

Passwordless – Phishing proof identities?!

Markus Lintuala

Workplace Ninja Summit 2022





www.wpninjas.eu
#WPNinjaS

Platinum Sponsor



PATCH MY PC



**Microsoft
Security**

Gold Sponsor

glueckkanja gab

baseVISION
SECURE & MODERN WORKPLACE



RECAST SOFTWARE

LIQUIT

Lenovo



Snapdragon

Silver and Special Sponsors



LUZERN
FACEBOOK
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC  USION


SCAPPMAN

APPMANAGEMENT.COM
2022
OCTOBER 7
NETHERLANDS

dinext.



About Markus

www.wpninjas.eu

Focus

Public cloud architectures and solutions with a focus on security

From

Finland



My Blog

Bloggerz.cloud



Certifications



Hobbies

- IT
- Aviation
- Cooking

Contact

LinkedIn: [lintuala](#)

Twitter: [@MarkusLintuala](#)

E-mail: markus@lintuala.fi



Key takeaways:

- **Passwordless is the most secure authentication method**
- **Start the passwordless journey**



Overall authentication

Different authentication security levels



What is passwordless authentication

Passwordless, FIDO2, W3C, what those are?



Using passwordless in Azure AD

What solutions does Azure AD provide for you and how does those work?



Real life use-case

Example of real life use case



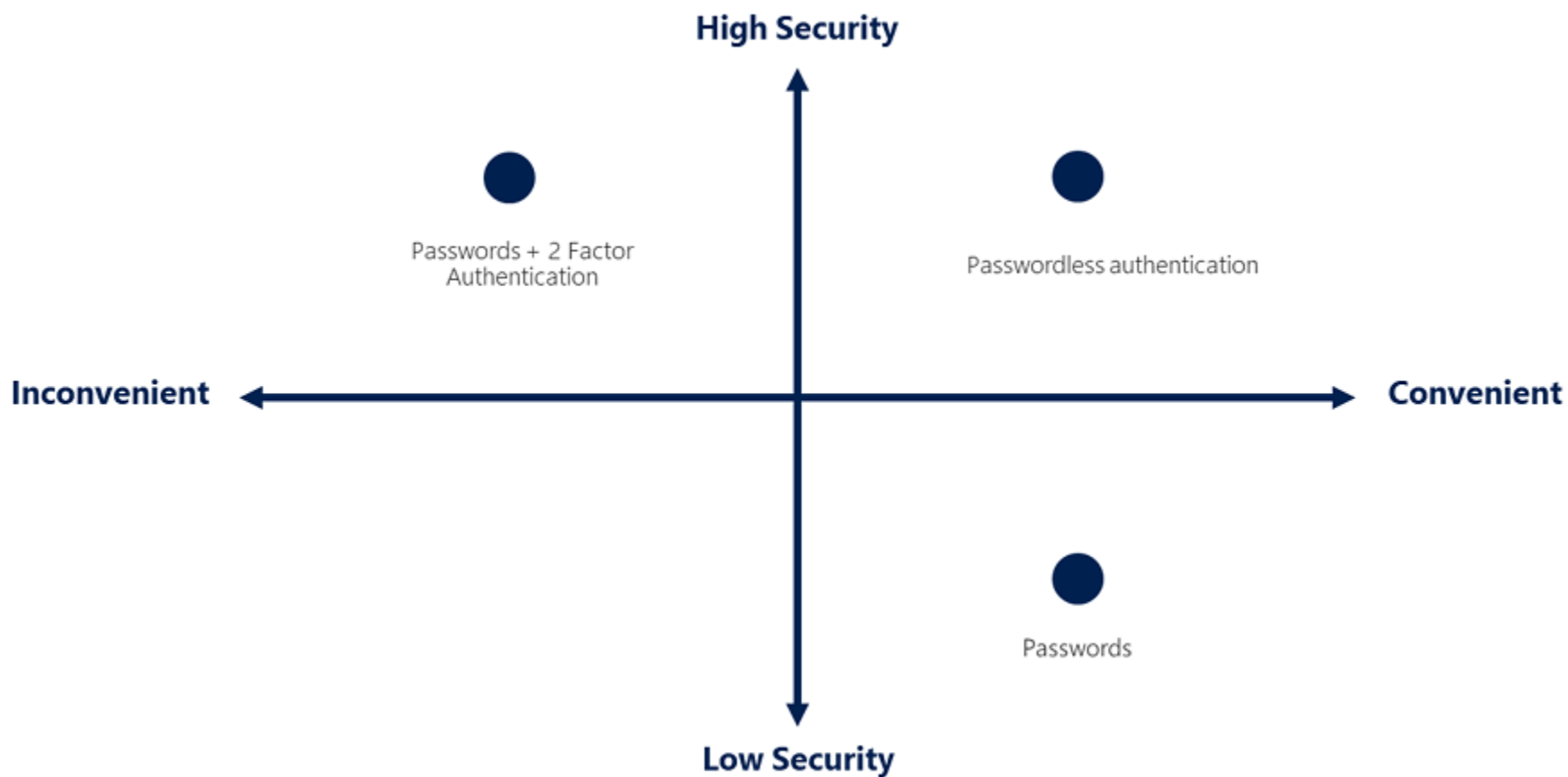
What about the future?

