

Passkeys in Entra ID Myth or reality

 Fabian Bader





Thank you Sponsors

#WPNinjaCH





About Fabian Bader

#WPNinjaCH

Focus

Cyber Security, Identity, Microsoft
SIEM & XDR @ [glueckkanja](#)

From

Hamburg, Germany

My Blog

[cloudbrothers.info](#)



Certifications

Microsoft MVP

Hobbies

Concerts, KQL, User Groups

Contact

Socials (BlueSky, Mastodon, Twitter)



Passkeys in Entra ID: Myth or reality

Generally available

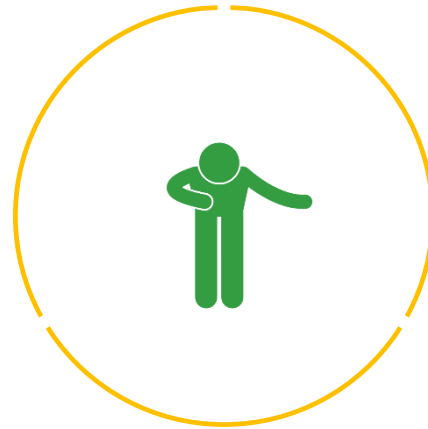
Device-bound passkeys

Phishing-resistant credential in Microsoft Authenticator

Available for both iOS
and Android

Meets strict security
requirements

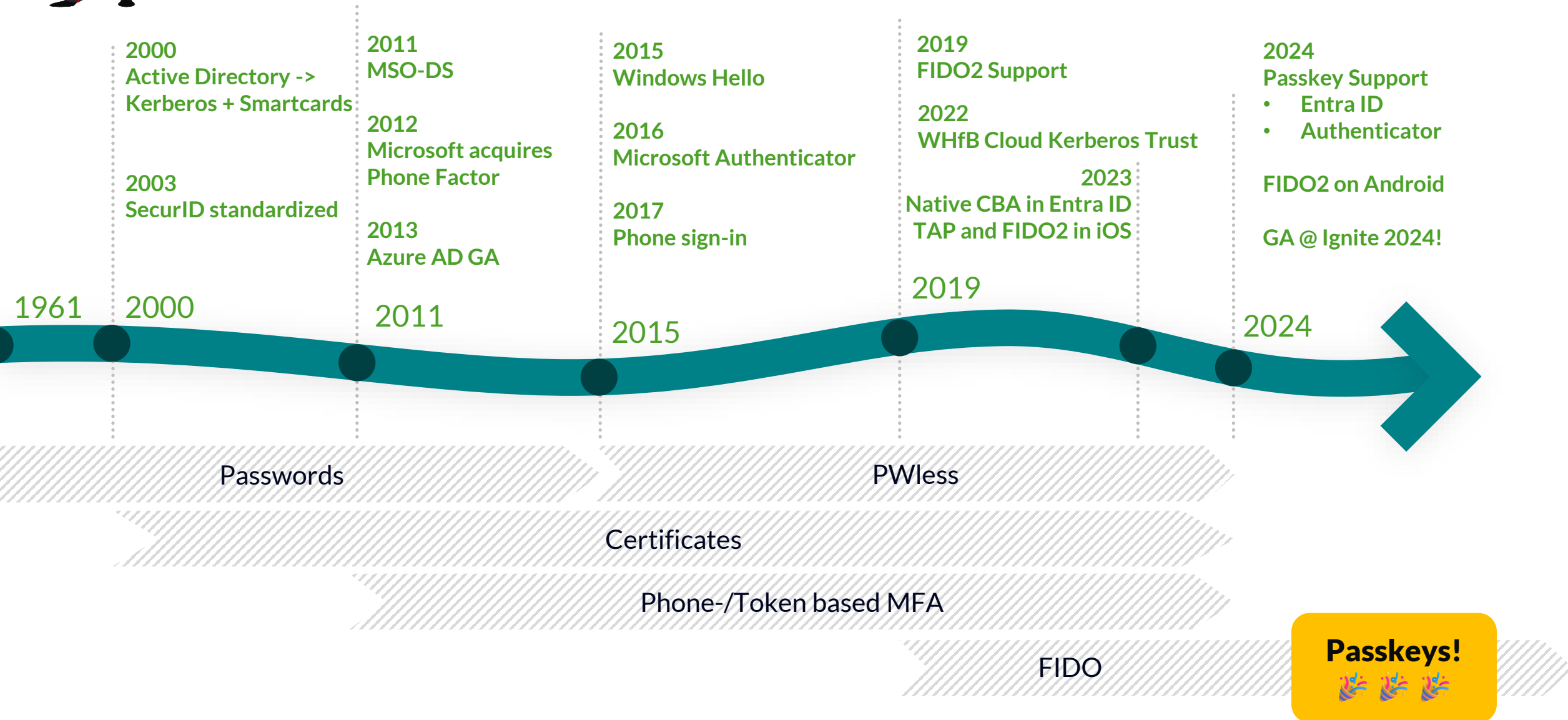
Cost-effective and
easy to deploy



Thank you



Evolution of Authentication at Microsoft





What is a passkey

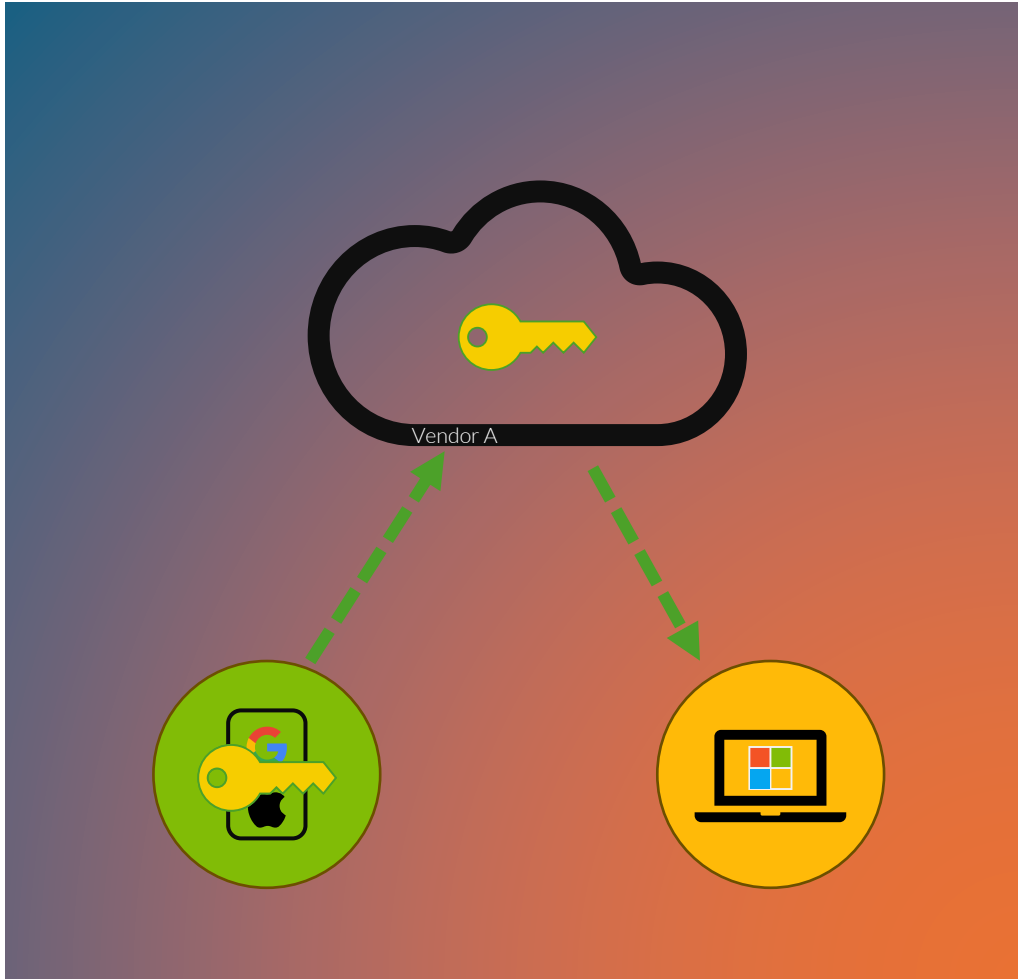
- A passkey is a FIDO2/WebAuthn Discoverable Credential
- “Discoverable Credential” means you don’t have to enter your username
- Password-less
- Phishing resistant
- Based on cryptographic public and private keys

A screenshot of a GitHub login interface. It features a dark background with white text. The first section is labeled 'Username or email address' and has a text input field. Below it is a 'Password' field with a 'Forgot password?' link to its right. A green 'Sign in' button is positioned below the password field. At the bottom, there is a link 'Sign in with a passkey' and a link 'New to GitHub? Create an account'.

A screenshot of a Microsoft sign-in options dialog. It has a white background with the Microsoft logo at the top left. The title is 'Sign-in options'. There are three options listed, each with an icon and a question mark icon to its right: 1. 'Face, fingerprint, PIN or security key' with a person icon, followed by the text 'Use your device to sign in with a passkey.' 2. 'Sign in with GitHub' with the GitHub logo, followed by the text 'Personal accounts only'. 3. 'Sign in to an organization' with a person and organization icon, followed by the text 'Search for a company or an organization you're working with.' At the bottom right, there is a 'Back' button.



