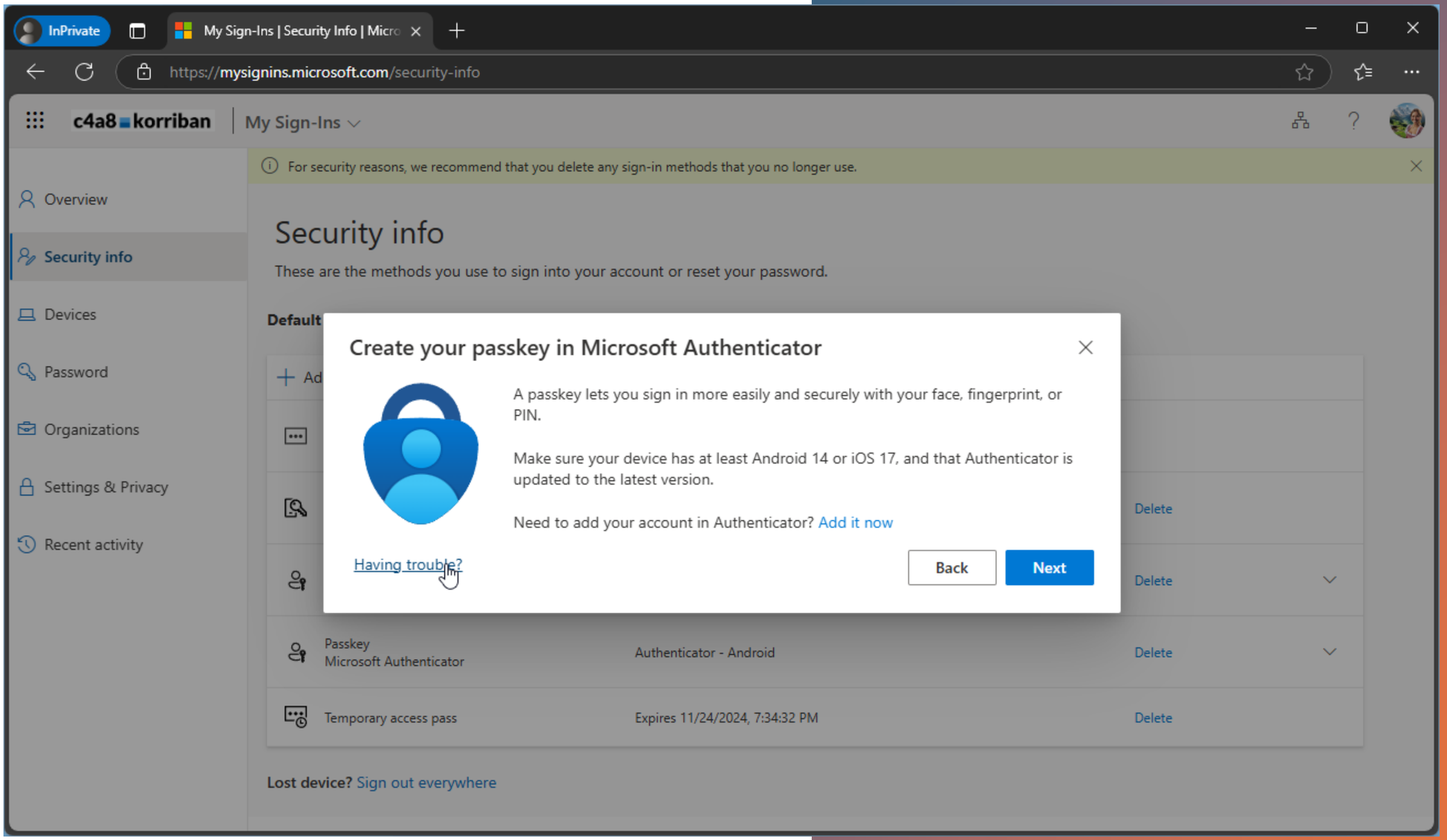
Cross Device Flow



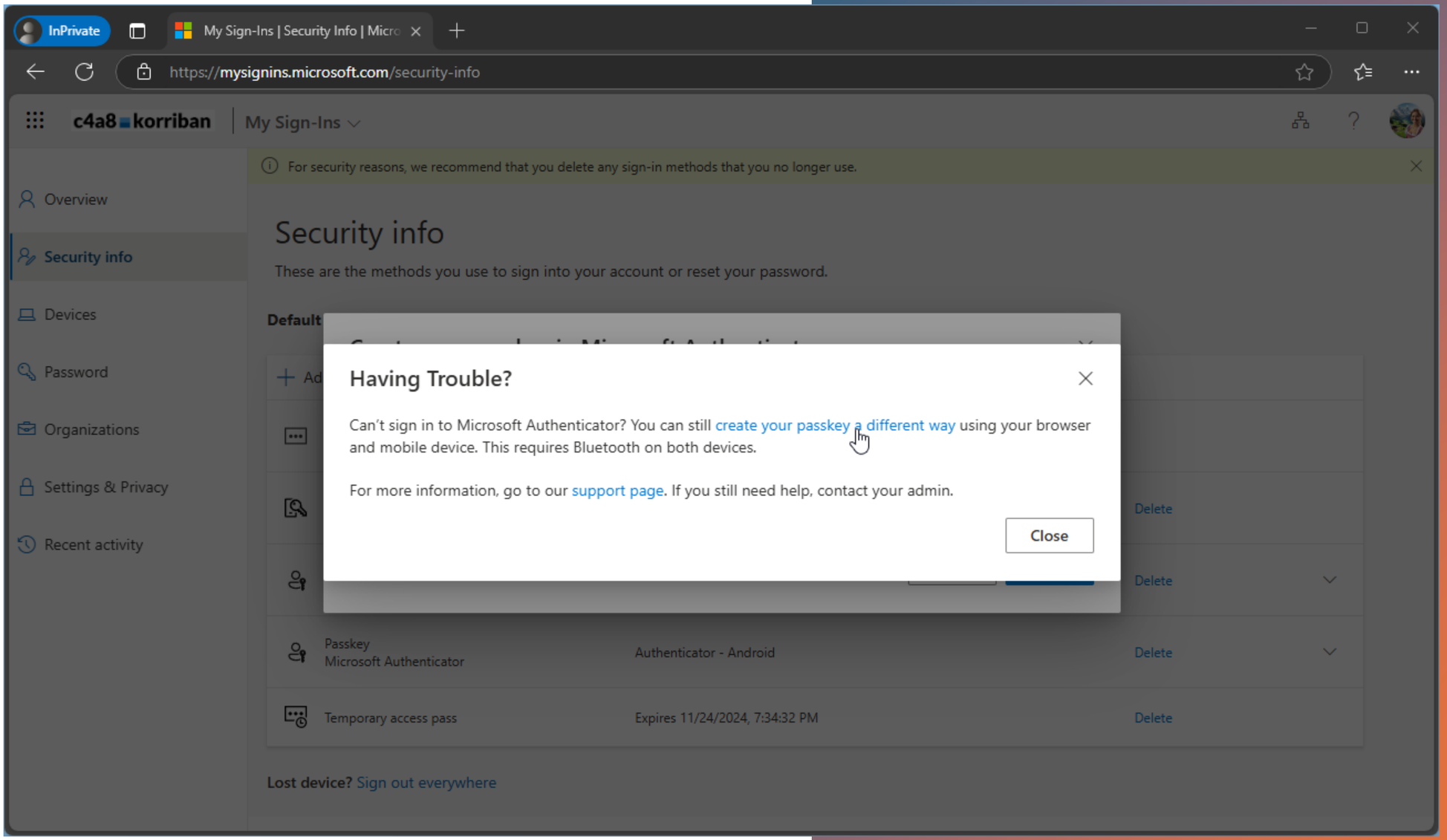
Cross Device Flow



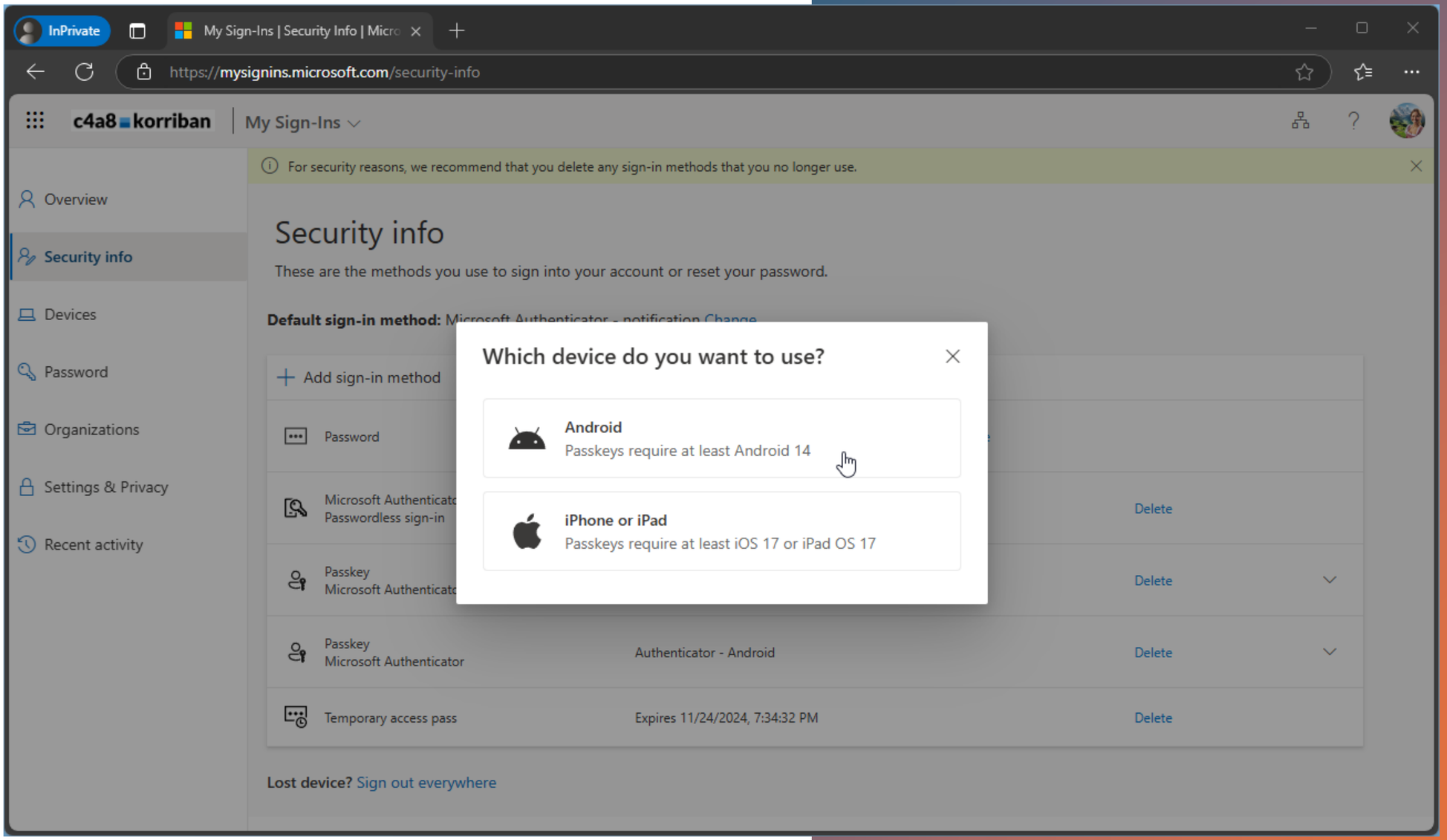
Cross Device Flow