What is coming up and what is the next step with passwordless



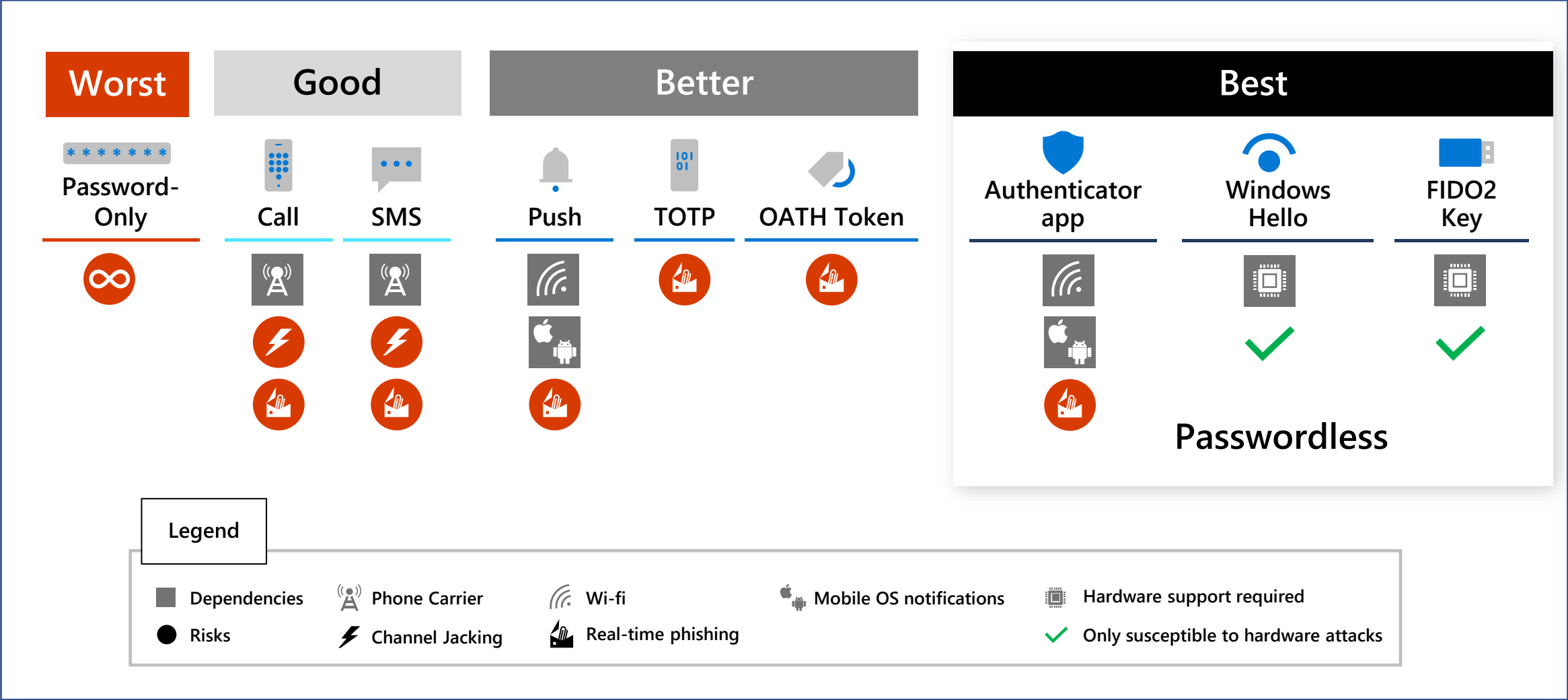
Authentication security levels

www.wpninjas.eu





Authentication security levels





Challenges in password authentication

- Passwords can be used anywhere
- Users are using same passwords almost everywhere
- Traditional MFA after password authentication is not a problem for real-time attacker
- The cost of password resets





Are we using it already?

www.wpninjas.eu





What is FIDO Alliance and W3C?

www.wpninjas.eu

- FIDO Alliance provides Client-to-Authentication Protocol (CTAP) specifications
- World Wide Web Consortium (W3C) provides Web Authentication (WebAuthn) specifications
- Together those are called FIDO2
- Together they provide open standards to tackle password challenges





What is FIDO and FIDO2?

www.wpninjas.eu

- FIDO = U2F = Way to give second factor authentication
- FIDO2 = Passwordless sign-in method provided by FIDO Alliance and W3C





Passwordless in Azure AD

- Easy to enable in cloud
- Little bit more to do if enabling in hybrid
- Several different options where to choose

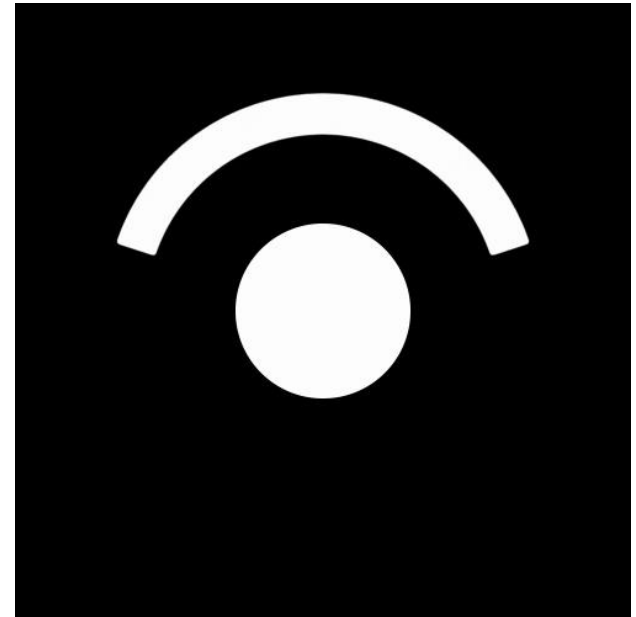
Method	Target	Enabled
FIDO2 Security Key	All users	Yes
Microsoft Authenticator	All users	Yes
Text message (preview)		No
Temporary Access Pass	All users	Yes
Certificate-based authentication (preview)		No



Windows Hello for Business

www.wpninjas.eu

- Based on certificates or asymmetric keys
- Stored in TPM and protected with gesture or PIN
- Gesture could be for example Facial Recognition or Fingerprint
- Credential is non-transferable → PIN works only with one device
- One device can contain 10 Windows Hello for Business identities





Windows Hello and Hello for business

www.wpninjas.eu

Windows Hello represents the biometric **framework** provided in Windows 10 and Windows 11.

Windows Hello lets **users** use biometrics to sign into their devices by securely storing their username and password and releasing it for authentication when the user successfully identifies themselves using biometrics.

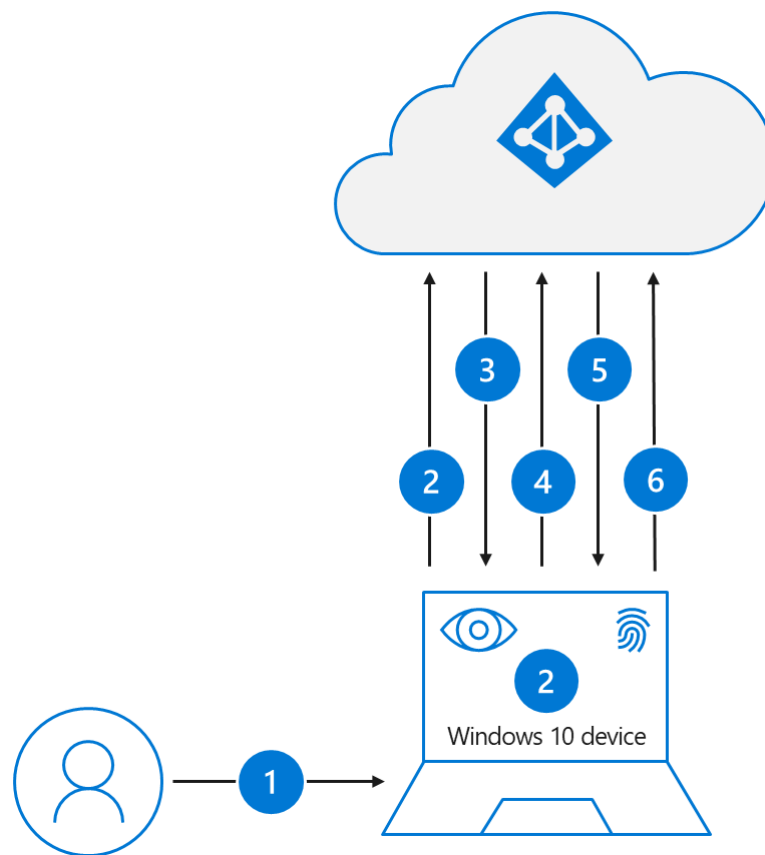
Windows Hello for Business uses **asymmetric keys** protected by the device's security module that requires a user gesture (PIN or biometrics) to authenticate.