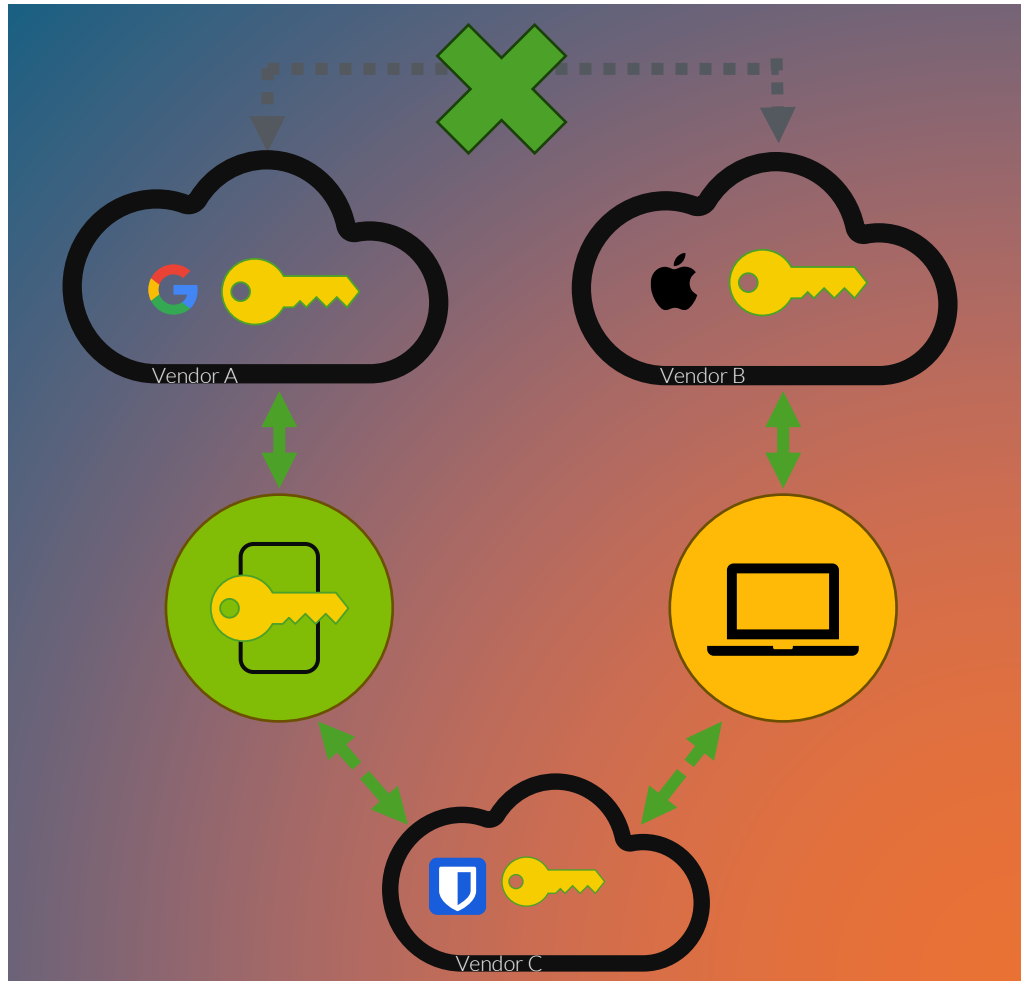
Synced vs. Device-bound passkeys



- 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

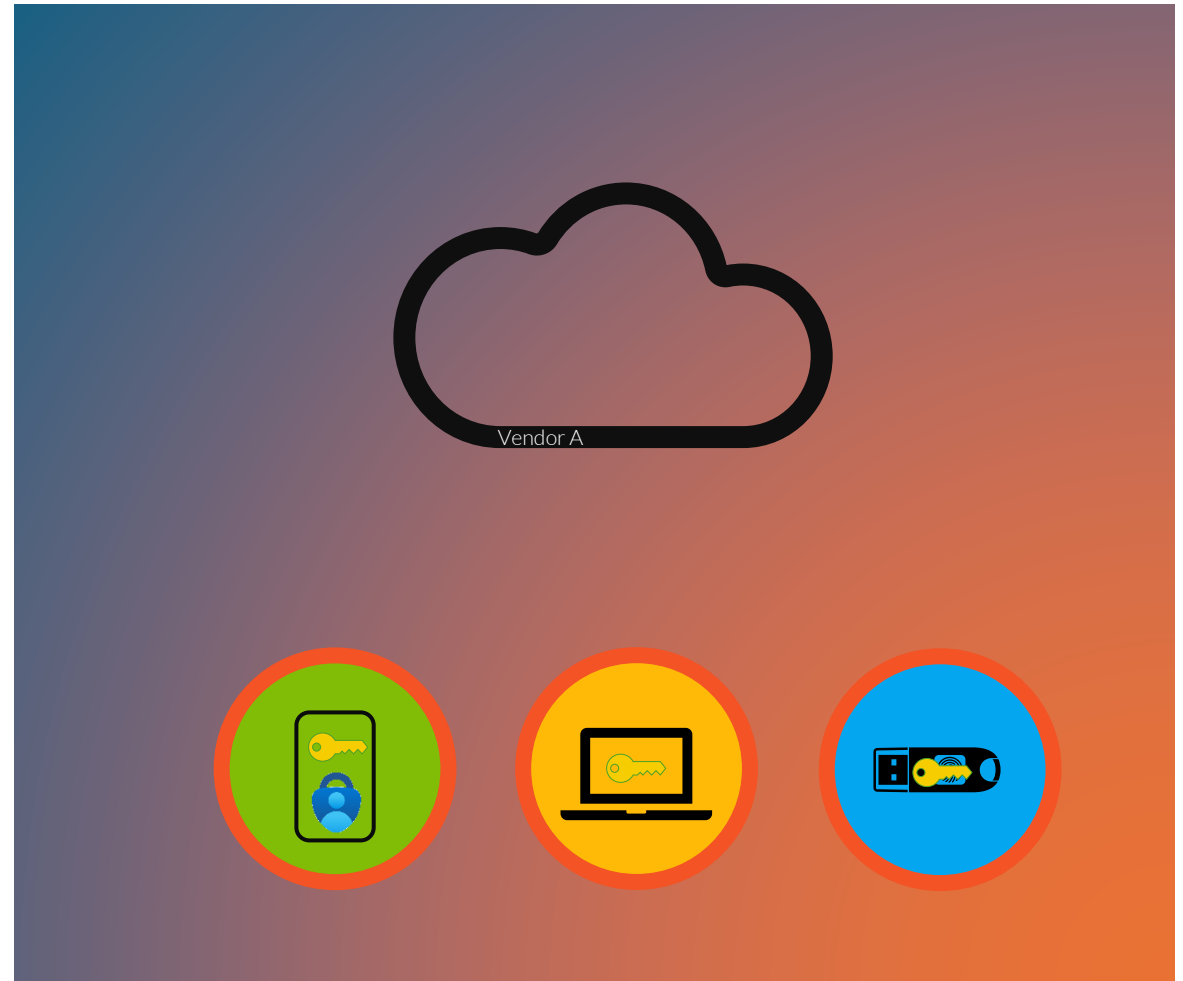


- Native cross vendor sync is not yet possible
- Workarounds
 - Cross-Device Authentication
 - Third-party passkey provider
- The future
 - Credential Exchange Protocol (CXP)



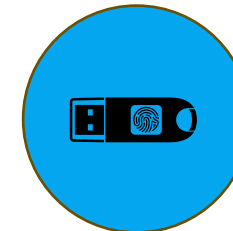
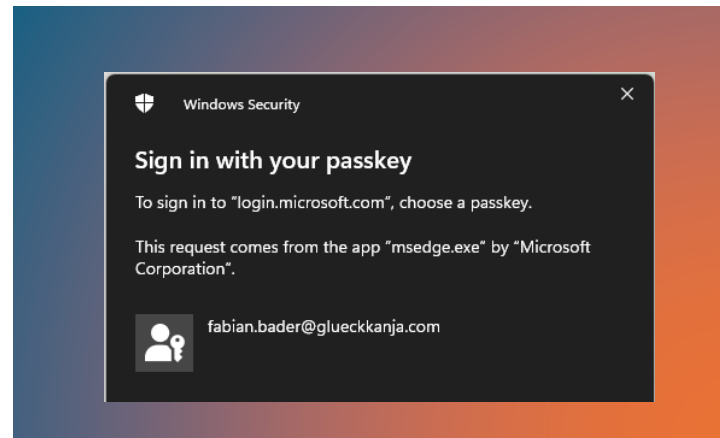
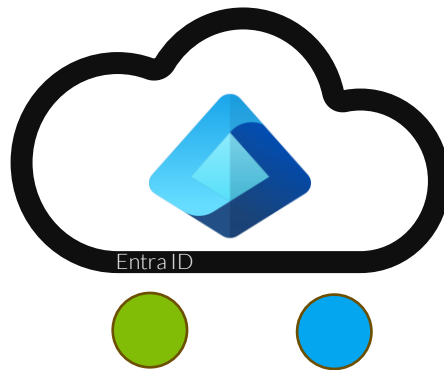
Synced vs. Device-bound passkeys

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



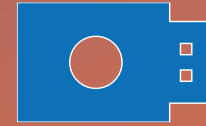
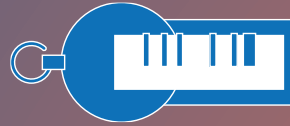
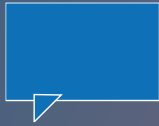


Microsofts current implementation





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



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

Enforce attestation

Yes No

KEY RESTRICTION POLICY

Enforce key restrictions

Yes No

Restrict specific keys

Allow Block

☐ Microsoft Authenticator (Preview) ⓘ

[Add AAGUID](#)

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

...

c5ef55ff-ad9a-4b9f-b580-adebaf026d0

...

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



Quick Tipp

#WPNinjaCH



```
PowerShell
FabianBader Install-Module EntraIDPasskeyHelper
FabianBader Connect-MgGraph -Scopes "AuditLog.Read.All", "Policy.ReadWrite.AuthenticationMethod", "User.Read.All", "UserAuthenticationMethod.Read.All"
```



PSGallery Version v1.0.3

PSGallery Downloads 5.7k



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

- Overview
- Audit logs
- Sign-in logs
- Diagnose and solve problems


Manage

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

Troubleshooting + Support

- New support request

You've reached your passkey limit



You can have a maximum of 10 passkeys. To add a new one, delete an old one first.

Having trouble?