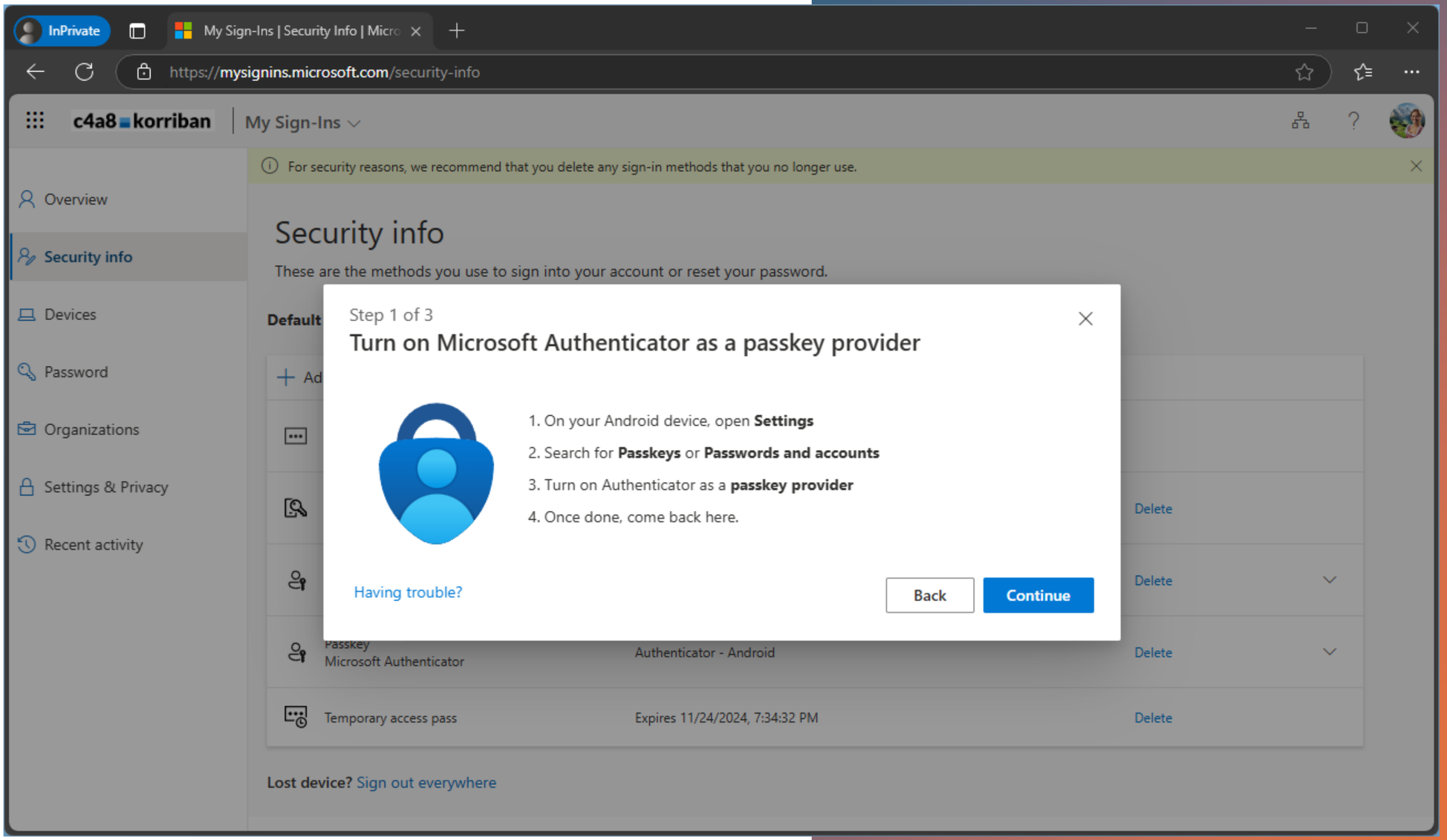
Cross Device Flow



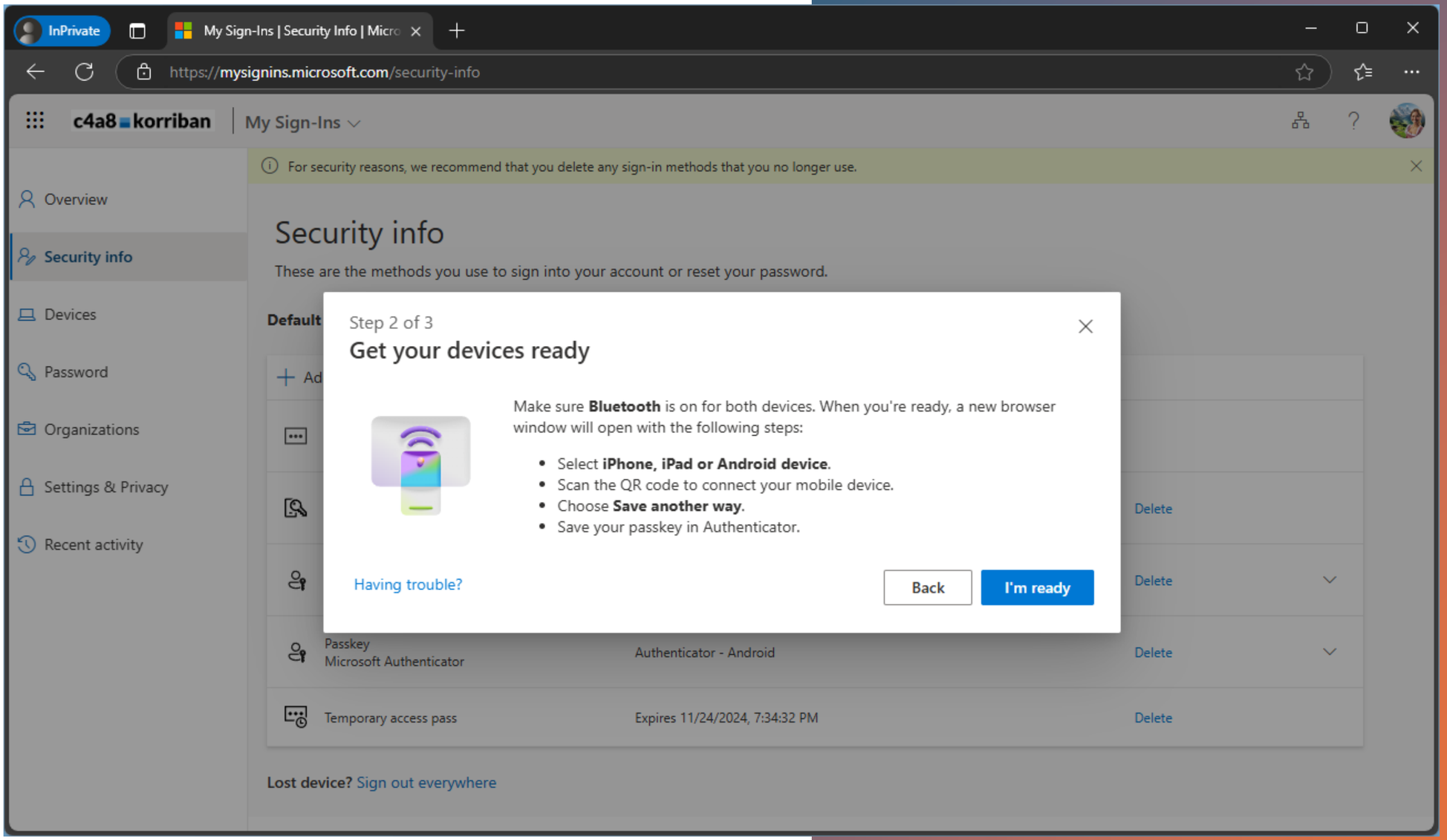
Cross Device Flow



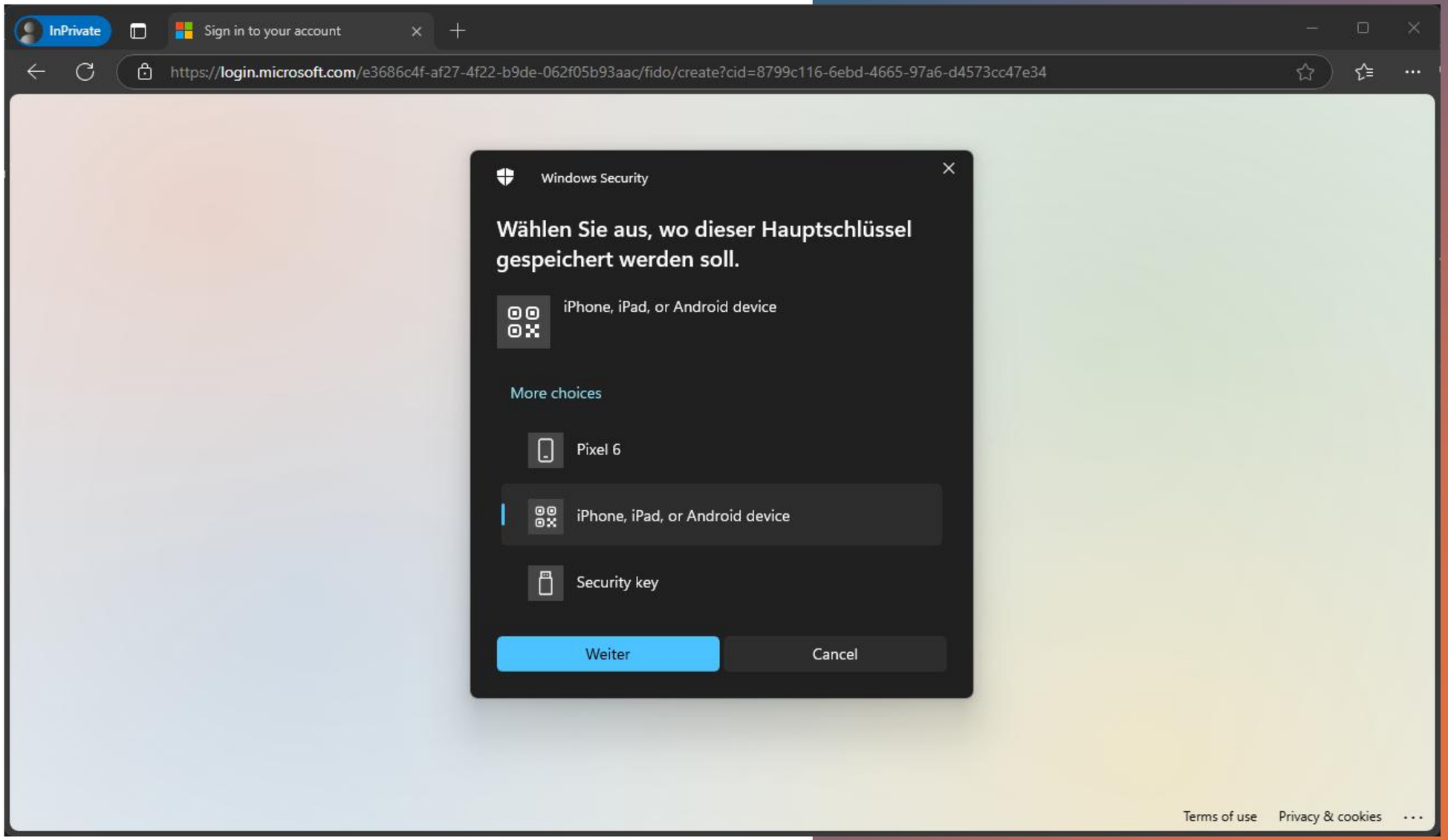
Cross Device Flow