Windows Hello for Business is configured by Group Policy or mobile device management (MDM) policy



WHfB under the hood

www.wpninjas.eu





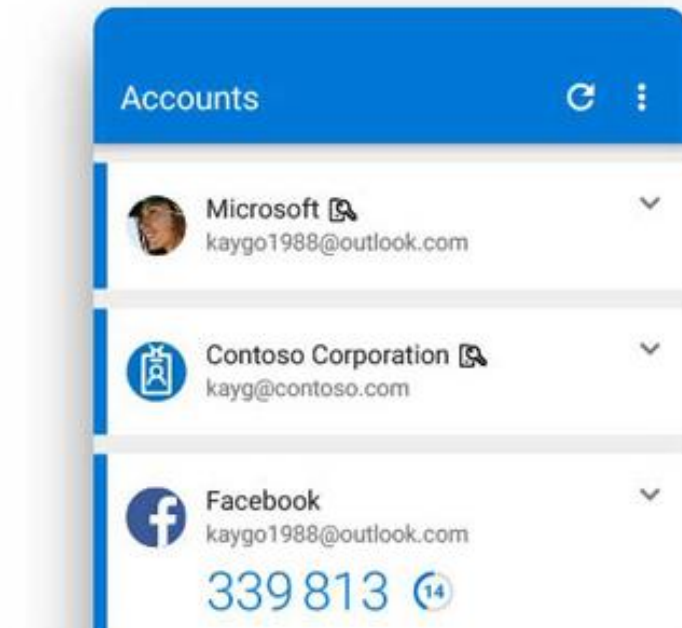
Microsoft Authenticator

www.wpninjas.eu

- Multiple identities, but one can only be passwordless
- Requires device to be registered towards the specific Azure AD tenant
- Cloud backup is backing up only account names
 - When phone is changed, everything should be re-registered



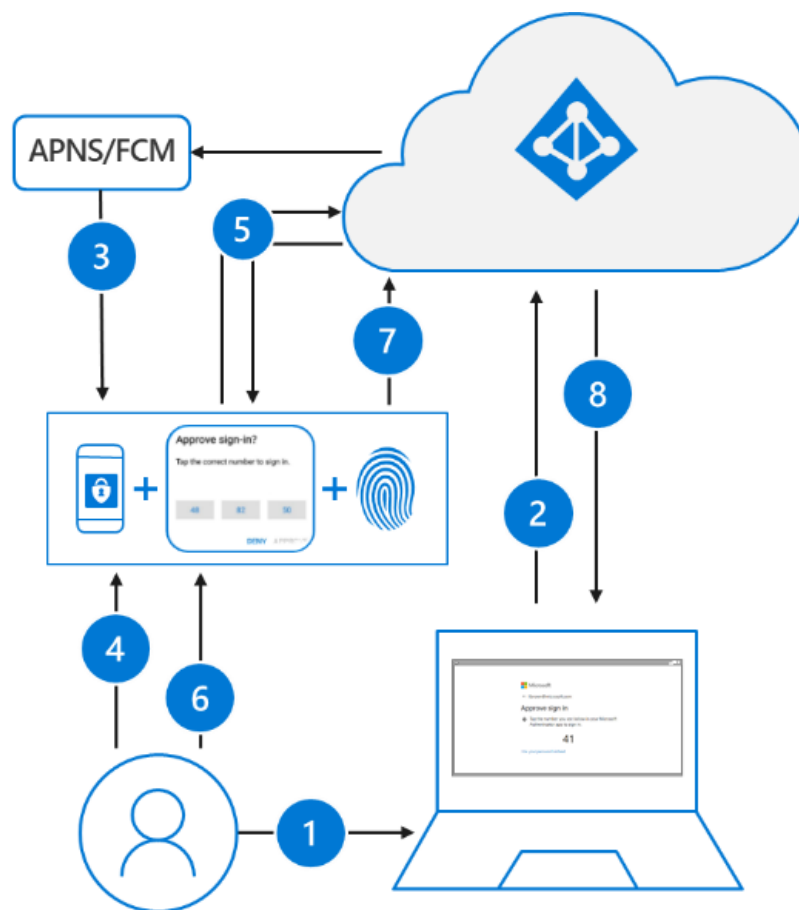
**Microsoft
Authenticator**
Microsoft Corporation