OK

Windows Hello for Business	
Microsoft Authenticator	Pixel
Non-usable authentication methods	

[Home](#) >

EPA 1 - Require YubiKey for Admin Access

Conditional Access policy

Delete View policy information

Name *

EPA 1 - Require YubiKey for Admin Access

Assignments

Users or workload identities ⓘ

[Specific users included and specific users excluded](#)

Target resources ⓘ

1 app included

Network NEW ⓘ

[Not configured](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

1 control selected

Session ⓘ

[0 controls selected](#)

Enable policy

Report-only On Off

Save

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

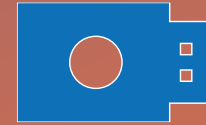
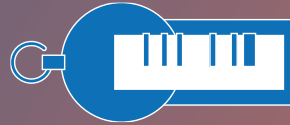
Name	YubiKey Only
Type	Custom
Description	
Creation Date	7/28/2024, 2:05 PM
Modified Date	7/28/2024, 2:05 PM
Authentication Flows	Passkeys (FIDO2)
	c5ef55ff-ad9a-4b9f-b580-adebaf026d0
	fa2b99dc-9e39-4257-8f92-4a30d23c4118
	2fc0579f-8113-47ea-b116-bb5a8db0202a

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

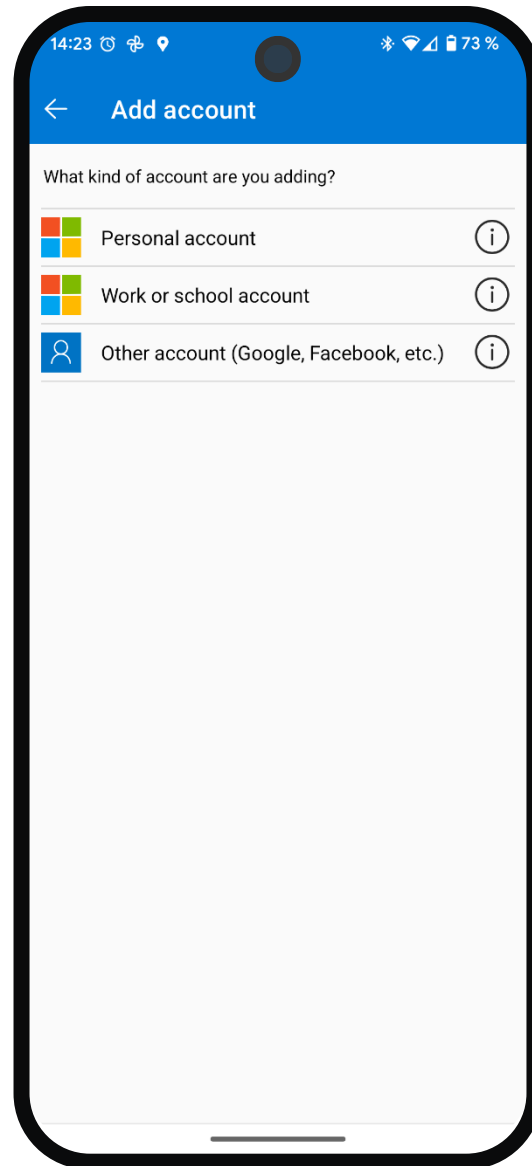




User experience

The myth

#WPNinjaCH

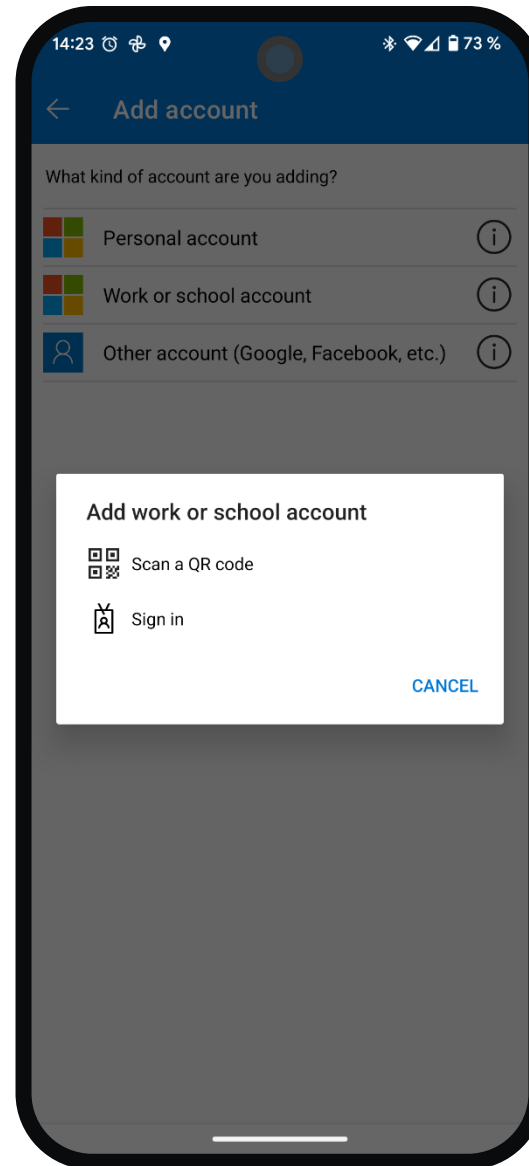




User experience

The myth

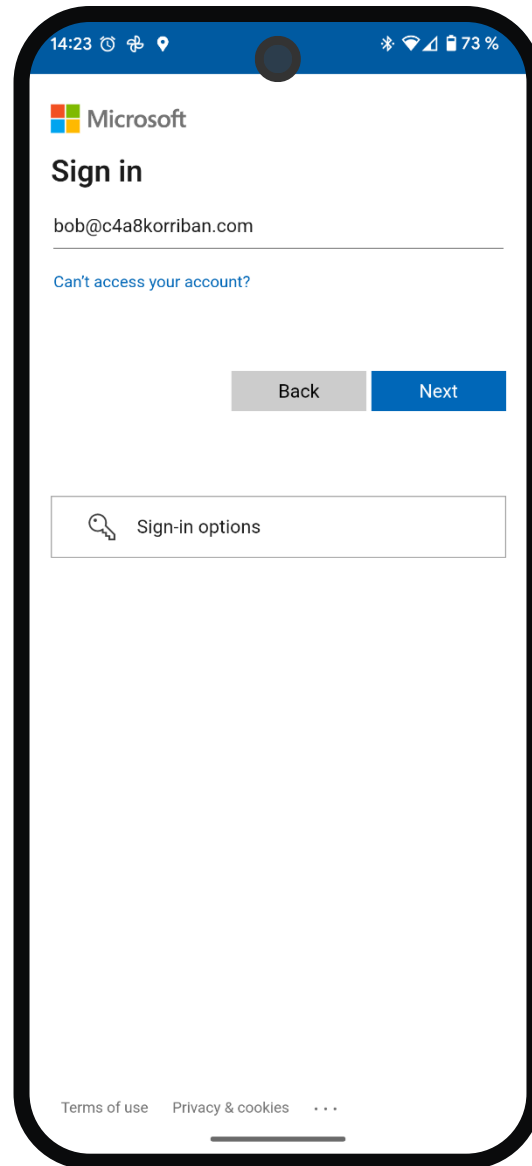
#WPNinjaCH





User experience

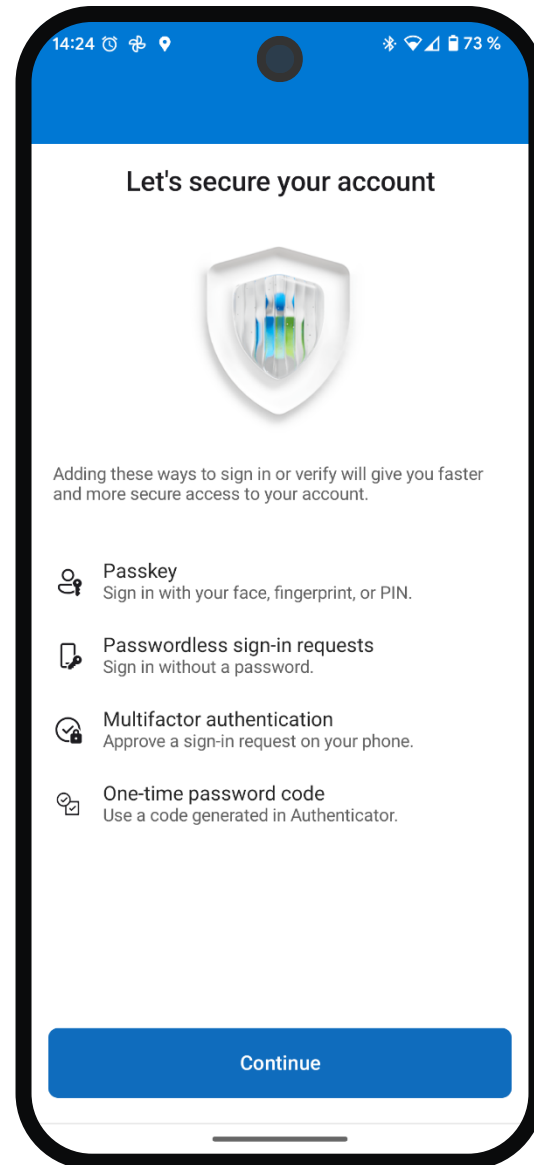
The myth





User experience

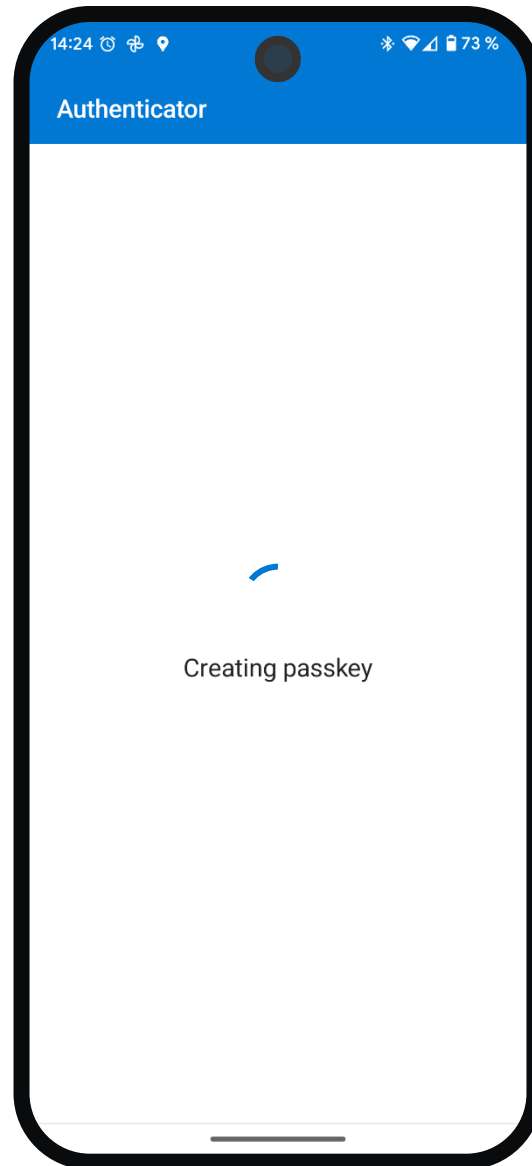
The myth





User experience

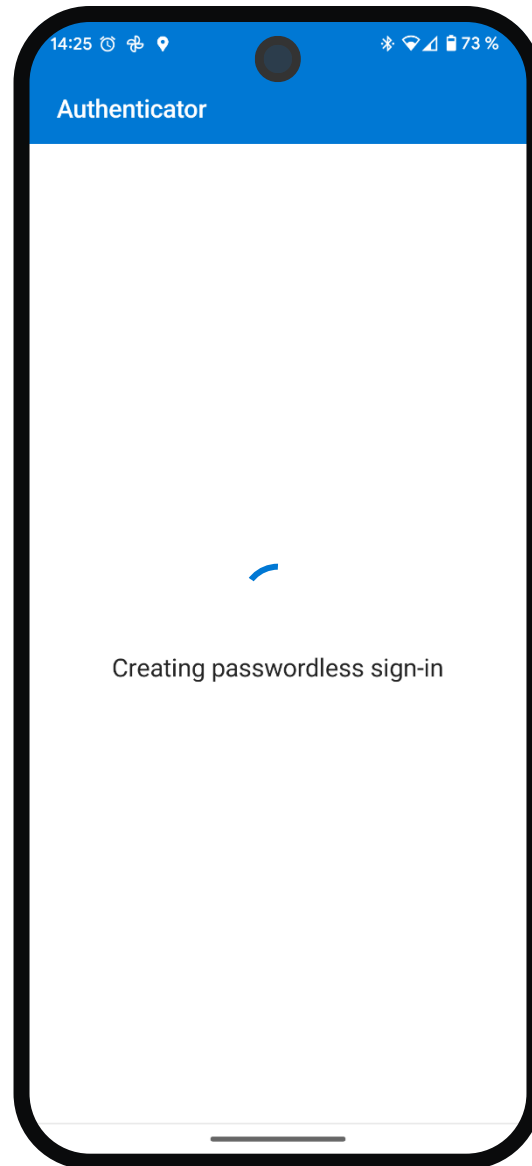
The myth





User experience

The myth

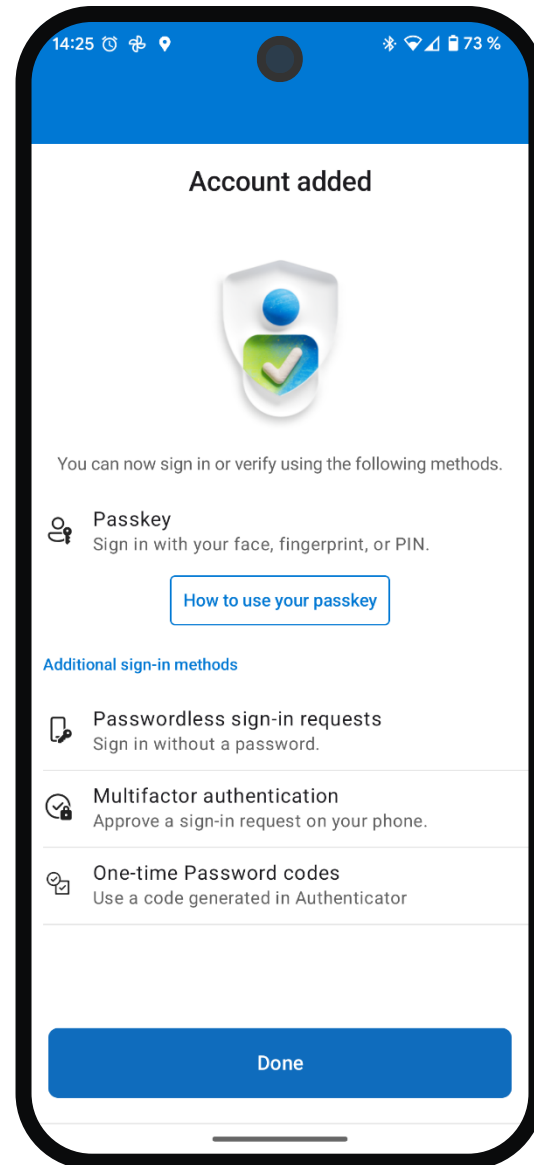




User experience

The myth

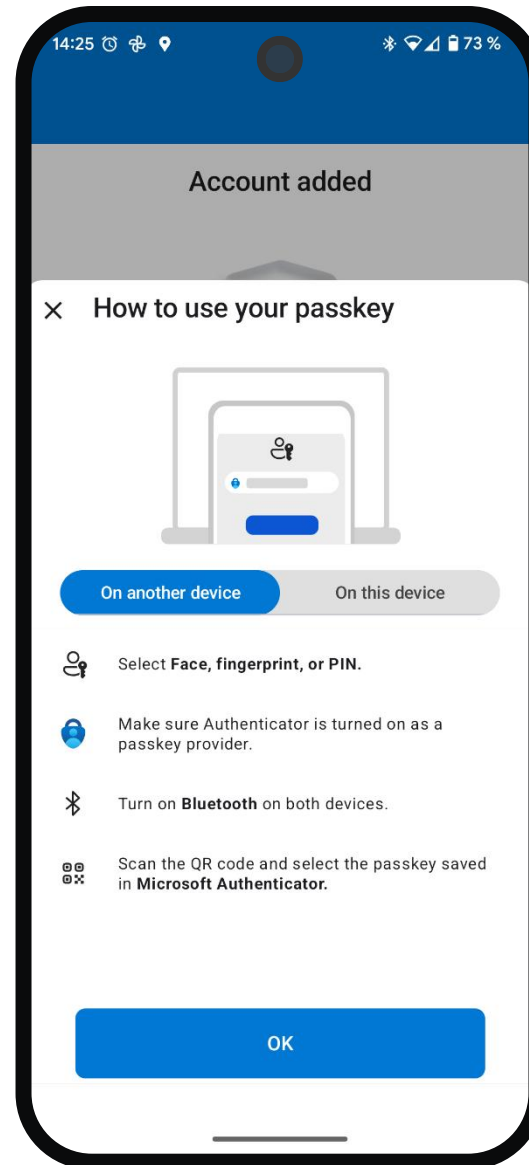
#WPNinjaCH





User experience

The myth

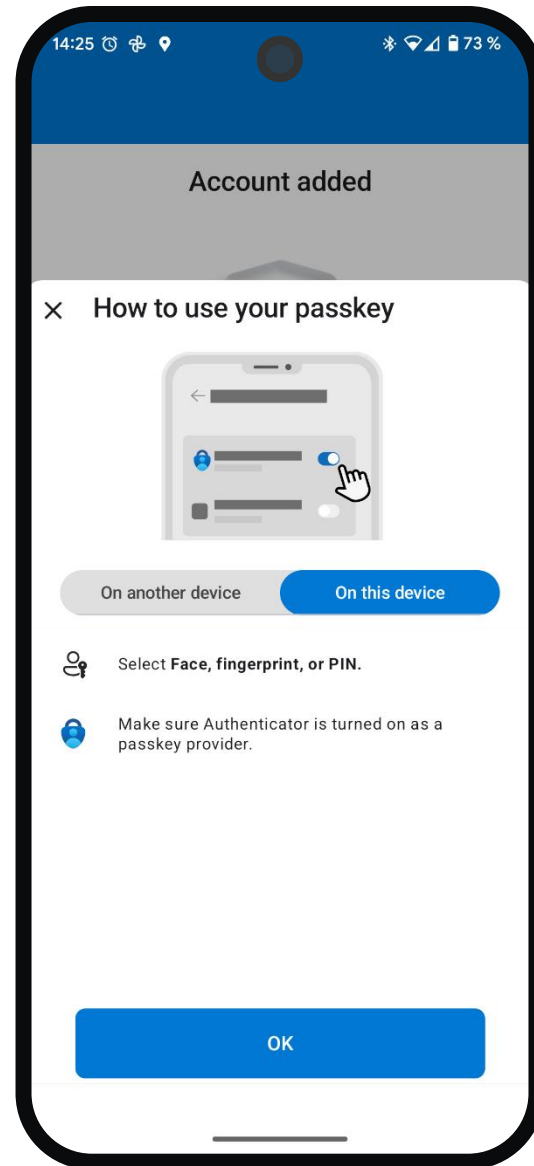




User experience

The myth