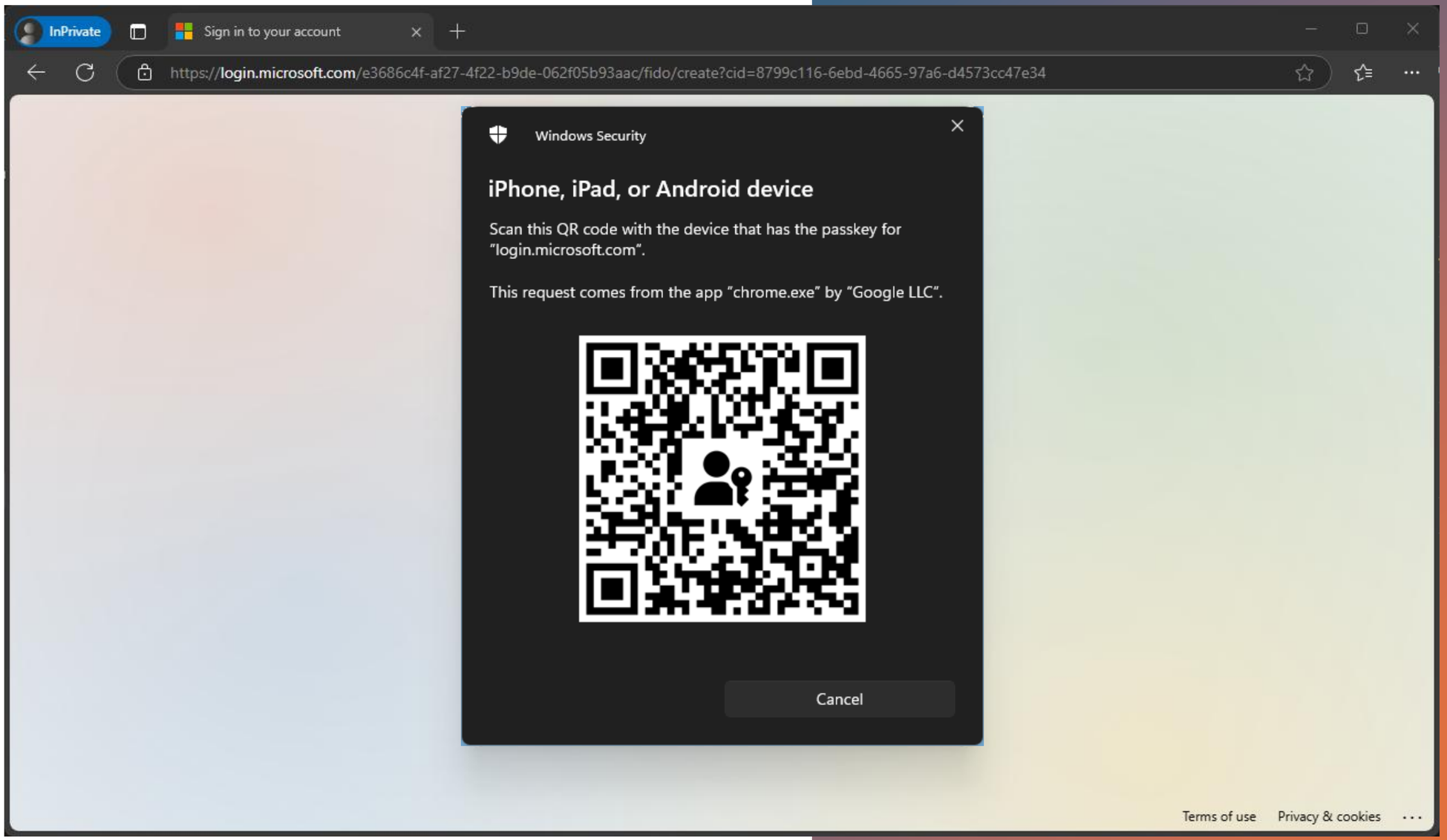
Cross Device Flow



Cross Device Flow



Cross Device Flow

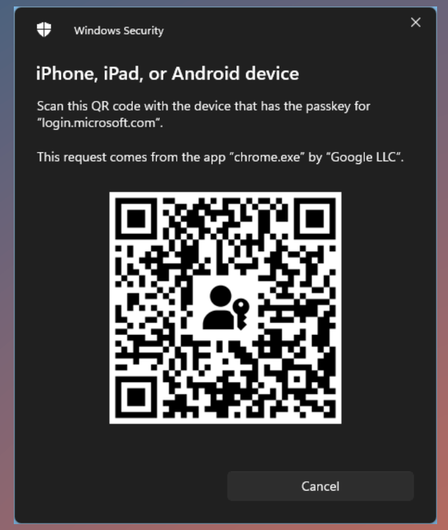


Maybe Cross-Device is not the answer…