Microsoft Authenticator under the hood

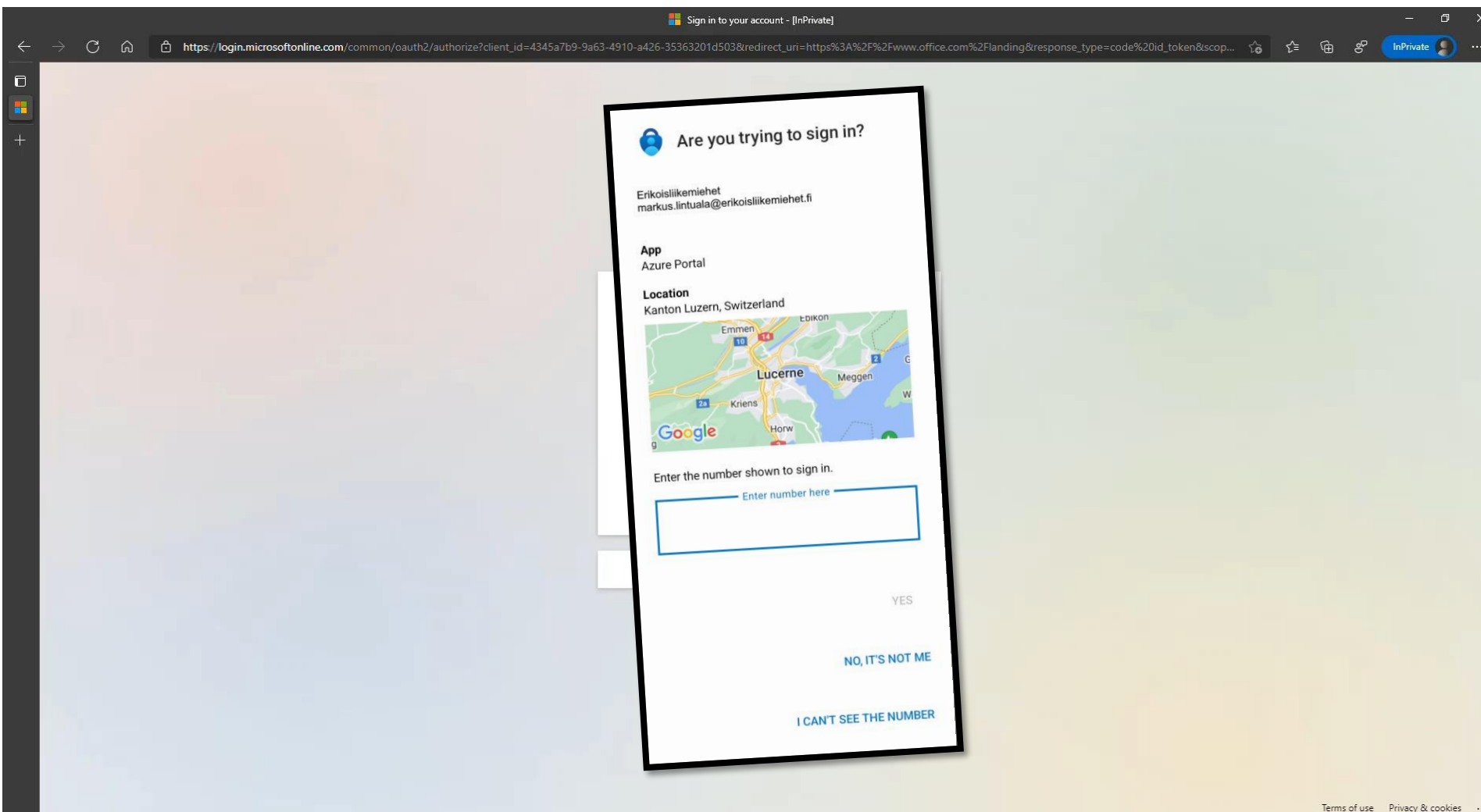
www.wpninjas.eu





Microsoft Authenticator under the hood

www.wpninjas.eu





FIDO2 Security Key

www.wpninjas.eu



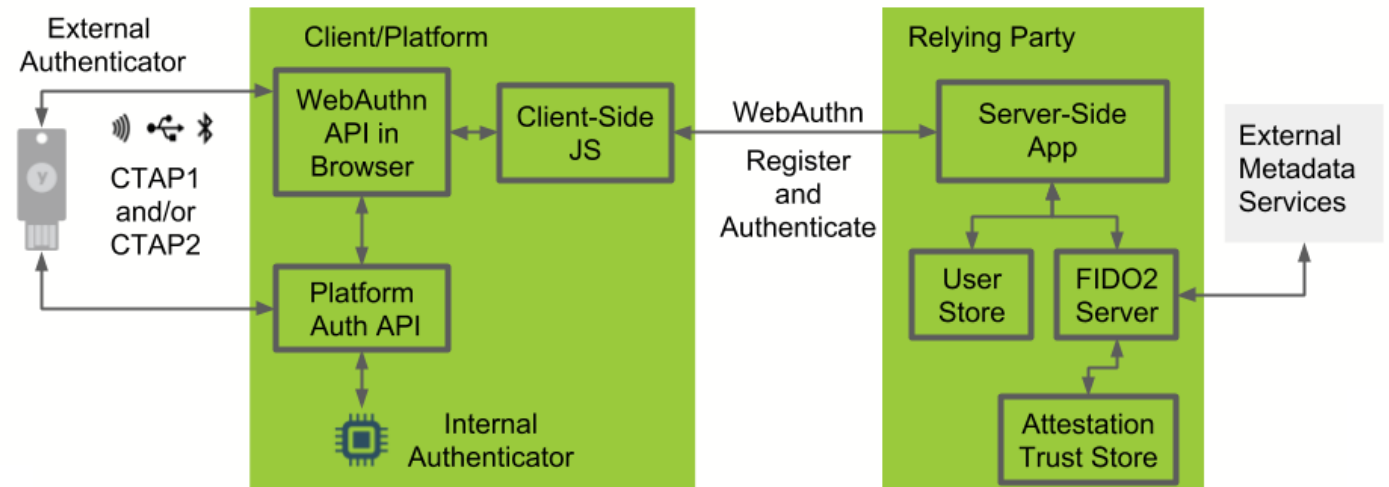
[Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs](#)



FIDO2 Security Key

- Private key is stored in a security key
- Provides also usernameless authentication with discoverable credentials feature
- Uses CTAP2 protocol on external authenticator