#WPNinjaCH

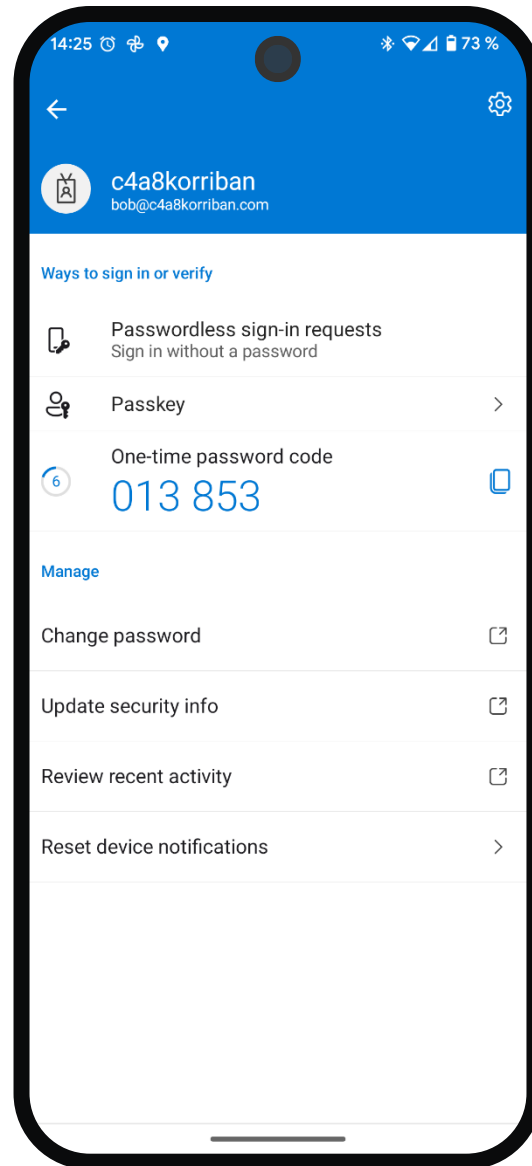




User experience

The myth

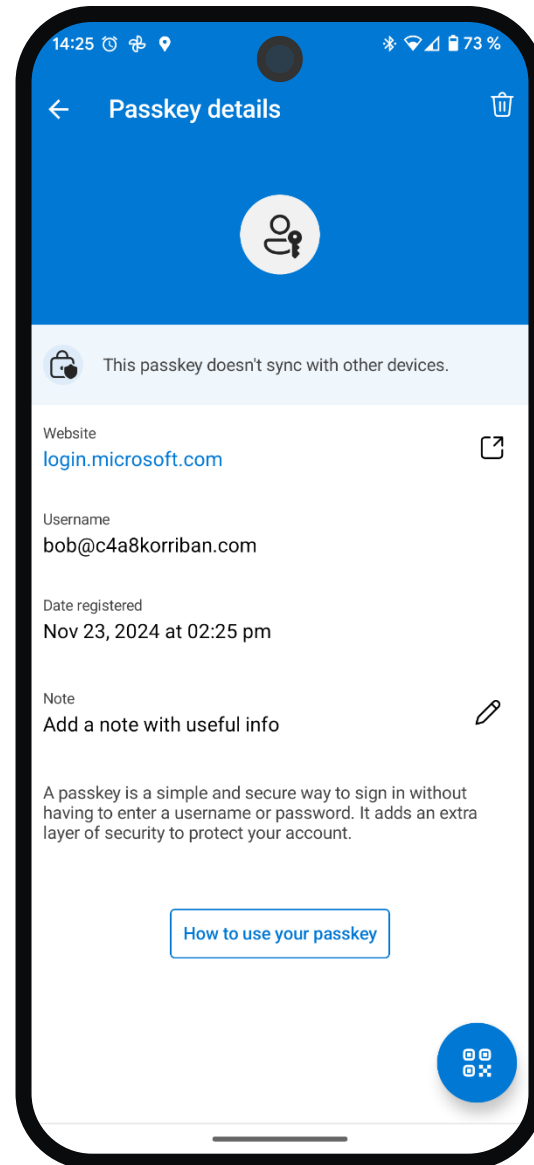
#WPNinjaCH





User experience

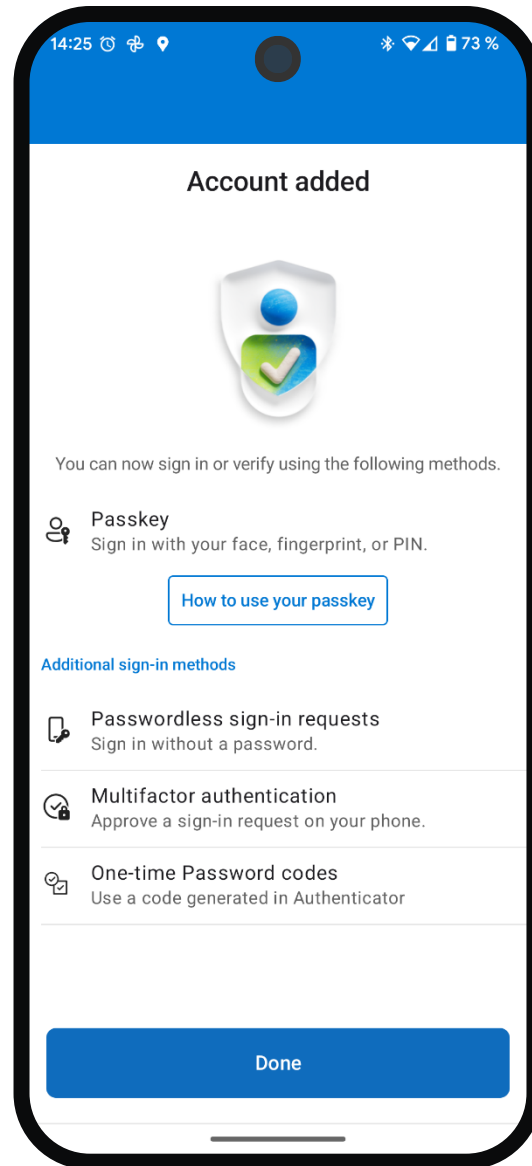
The myth





User experience Reality

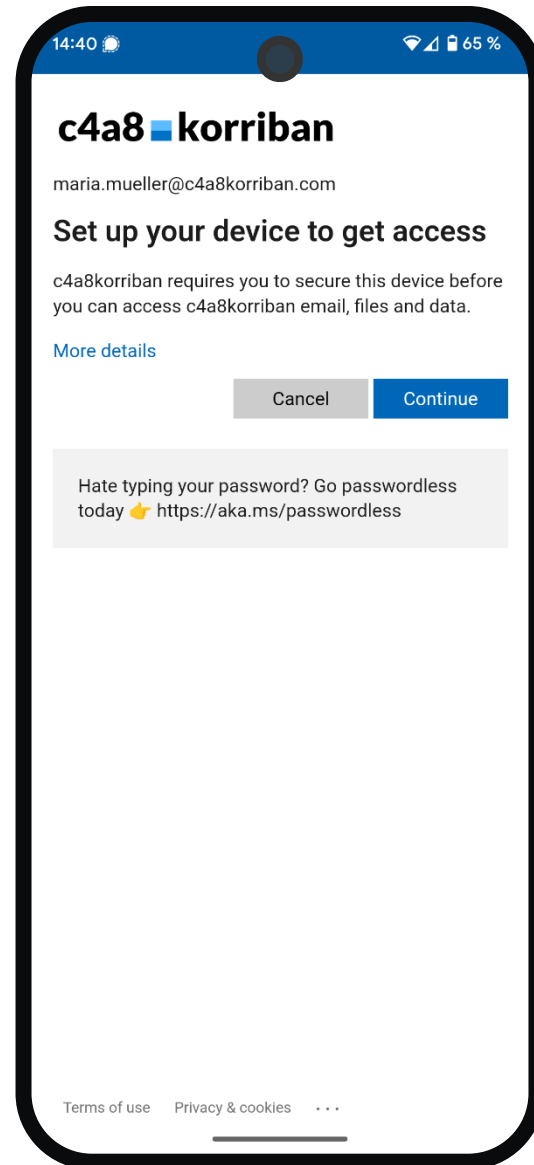
#WPNinjaCH





User experience Reality

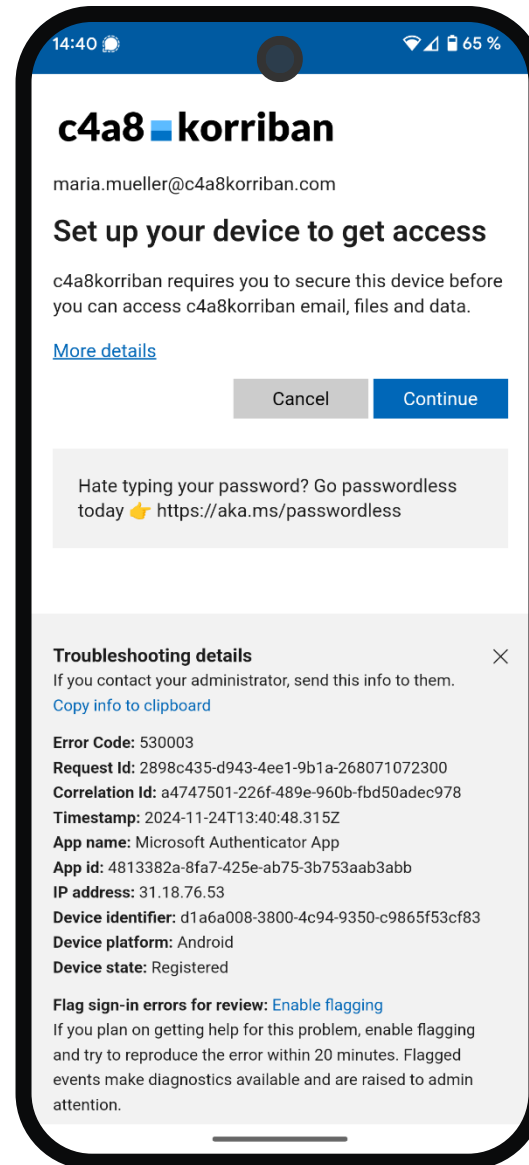
#WPNinjaCH





User experience Reality

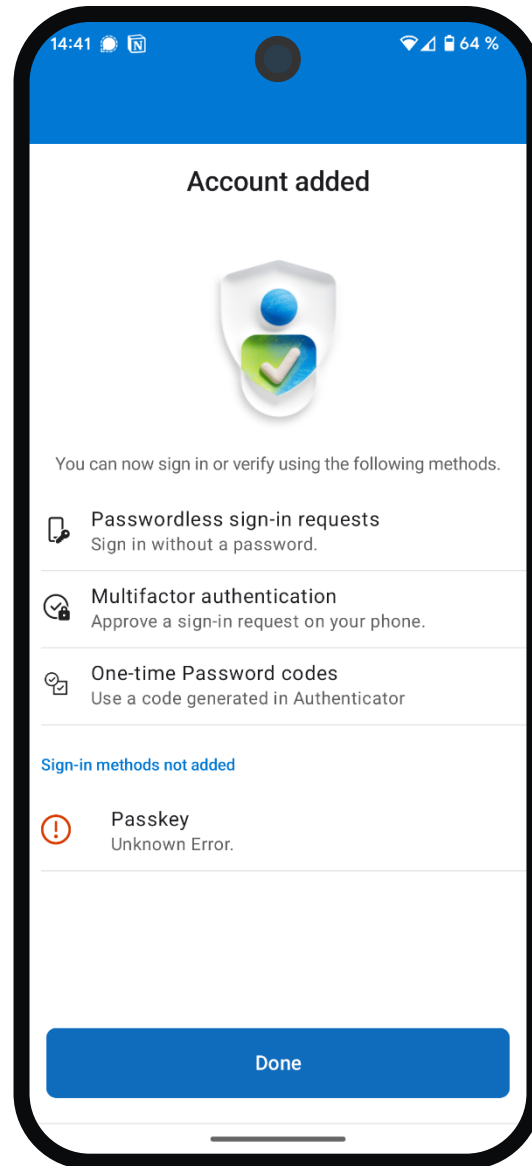
#WPNinjaCH





User experience Reality

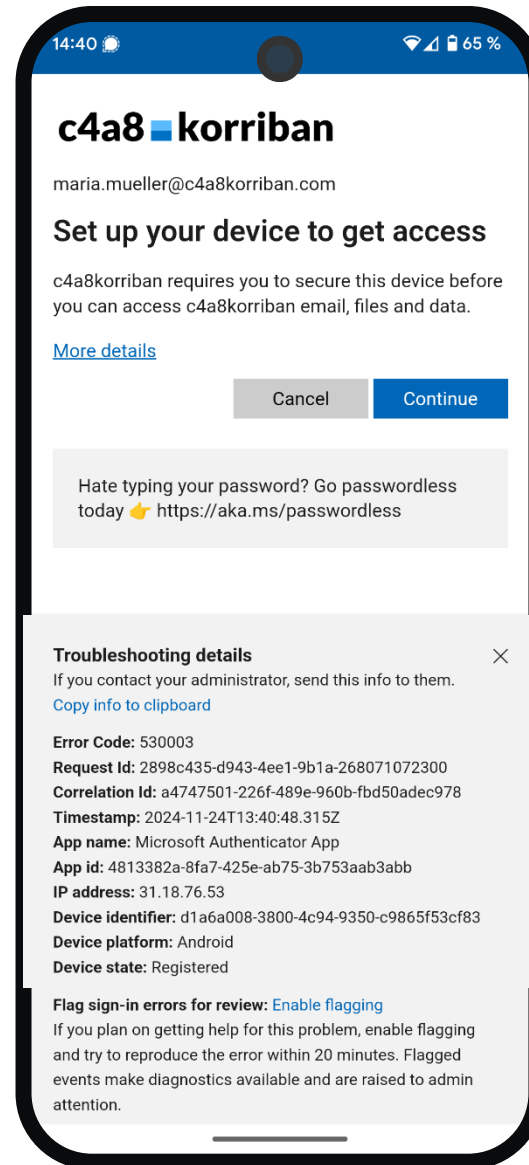
#WPNinjaCH





User experience Reality

#WPNinjaCH

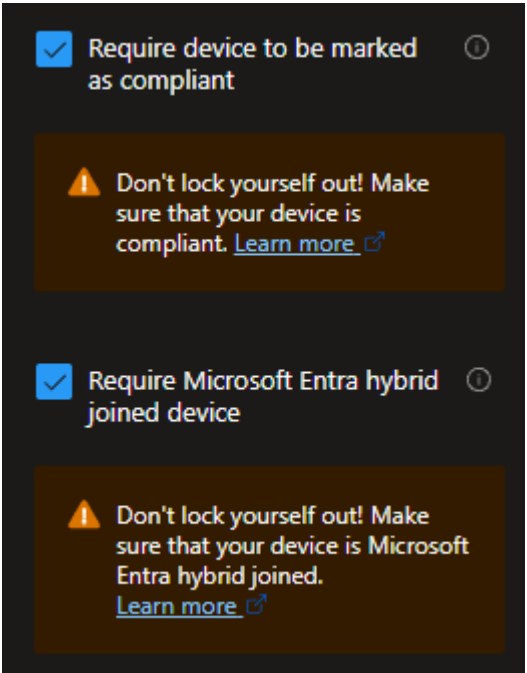
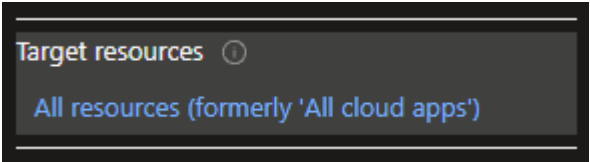




What's happening here

<input type="checkbox"/>	TimeGenerated [UTC] ↑↓	Category	ResultType	ResultDescription	CorrelationId	AppDisplayName	AppId	ResourceDisplayName	ResourceIdentity
