# Passwordless 2025

# Mika Vilpo

*IT Geek Building Clouds*

*@Elisa Oyj*

Like to talk about identity, automation and serverless

25+ years in IT and 15+ years in cloud

Spending free time as Red Cross volunteer in disaster management, first aid and search & rescue


mika@vilpo.fi

@mikavilpo

Microsoft Certified: Azure Solutions Architect Expert

Microsoft Certified: Cybersecurity Architect Expert

Microsoft Certified: DevOps Engineer Expert

Microsoft 365 Certified: Enterprise Administrator Expert

Microsoft Certified Trainer: MCT

# What is Passwordless Authentication?

AUTHENTICATION METHODS NOT RELIANT ON PASSWORDS

BENEFITS:

SECURITY, USABILITY, COST

EXAMPLES:

WINDOWS HELLO, FIDO2, PASSKEYS, MICROSOFT AUTHENTICATOR

# Current State (3.6.2025)

- Entra ID supports
  - Passkeys (FIDO2)
  - Windows Hello for Business
  - Authenticator App
  - Certificates
    - on smartcards
    - on smartcard emulators
  - Temporary Access Pass (TAP)
- Most ”real” web services support passkeys
- Google, Apple, Microsoft aligned on passkeys

# What’s Sunsetting / Deprecated

- SMS and voice-based MFA are being deprecated in best practices
- Legacy MFA settings phased out
- Legacy Multifactor Authentication (MFA) and Self-Service Password Reset (SSPR) Policies
  → Converged Policy

# Passkeys

*FIDO2 is a broad authentication standard enabling passwordless login using hardware or biometric credentials, while passkeys are a user-friendly implementation of FIDO2 credentials that sync across devices and are designed to replace passwords entirely.*

- Public/private key pair: user device holds private key
  - Unique for each service
- Auth with biometric/PIN, no shared secret
  - Something you have (passkey) and something you know (PIN) or something you are (biometrics)
- Domain binding prevents replay attacks (discoverable FIDO2 → Passkey)

- Can be stored (with Entra ID support)
  - External device (USB, Bluetooth)
  - Microsoft Authenticator
  - (Windows Hello)

# How can we use these Passkeys with Entra ID?

## External device (USB, NFC, Bluetooth) aka. Security Key

- USB-stick, FIDO2 with Bluetooth

## Microsoft Authenticator (on Android or iOS)

- Locally on mobile device
- Via Bluetooth on different device
- NB: Does not require device registration on Entra ID

## Windows Hello

- Used in background for WHfB, keys visible but not creatable in UI.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-fido2-compatibility

# Where can we use Passkeys with Entra ID?

- Web applications
- Apps that use modern authentication
- Windows login via Web sign-in credential provider
  - Enables also TAP support
  - NB: Only Entra Joined devices supported
  - NB: Requires internet
- Security key (USB etc.) works with Windows login

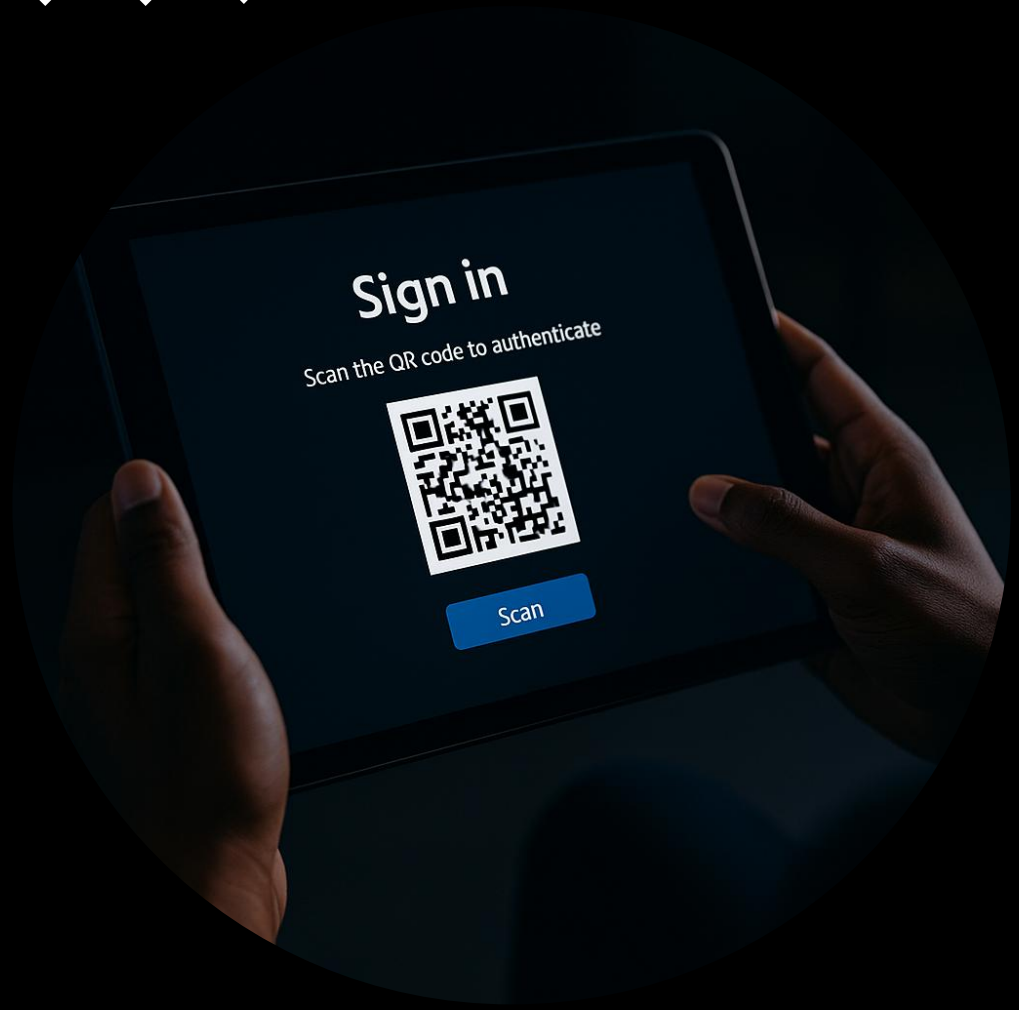
# Near-Future & Preview Features (Entra ID)