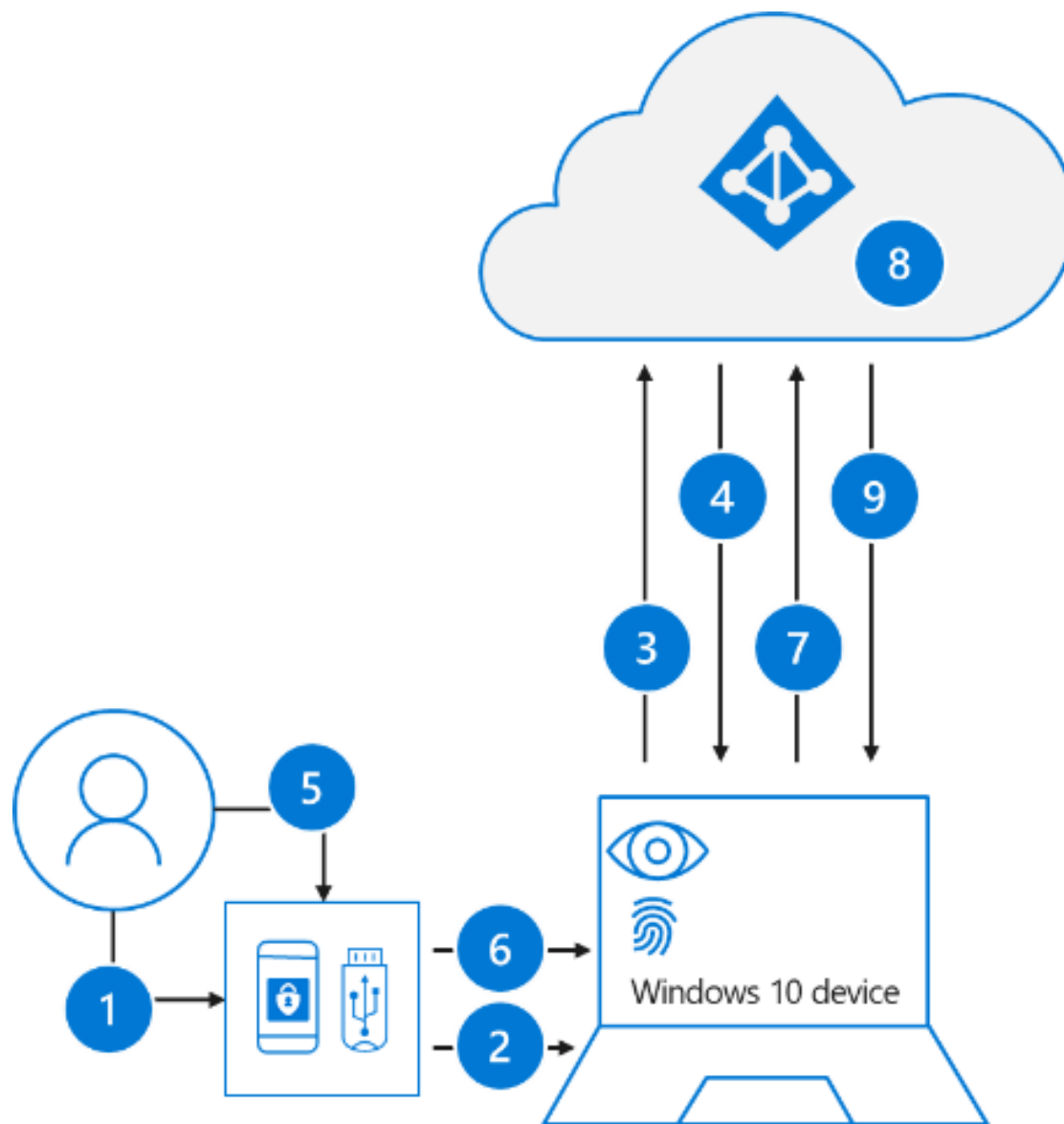
FIDO2 Application Architecture





Security key under the hood

www.wpninjas.eu





Security key in browser

www.wpninjas.eu

Sign in to your account

https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response_type=co...

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

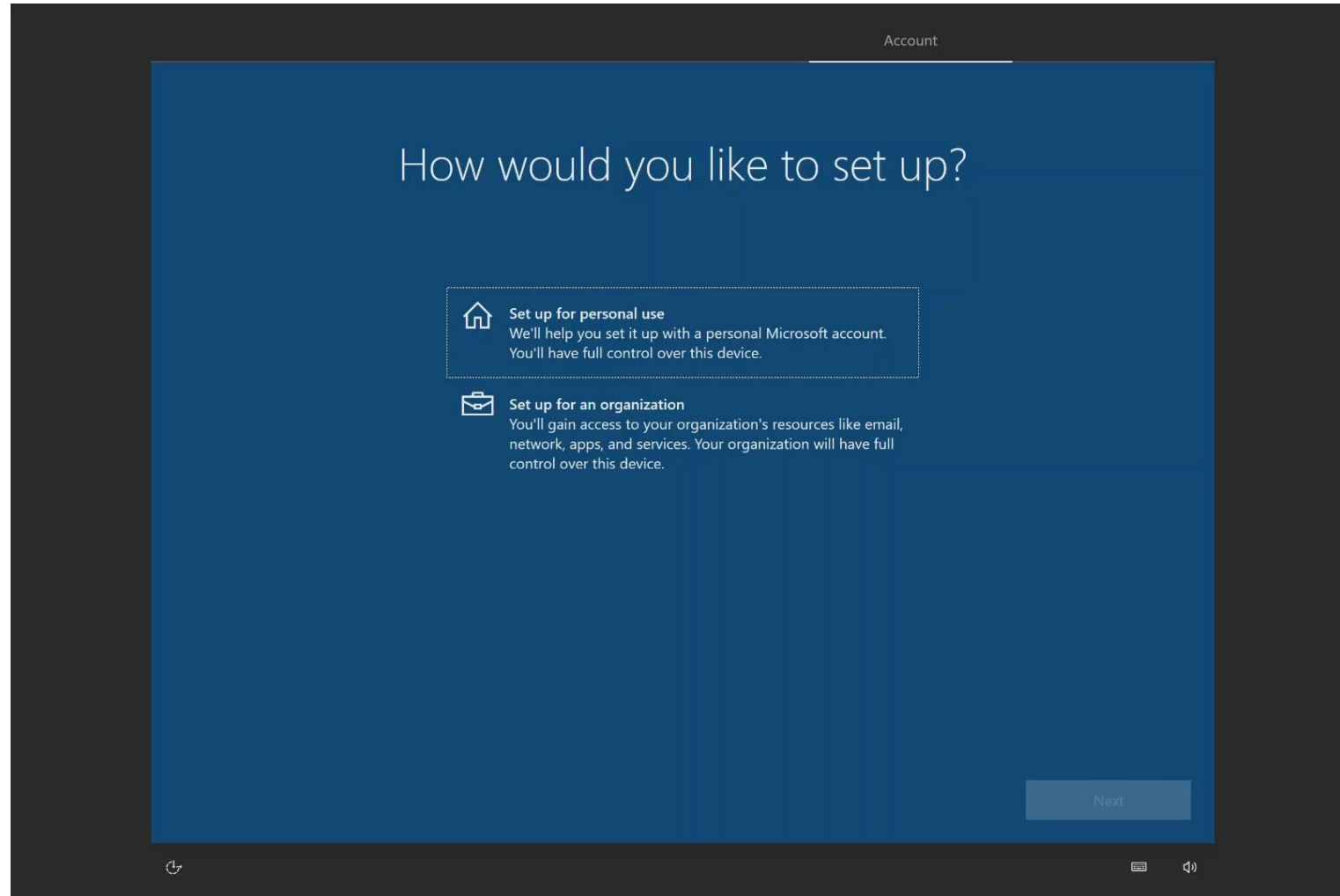
Sign-in options

Terms of use Privacy & cookies ...



Security key on enrollment

www.wpninjas.eu





Temporary Access Pass

- One time password to get user onboarded
- Temporary sign-in without a MFA
- Requirements can be set on tenant level
- When creating a temporary access pass, settings can be modified
- Accessible via API

The screenshot shows a Microsoft sign-in window. At the top is the Microsoft logo. Below it is the email address 'markus.demo@erikoisliikemiehet.fi' with a back arrow. The main heading is 'Enter Temporary Access Pass'. Below this is a text input field containing 'Temporary Access Pass'. Under the input field is a checkbox labeled 'Show Temporary Access Pass'. Below the checkbox is a blue link that says 'Use your password instead'. At the bottom right is a blue 'Sign in' button.



Temporary access pass settings

Setting	Default values	Allowed values	Comments
Minimum lifetime	1 hour	10 – 43200 Minutes (30 days)	Minimum number of minutes that the Temporary Access Pass is valid.
Maximum lifetime	24 hours	10 – 43200 Minutes (30 days)	Maximum number of minutes that the Temporary Access Pass is valid.
Default lifetime	1 hour	10 – 43200 Minutes (30 days)	Default values can be override by the individual passes, within the minimum and maximum lifetime configured by the policy.
One-time use	False	True / False	When the policy is set to false, passes in the tenant can be used either once or more than once during its validity (maximum lifetime). By enforcing one-time use in the Temporary Access Pass policy, all passes created in the tenant will be created as one-time use.
Length	8	8-48 characters	Defines the length of the passcode.