<input type="checkbox"/>	> 24.11.2024, 13:42:15.362	SignInLogs	530003	Other	a4747501-226f-489e-960b-fbd50adec978	Microsoft Authenticator App	4813382a-8fa7-425e-ab75-3b7...	Microsoft Graph	00000003-0000-0000-c000-000000000000
<input type="checkbox"/>	> 24.11.2024, 13:42:09.266	NonInteractiveUserSignInLogs	530003	Other	a4747501-226f-489e-960b-fbd50adec978	Microsoft Authenticator App	4813382a-8fa7-425e-ab75-3b7...	Microsoft Graph	00000003-0000-0000-c000-000000000000
<input type="checkbox"/>	> 24.11.2024, 13:42:04.808	SignInLogs	50097	Device Authentication Required...	a4747501-226f-489e-960b-fbd50adec978	Microsoft Authenticator App	4813382a-8fa7-425e-ab75-3b7...	Microsoft Graph	00000003-0000-0000-c000-000000000000

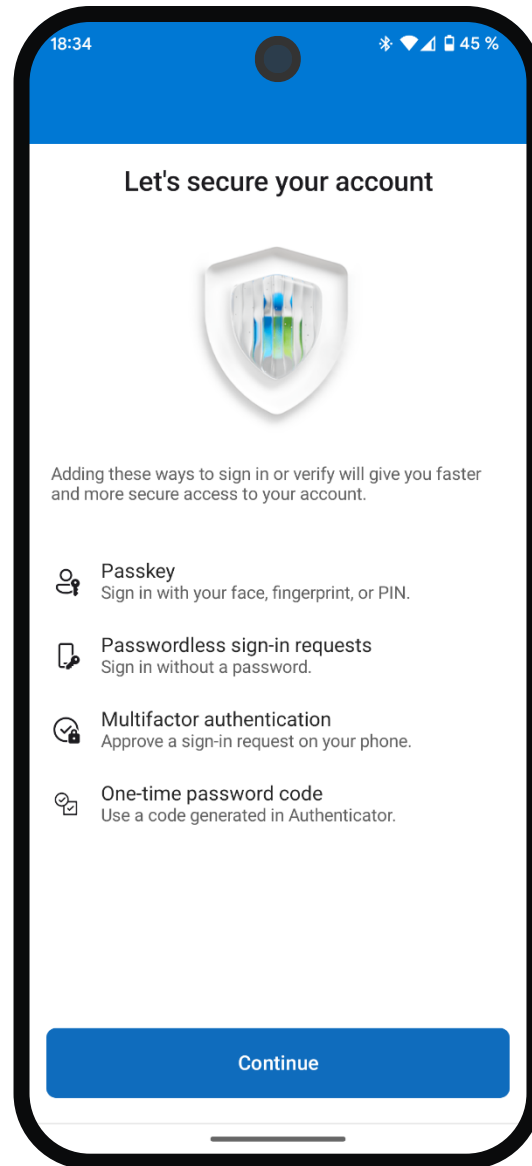
- 530003
Your device is required to be managed to access this resource.
- 50097
Device authentication required