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

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

QR Code Deep Dive

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

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

QR Code Deep Dive

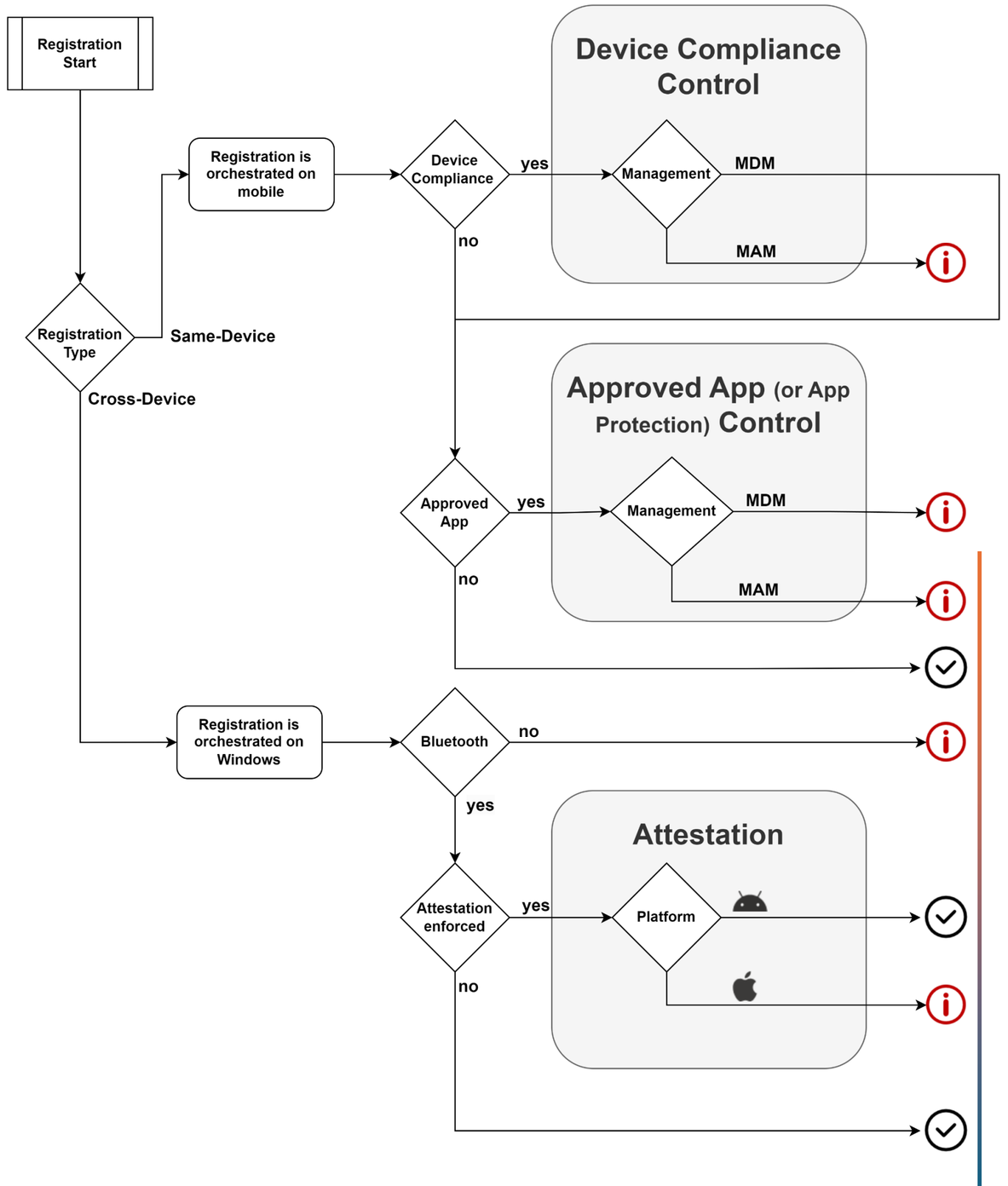
- Base10 encoded string
- Concise Binary Object Representation (CBOR) data format