Registration experience

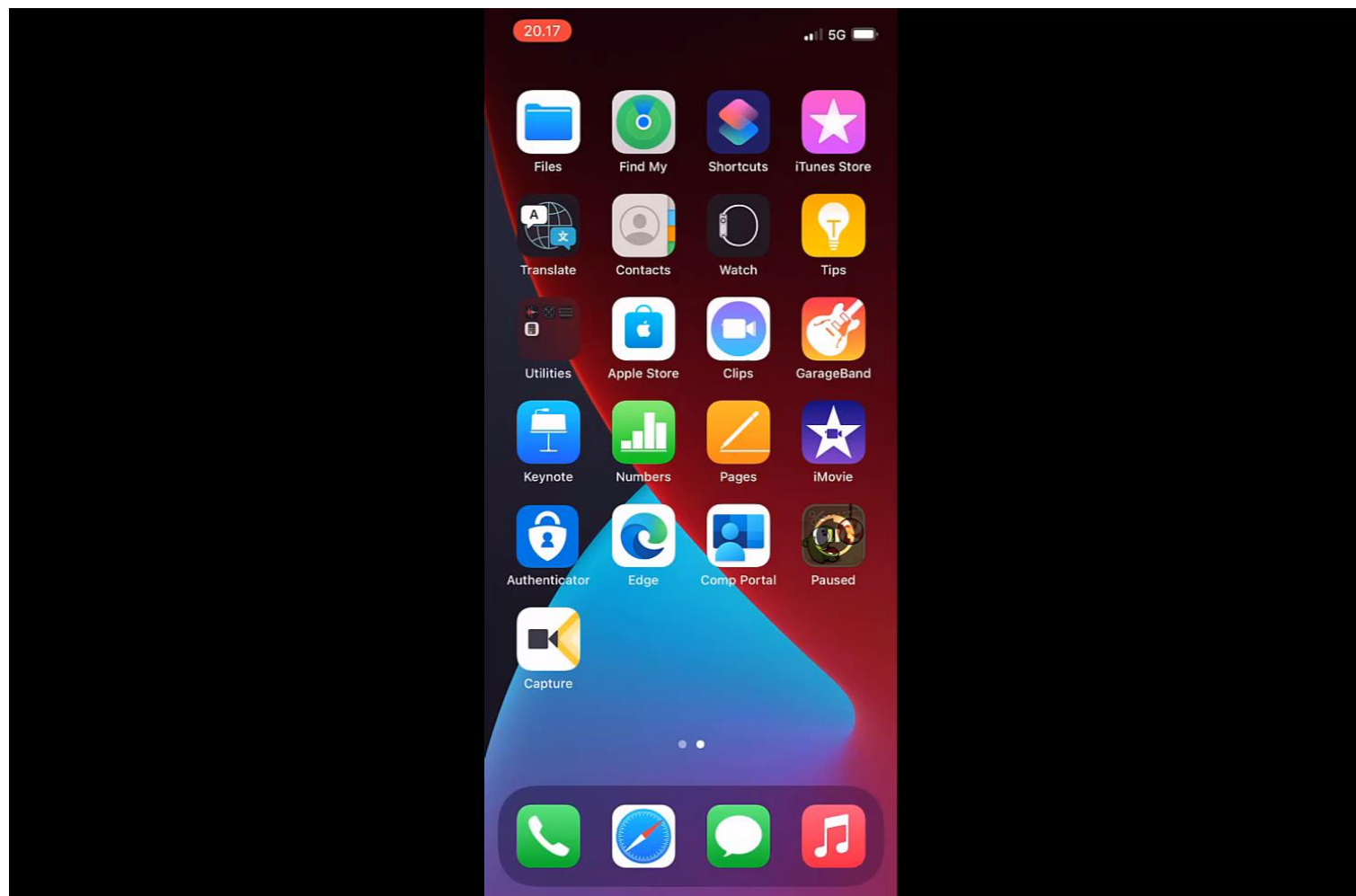
- Windows Hello for Business experience starts in Windows itself
- Microsoft Authenticator experience is initiated in Authenticator
- Security key registration is initiated in browser





Registering Microsoft Authenticator

www.wpninjas.eu






Security key registration

www.wpninjas.eu

New tab - [InPrivate]

← → ↻ 🏠 🔍 <https://aka.ms/mysecurityinfo> ☆ 📌 🔍 InPrivate ...

For quick access, place your favorites here on the favorites bar. Looking for your favorites? [Check your profiles](#)



InPrivate browsing

InPrivate search with Microsoft Bing 🔍

✓ **What InPrivate browsing does**

- Deletes your browsing info when you close all InPrivate windows
- Saves collections, favorites, and downloads (but not download history)
- Prevents Microsoft Bing searches from being associated with you

✗ **What InPrivate browsing doesn't do**

- Hide your browsing from your school, employer, or internet service provider
- Give you additional protection from [tracking](#) by default
- Add additional protection to what's available in normal browsing

Always use "Strict" tracking prevention when browsing InPrivate

If this is off, we'll use the same tracking prevention setting as a normal browsing window