User experience Reality

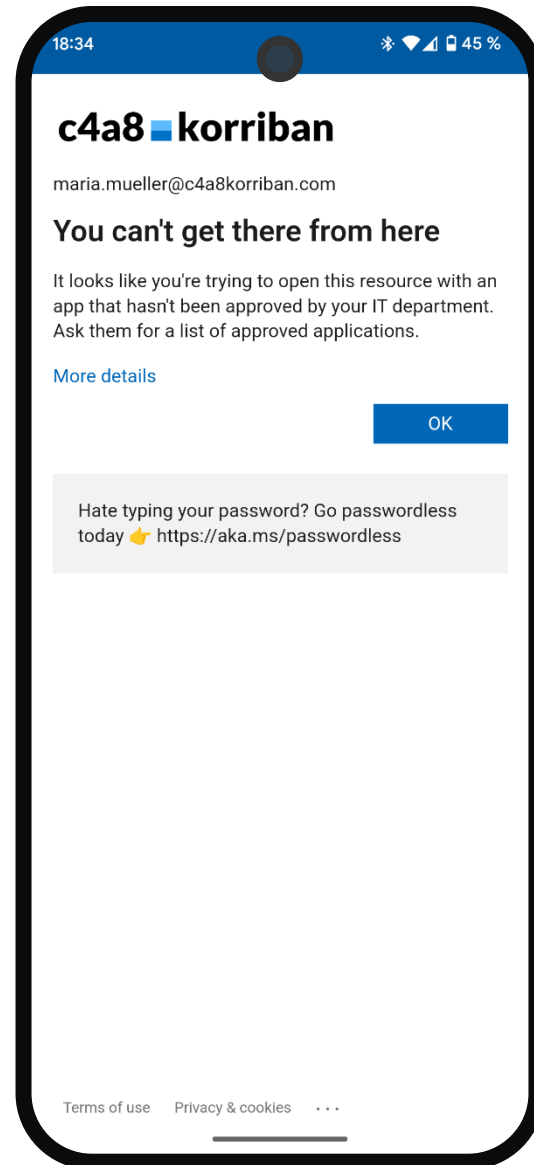
#WPNinjaCH





User experience Reality

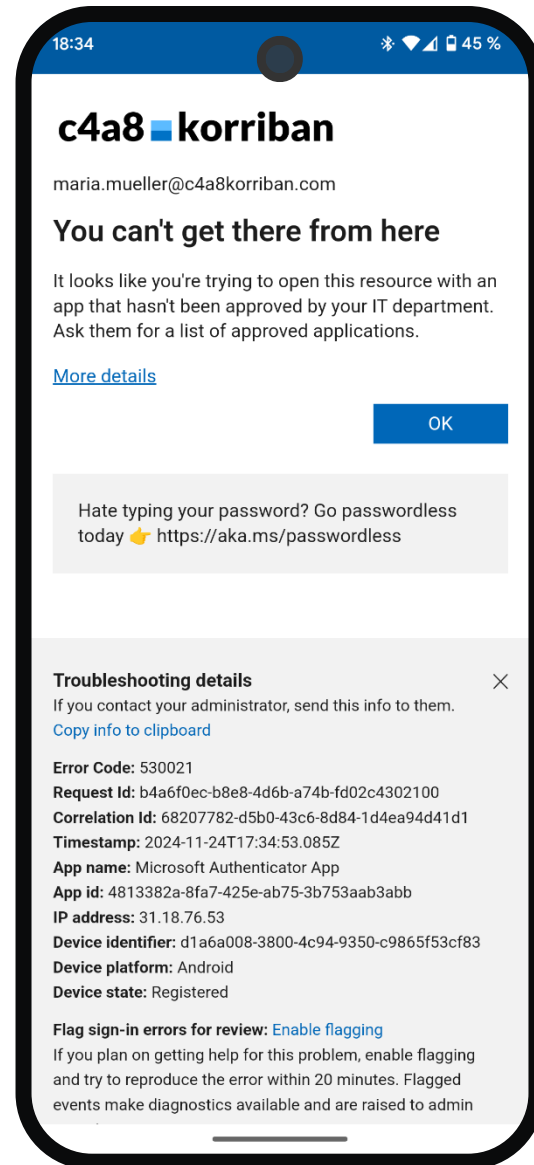
#WPNinjaCH





User experience Reality

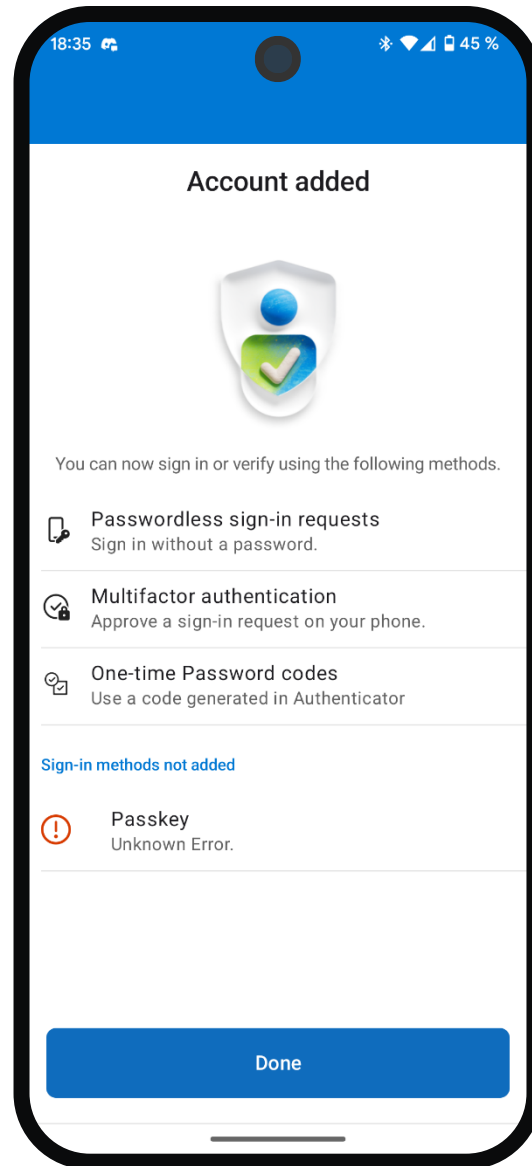
#WPNinjaCH





User experience Reality

#WPNinjaCH





Workaround #1

- Create a second, Conditional Access Policies for device compliance and approved apps
- Set target resources to only selectable apps
- Assign it to a specific "Passkey Onboarding" group
- Exclude this group from the regular Conditional Access Policies
- Use an access package with self service to add users to the "Passkeys Onboarding" group for one or two days.
 - Optional: Let the helpdesk delegate the access package for users in scope of your onboarding campaign





Workaround #2 - Cross Device

The screenshot shows a web browser window with the URL <https://mysignins.microsoft.com/security-info>. The page is titled "Security info" and contains a list of sign-in methods. A yellow banner at the top states: "For security reasons, we recommend that you delete any sign-in methods that you no longer use." The left sidebar shows navigation options: Overview, Security info (selected), Devices, Password, Organizations, Settings & Privacy, and Recent activity. The main content area lists the following sign-in methods:

Sign-in method	Last updated	Action
+	+	+
...
Microsoft Authenticator
Passkey
Temporary access pass

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



Workaround #2 - Cross Device

The screenshot shows a web browser window at <https://mysignins.microsoft.com/security-info>. The user is logged in as 'c4a8 korriban'. The left sidebar contains links to Overview, Security info (selected), Devices, Password, Organizations, Settings & Privacy, and Recent activity. The main content area is titled 'Security info' and includes a warning: 'For security reasons, we recommend that you delete any sign-in methods that you no longer use.' Below this, it shows the 'Default sign-in method: Microsoft Authenticator'. A modal titled 'Add a sign-in method' is open, displaying four options: 'Passkey in Microsoft Authenticator' (selected), 'Security key or passkey', 'Security key', and 'Microsoft Authenticator'. The background page shows a list of existing sign-in methods with 'Delete' buttons.

Add a 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

Lost device? [Sign out everywhere](#)



Workaround #2 - Cross Device

The screenshot shows a web browser window at <https://mysignins.microsoft.com/security-info>. The user is logged in as 'c4a8 korriban'. The left sidebar contains navigation links: Overview, Security info (selected), Devices, Password, Organizations, Settings & Privacy, and Recent activity. The main content area is titled 'Security info' and includes a warning: 'For security reasons, we recommend that you delete any sign-in methods that you no longer use.' Below this, it shows the 'Default sign-in method: Microsoft Authenticator'. A modal titled 'Add a sign-in method' is open, displaying four options: 'Passkey in Microsoft Authenticator' (selected), 'Security key or passkey', 'Security key', and 'Microsoft Authenticator'. The background page shows a list of existing sign-in methods with 'Delete' buttons. At the bottom, there is a 'Lost device? Sign out everywhere' link.

Security info

These are the methods you 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

Lost device? [Sign out everywhere](#)



Workaround #2 - Cross Device

InPrivate My Sign-Ins | Security Info | Micro x +

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

c4a8 korriban My Sign-Ins v

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 use to sign into your account or reset your password.

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](#)

[Having trouble?](#)

Back Next

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

Lost device? [Sign out everywhere](#)



Workaround #2 - Cross Device

InPrivate My Sign-Ins | Security Info | Micro x +

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

c4a8 korriban My Sign-Ins v

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 use to sign into your account or reset your password.

Default

+ Add

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

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

Lost device? [Sign out everywhere](#)



Workaround #2 - Cross Device

InPrivate My Sign-Ins | Security Info | Micro x +

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

c4a8 korriban 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 use to sign into your account or reset your password.

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

+ Add sign-in method

Passkey

Microsoft Authenticator Passwordless sign-in

Passkey Microsoft Authenticator

Passkey Microsoft Authenticator Authenticator - Android

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

Lost device? [Sign out everywhere](#)

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

Delete

Delete

Delete

Delete



Workaround #2 - Cross Device

InPrivate My Sign-Ins | Security Info | Micro x +

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

c4a8 korriban My Sign-Ins v

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 use to sign into your account or reset your password.

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.

[Having trouble?](#)

[Back](#) [Continue](#)

Default			
+ Add			
...			Delete
🔍			Delete
👤			Delete
👤	Passkey Microsoft Authenticator	Authenticator - Android	Delete
🔑	Temporary access pass	Expires 11/24/2024, 7:34:32 PM	Delete

Lost device? [Sign out everywhere](#)



Workaround #2 - Cross Device

InPrivate My Sign-Ins | Security Info | Micro x +

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

c4a8 korriban My Sign-Ins v

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 use to sign into your account or reset your password.

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.

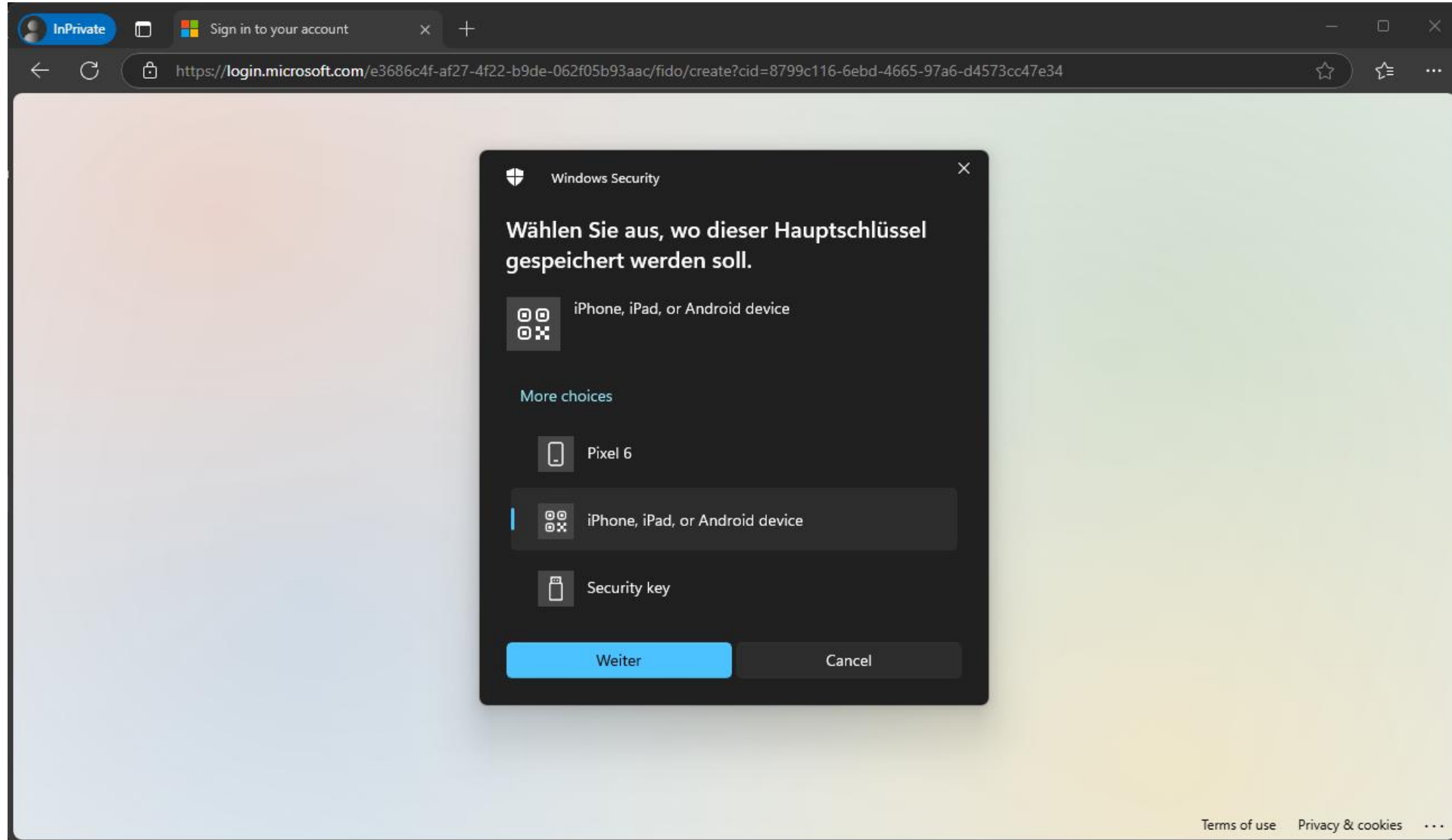
[Having trouble?](#) [Back](#) [I'm ready](#)

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

Lost device? [Sign out everywhere](#)