- Device-bound passkeys on mobile devices
- Roaming/synced Passkeys
- Passkeys on 3rd party password manager
- Provision Passkeys on behalf of user
- Platform Credential (Mac OS)

- QR codes for first line workers

**Microsoft Entra ID currently supports only device-bound passkeys stored on FIDO2 security keys or in Microsoft Authenticator.** Microsoft is committed to securing customers and users with passkeys, and **plans to support synced passkeys for Microsoft Entra ID.**

2.6.2025: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-fido2-compatibility




# QR codes for first line use cases

- QR-code + PIN
- Considered as single factor authentication
- Works only on mobile devices
  - Shared devices, kiosk modes
  - *Login to warehouse handheld device*
- QR scan → PIN → session

- Think twice before enabling

# Passkeys and RDP

Client Windows 10/11 (22H2) and Windows Server 2022+ that is Entra joined/hybrid joined are good to go

Azure Virtual Desktop, Windows 365 and DevBox are good to go
(at least when using native clients, not web)

**In session** (WebAuthn redirect) is supported with Windows Server 2022+

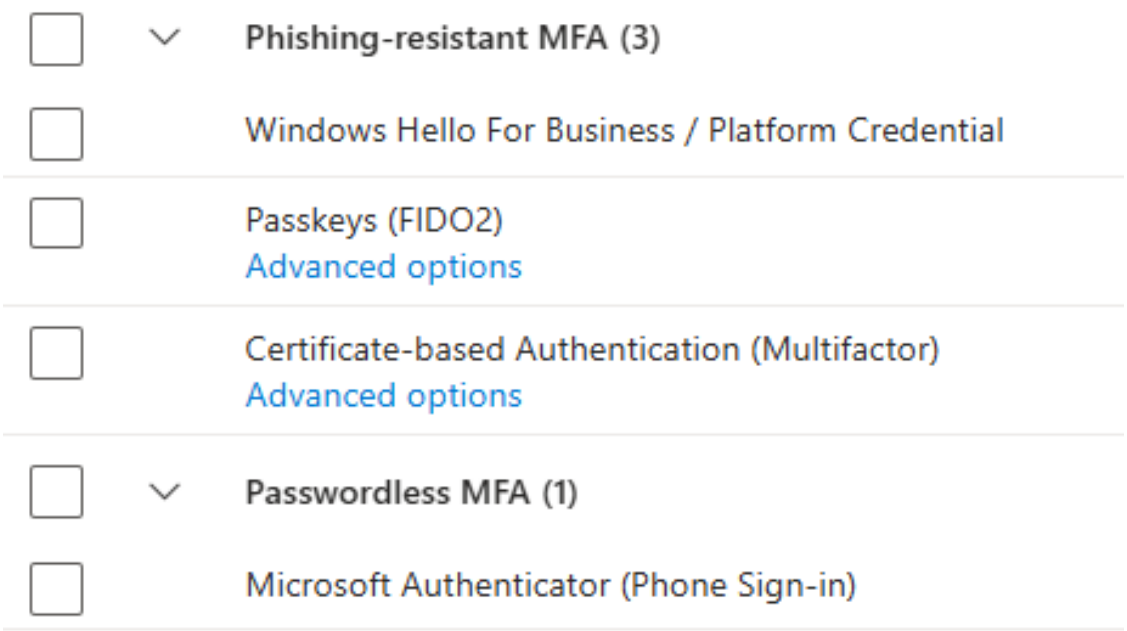
No mobile device support

https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-plan-rdp-phishing-resistant-passwordless-authentication
https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/passwordless-authentication-with-fido2-security-key-for-remote-desktop-connectio/4398347

# Authentication Strengths

- Can define what authentication methods are usable and when
  - Works with Conditional Access and Authentication Context
- Whitelist/blacklist what passwordless methods are allowed and what are not
- Whitelist/blacklist passkey types

- **PIM:** Global Admin requires approved FIDO2 device
- **Protected Actions:** Deletion of objects requires Phishing Resistant authentication



# User Adoption Strategy

Enable passwordless methods to everybody to use

Pilot with IT/security champions

Train and communicate benefits

Think what methods to boost for different personas

# What next?

- Enable possibility to use passwordless
- Evaluate what is coming
- It’s all about communication to the users
- Secure admin actions with strong and phishing resistant authentication


Q & A

# Resources & References

- Microsoft: https://aka.ms/passwordless
- FIDO Alliance: https://fidoalliance.org
- Passkeys: https://www.passkeys.dev
- Entra Auth Strengths: https://learn.microsoft.com/en-us/entra/id-protection/howto-authentication-strengths
- Phishing-Resistance: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths#phishing-resistant-mfa
- RDP Passwordless: https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-plan-rdp-phishing-resistant-passwordless-authentication