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

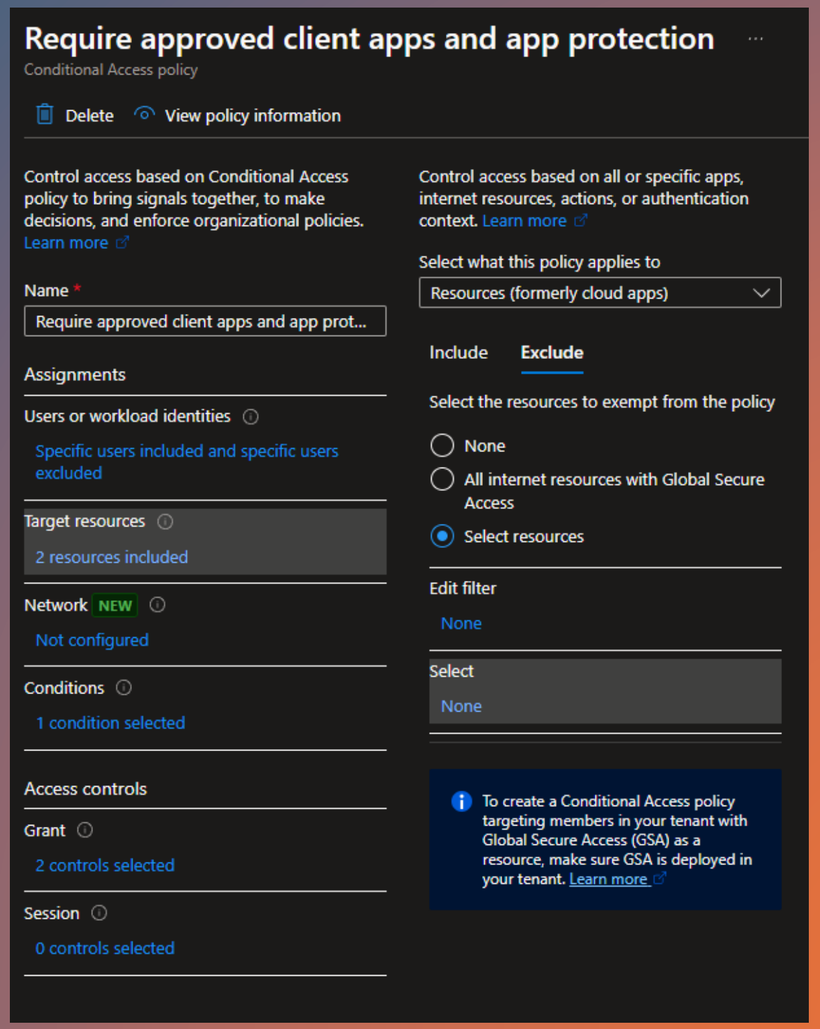
	Management	Conditional Access	BT	Method	Attestation	Result
	MAM	Compliant device: All resources		Same-Device	Yes/No	
	MAM	Compliant device: All resources		Cross-Device	Yes	
	MAM	Compliant device: All resources		Cross-Device	No	
	All	Approved apps: All resources		Same-Device	Yes/No	
	MAM	Approved apps: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

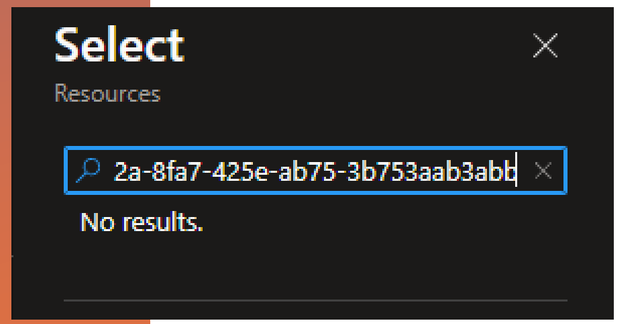
Passkey "support" matrix caveats

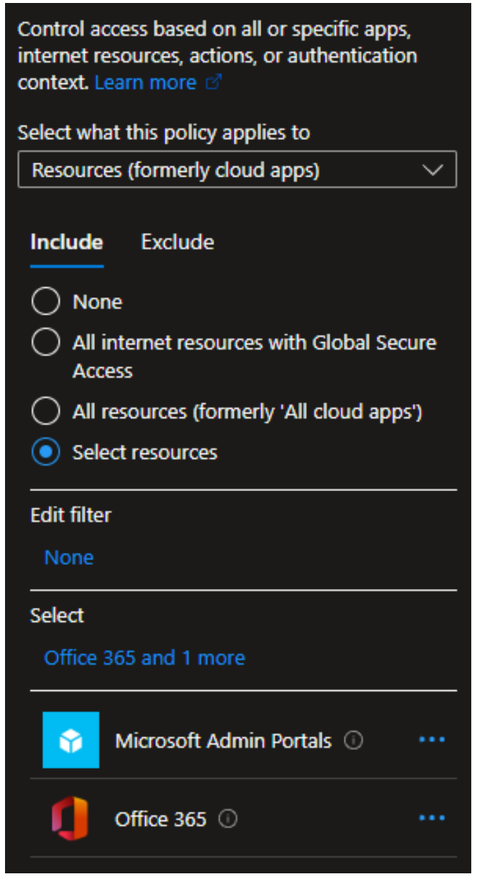
- Update to the latest OS version
- On Android also update the Play Service
  Settings → About phone → Android version → Google play system update
- On Android 14 the device vendor third party passkeys are optional
  - Not supported by e.g. Motorola, Fairphone, Oppo, Oneplus, Sony*