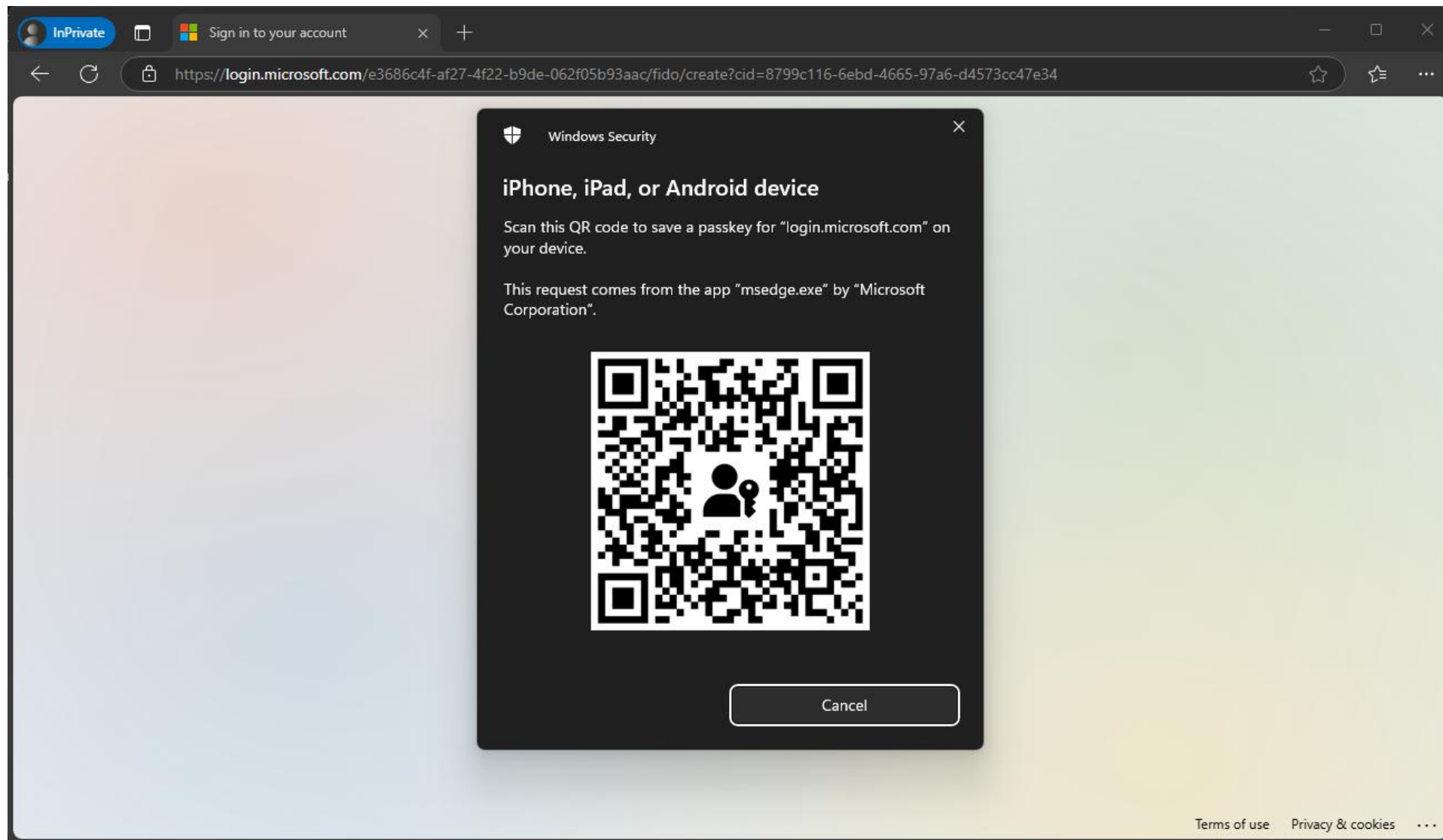


Workaround #2 - Cross Device





Workaround #2 - Cross Device





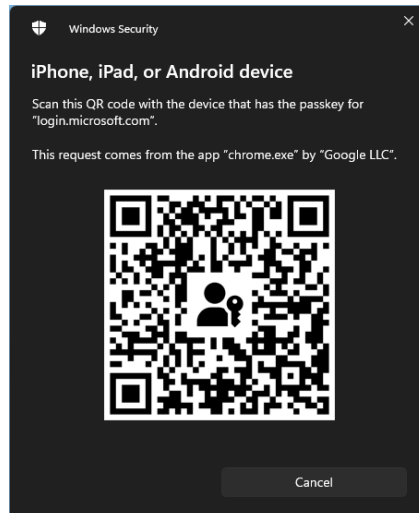
Workaround #2 - Cross Device





Cross Device



























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



FIDO: /08852177264574630425662919689802380521379
19748878851599699467519287713887017934854010709
23423366366303159168738737767290060661159865120
837177011010667266107096654083332



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	

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

Attestation? AAGUID?

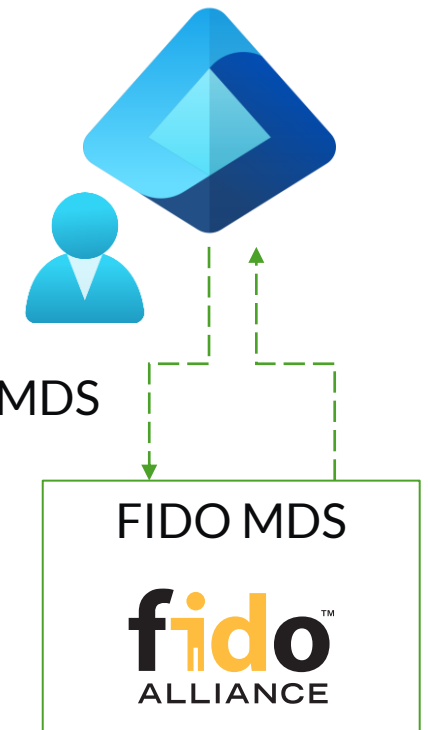
Authenticator Attestation **GUID** = **AAGUID**



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





Passkeys in Entra ID: Myth or reality

- Passkeys are reality
- There are hurdles, a lot of hurdles
- 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.



Android - How to check

- adb shell pm has-feature android.software.credentials

A composite image showing a PowerShell terminal window on the left and an Android 'Passwords & accounts' settings screen on the right. The PowerShell window has a title bar with 'PowerShell' and standard window controls. It shows a command prompt where the user 'Grüezi' has entered the command '.\adb shell pm has-feature android.software.credentials', resulting in the output 'false'. The Android settings screen has a title bar with 'Passwords & accounts' and standard window controls. It lists sections: 'Passwords' with a Google account, 'Autofill service' with a Google account and a settings gear icon, and 'Accounts for Owner' at the bottom.

PowerShell

```
Grüezi > .\adb shell pm has-feature android.software.credentials  
false  
Grüezi > |
```

Passwords & accounts

Passwords

Google

Autofill service

Google

Accounts for Owner



Tips

- Use temporary access pass for passkey enrollment
- Use same device registration whenever if possible
- Windows ❤️ Windows Hello for Business + Cloud Kerberos Trust
- Enable attestation to verify the passkey provider
- Allow phone sign-in as a backup
- Restrict security info registration to phishing resistant methods
- Enforce phishing resistance using Authentication Strength
- Every passkey is better than no passkey



But what about the recent Yubikey flaws?



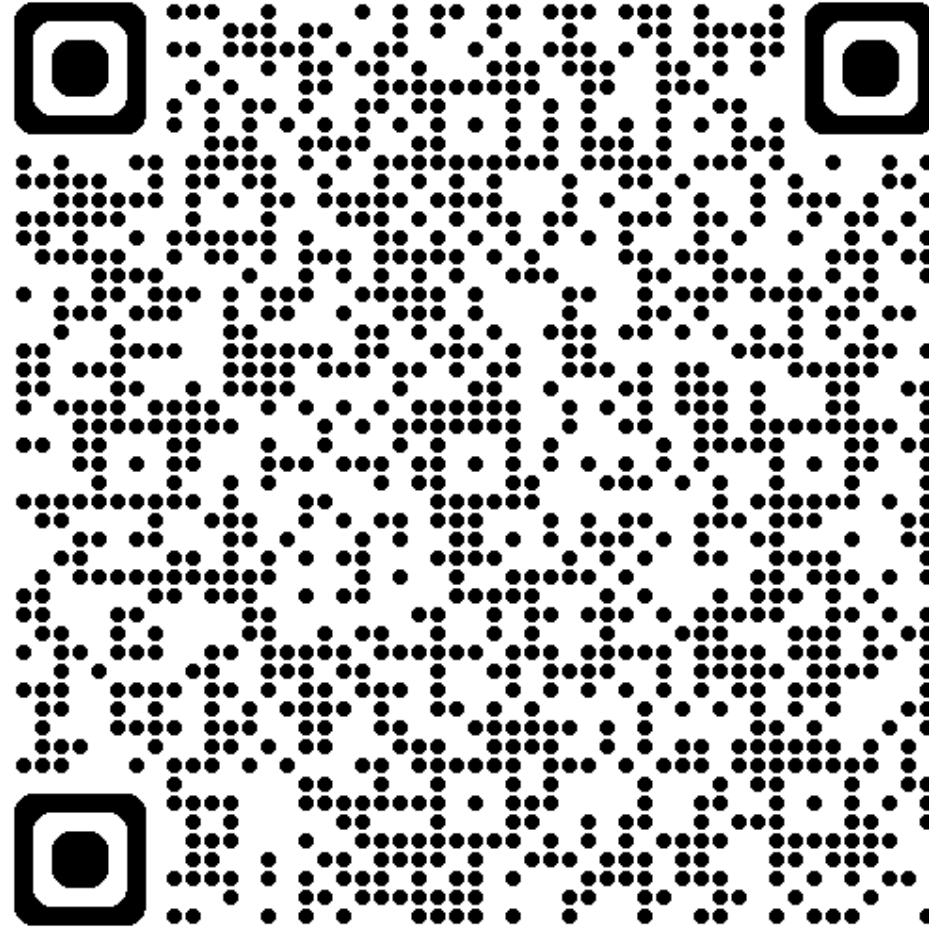
Figure A.3: YubiKey 5C – Second Opening

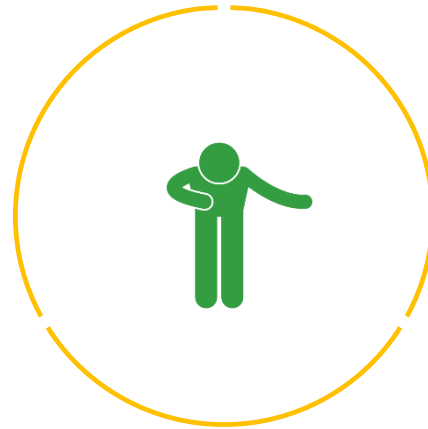
In both cases however, the device needs to be re-packaged if the adversary wants to give it back to legitimate user without him noticing. We did not study further this issue.



Session Feedback

#WPNinjaCH





Thank you