☐

↓ More details



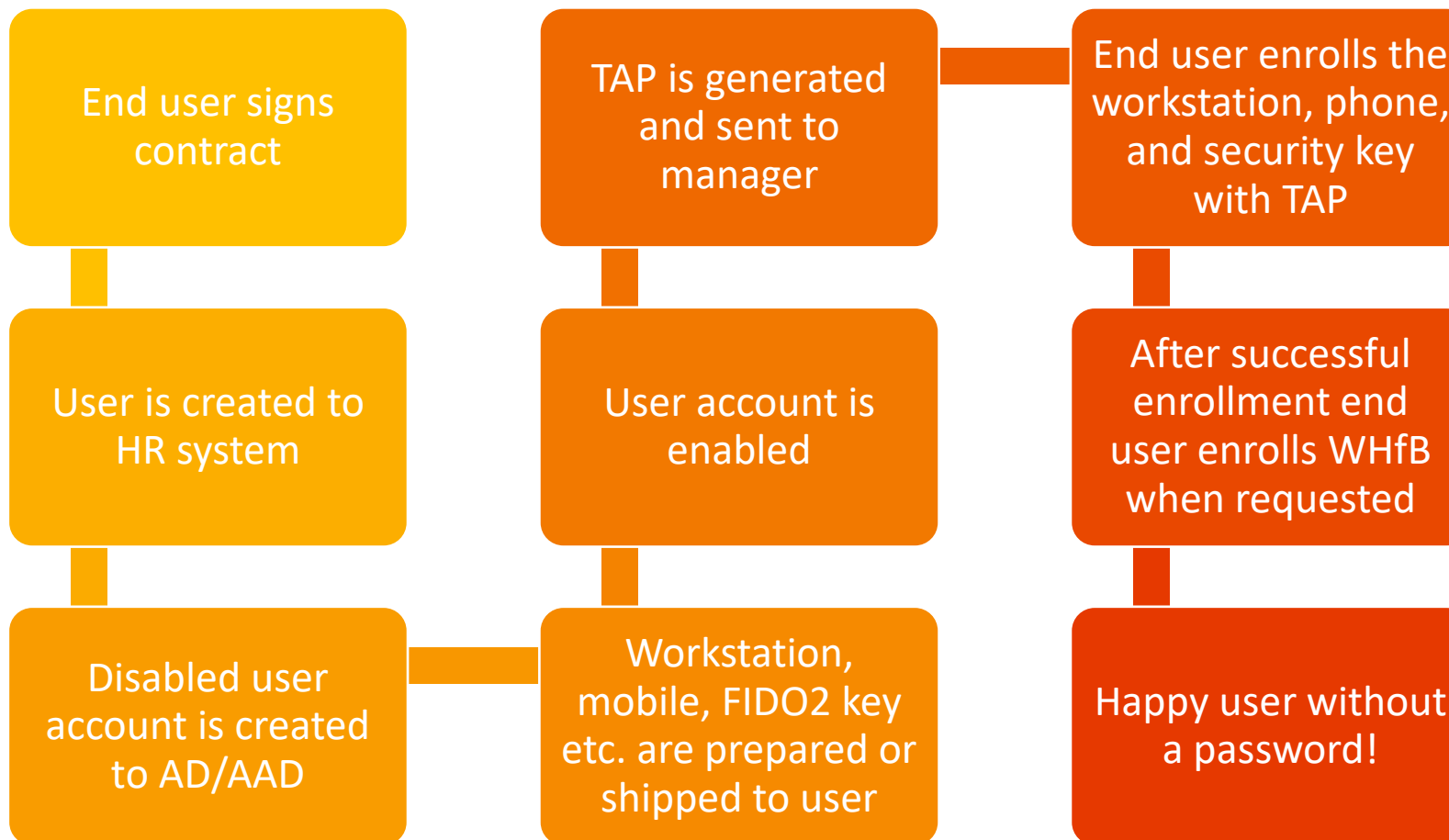
FIDO2 Registration under the hood

www.wpninjas.eu

- Let's draw...



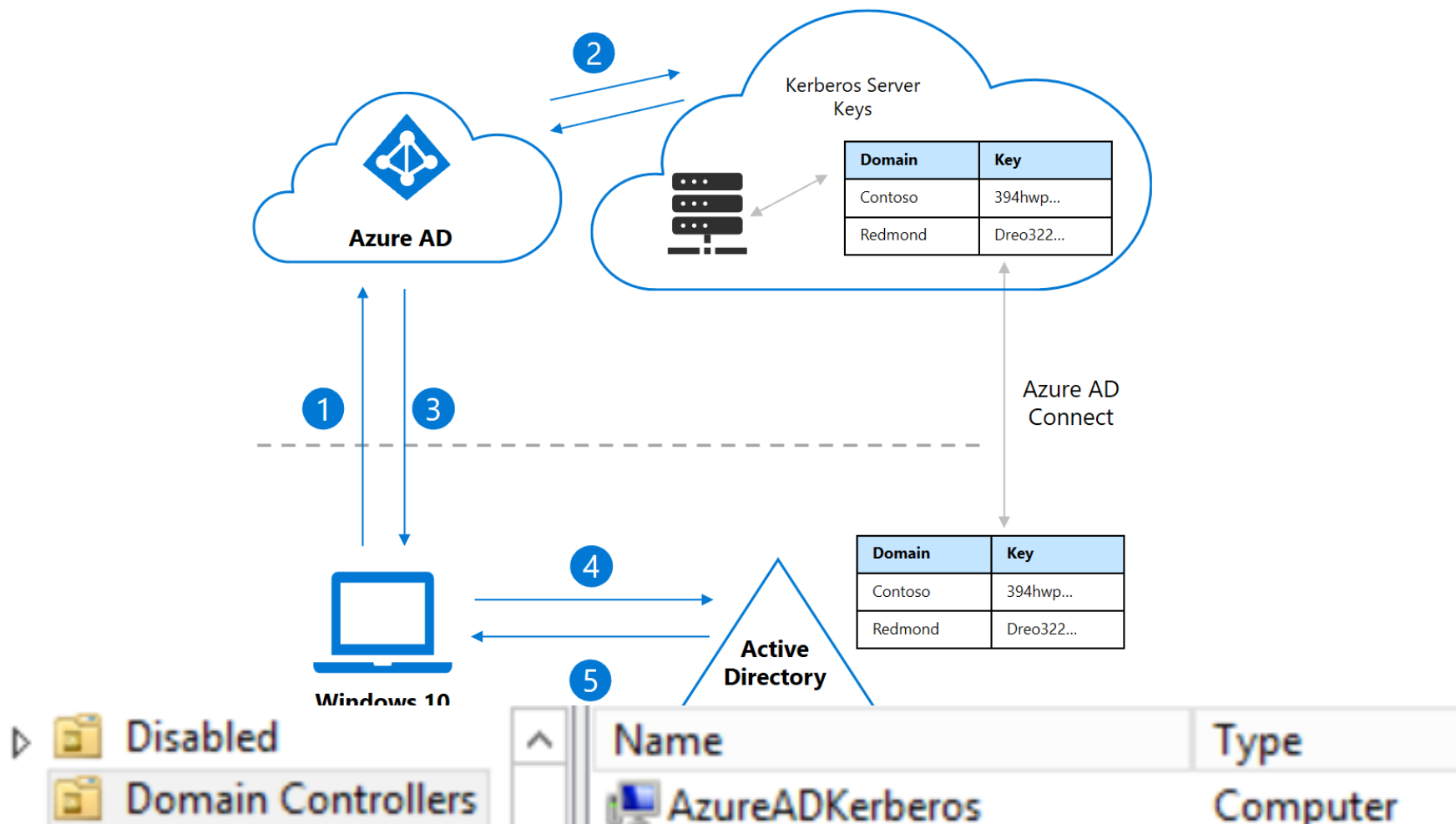
Real life use case





Still in hybrid? – No problem!

www.wpninjas.eu





Still in hybrid? – No problem!

www.wpninjas.eu

Multi-valued Distinguished Name With Security Principal Editor

Attribute: msDS-NeverRevealGroup

Values:

Name	Container	Distinguished Name / SID
Account Operators		CN=Account Operators,CN=Builtin...
Server Operators		CN=Server Operators,CN=Builtin,...
Domain Admins		CN=Domain Admins,CN=Users,DC...
Cert Publishers		CN=Cert Publishers,CN=Users,DC...
Enterprise Admins		CN=Enterprise Admins,CN=Users,...
Schema Admins		CN=Schema Admins,CN=Users,D...
Domain Controllers		CN=Domain Controllers,CN=Users...
Backup Operators		CN=Backup Operators,CN=Builtin,...
Administrators		CN=Administrators,CN=Builtin,DC...

Add Windows Account... Remove

Add DN...