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

Workaround

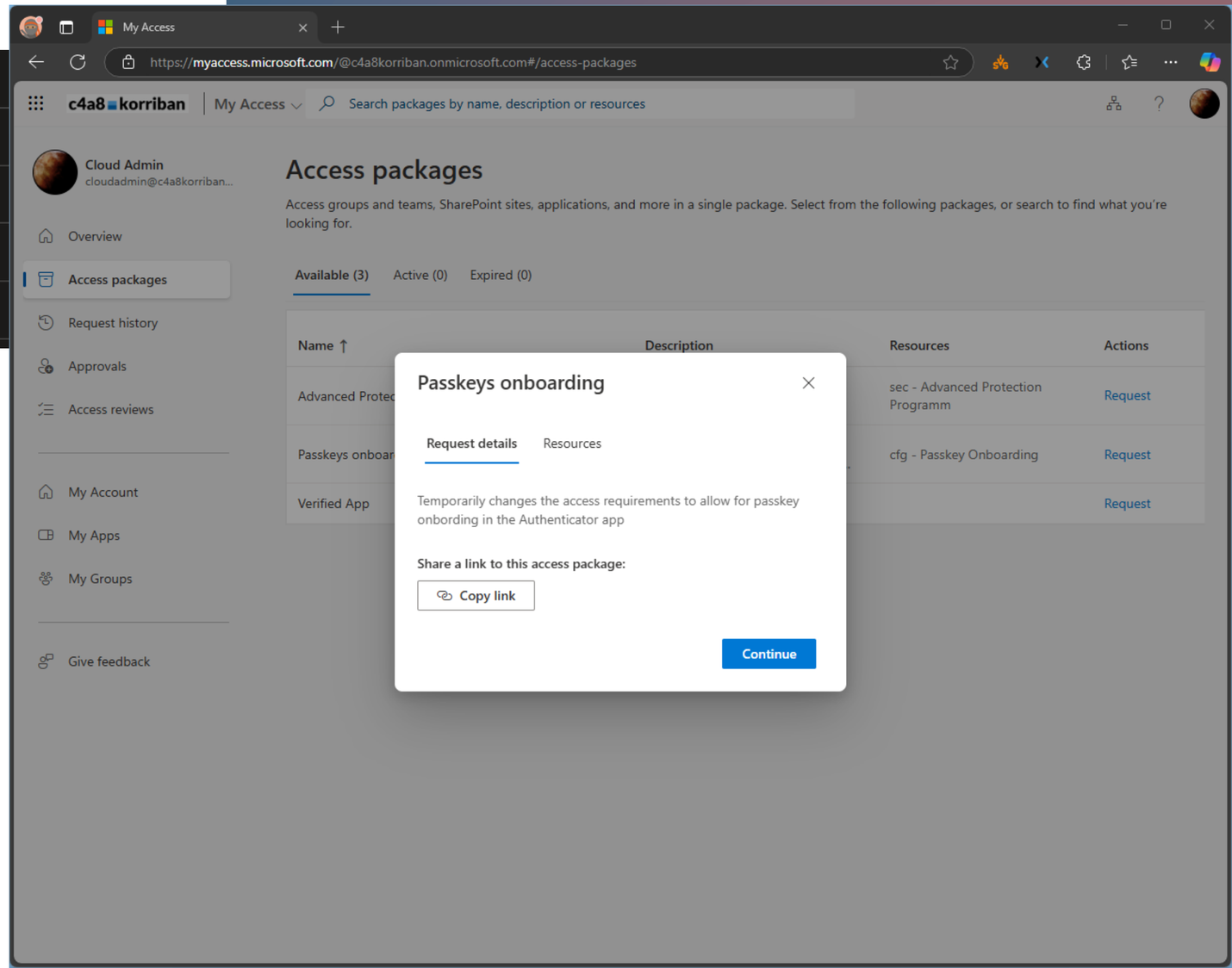

Require approved client apps and app protection
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
Require approved client apps and app prot...
Assignments
Users or workload identities
Specific users included and specific users excluded
Target resources
2 resources included
Network NEW
Not configured
Conditions
1 condition selected
Access controls
Grant
2 controls selected
Session
0 controls selected
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
Select the resources to exempt from the policy
None
All internet resources with Global Secure Access
Select resources
Edit filter
None
Select
None
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


Select
Resources
2a-8fa7-425e-ab75-3b753aab3abb
No results.


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
Office 365

Workaround

Policy name
Require approved client apps and app protection
Require approved client apps and app protection for passkey onboarding
Require compliant or hybrid Azure AD joined device for some users
Require compliant or hybrid Azure AD joined device for some users for passkey onboarding



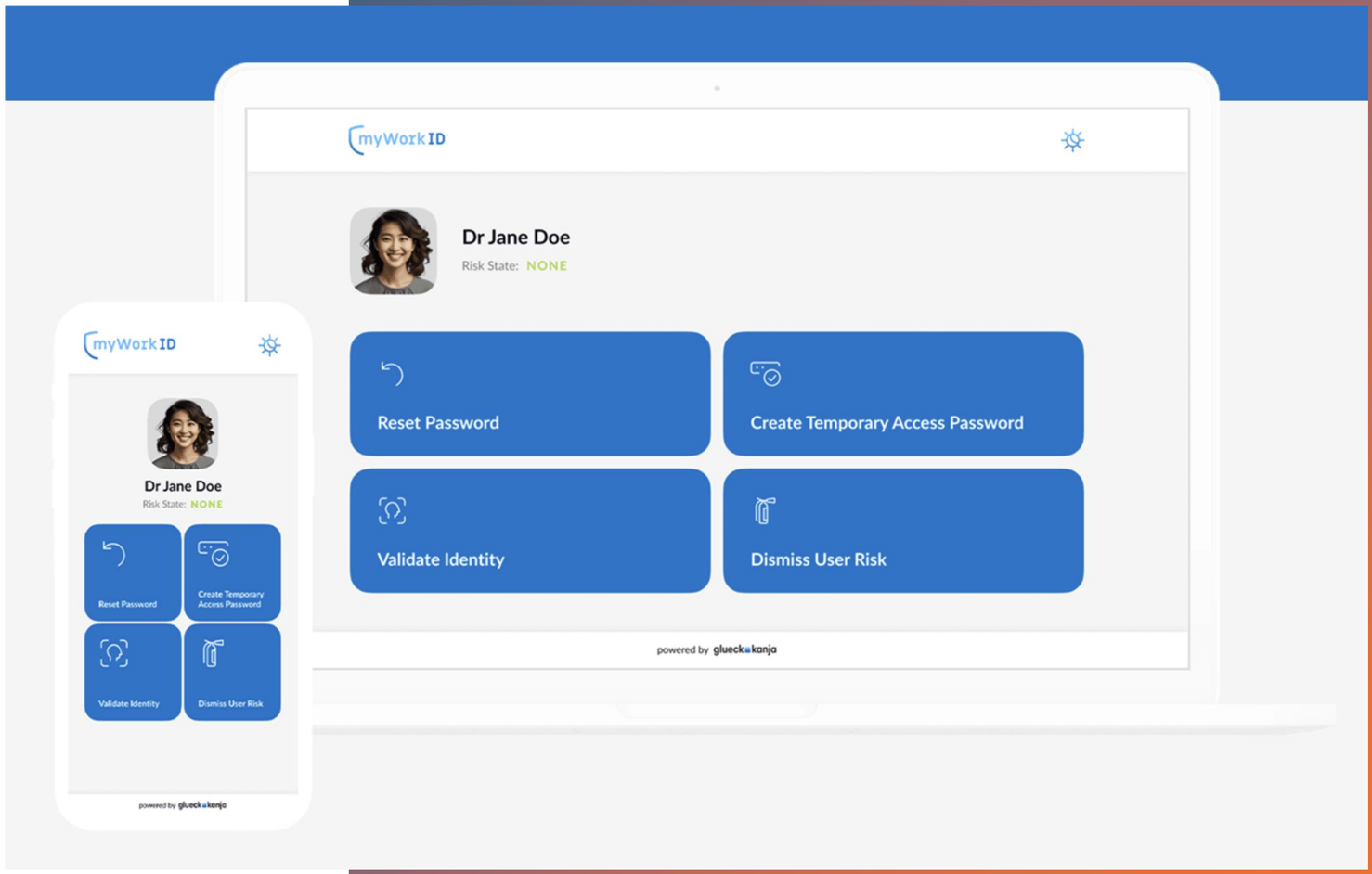
Our best practices and tips

- ☑ 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!

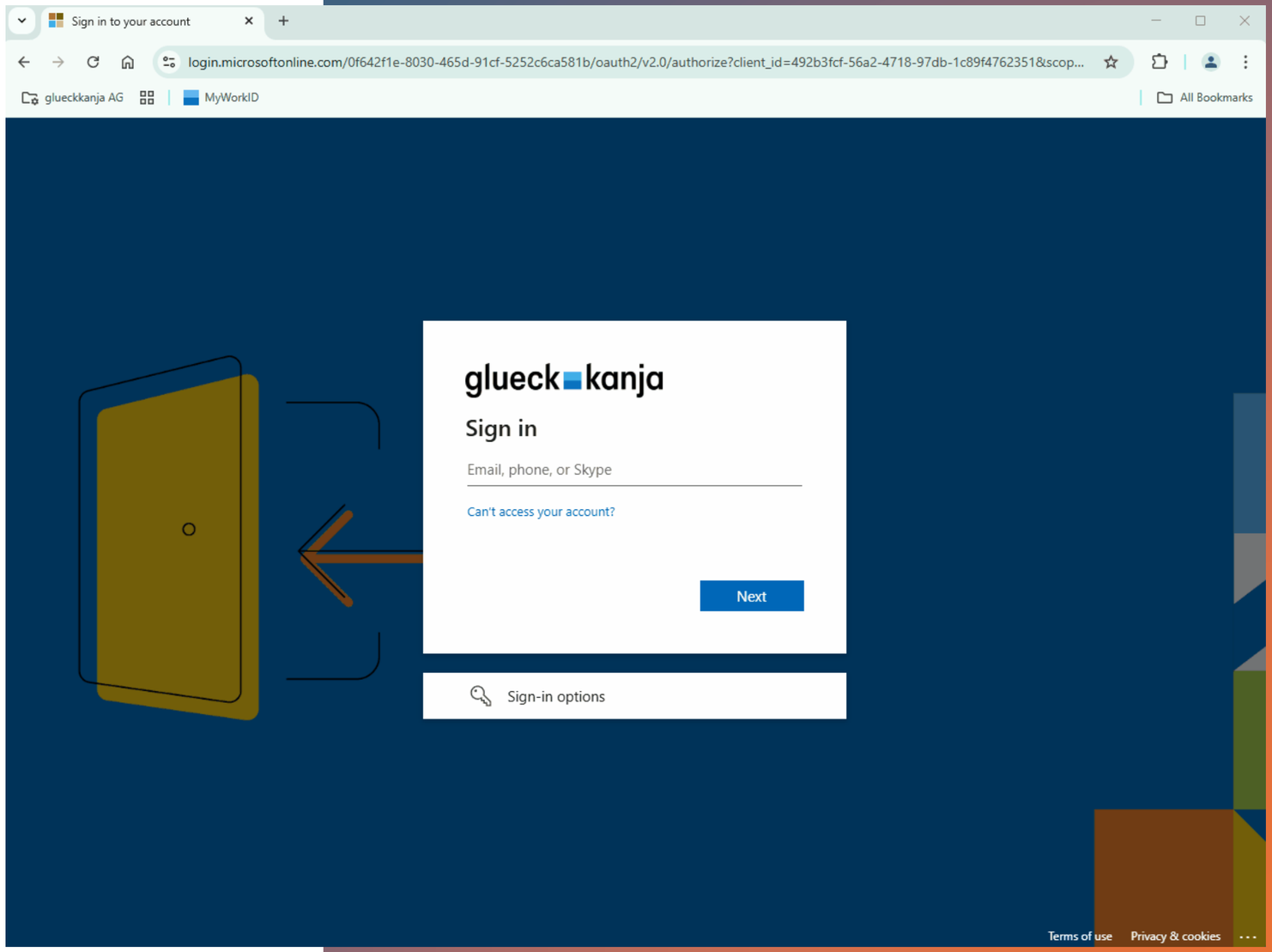
myWorkID

Bootstrap your Passkey rollout with a TAP self service



myWorkID

Bootstrap your Passkey rollout with a TAP self service



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