OK Cancel



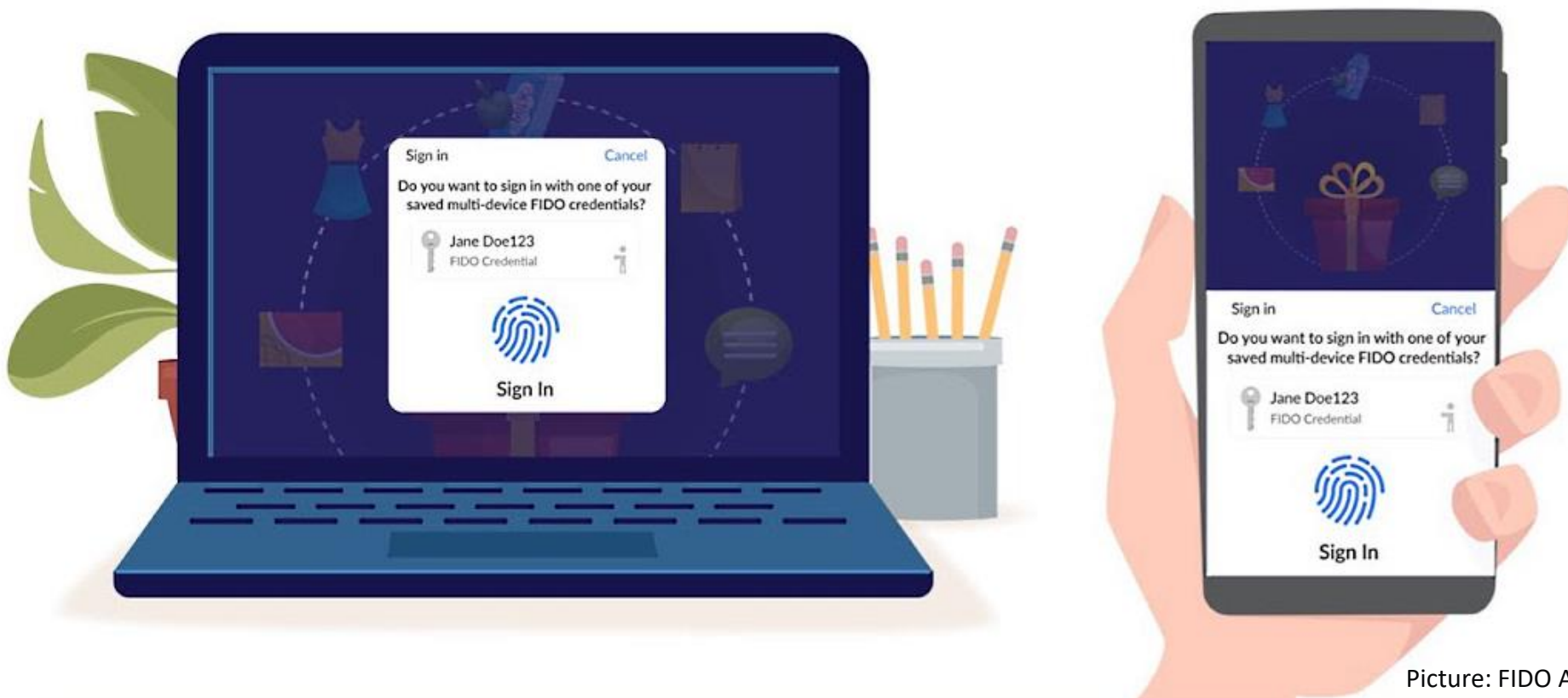
Future of passwordless

- Passwordless to remote desktop sessions including Azure Virtual Desktop and Windows 365 requires WebAuthn redirection
- Requires the source operating system and target session host to be at least Windows 11 2H22 Enterprise x64
- [Azure Virtual Desktop identities and authentication - Azure | Microsoft Docs](#)



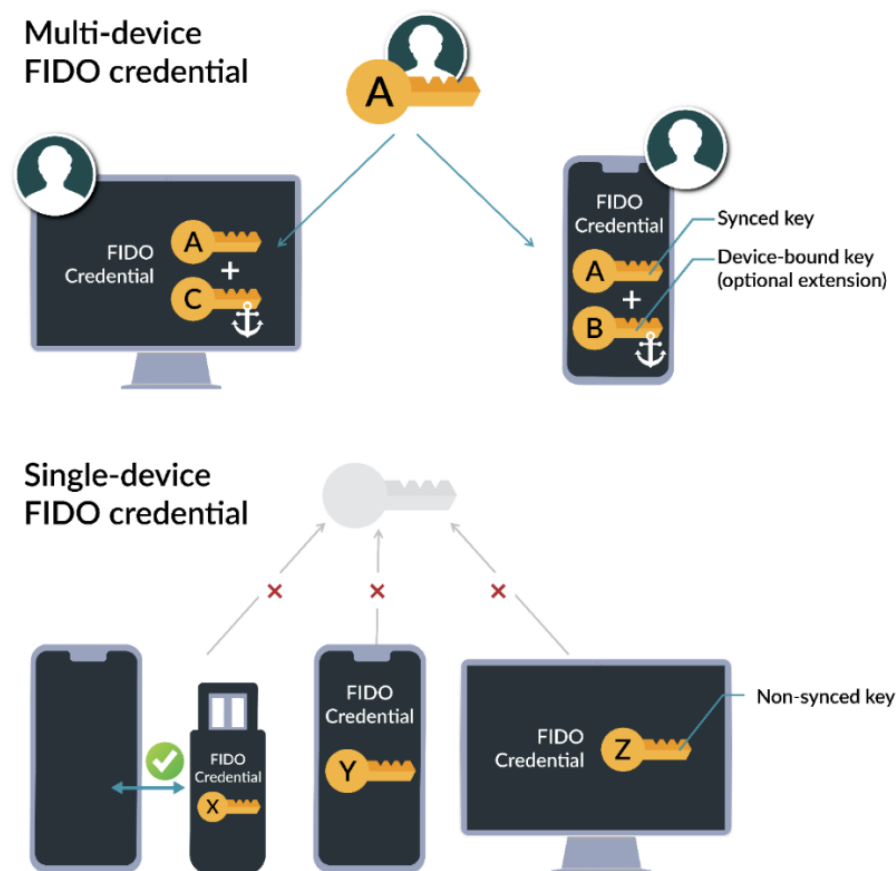
Future of passwordless

- Multi-device FIDO
- Apple, Google and Microsoft are working together to make the world passwordless





Multi device FIDO credentials



Picture: FIDO Alliance



Are those really phishing proof?

www.wpninjas.eu

- For now 9/2022 – Yes
- Public key architecture is phishing proof as long as private key stays private





How to get started?

- Plan what you want to achieve – make your passwordless strategy
- Enable passwordless as an option
- Convert all sign in processes to single sign on
- Challenge users to use passwordless methods
- Restrict use of passwords





Key takeaways

- Start testing and using passwordless
- Make a passwordless strategy
- Use single sign-on
- Provide more than one method for passwordless





Thank You



Workplace Ninja Summit 2022