Přichází čas Passwordless?

Petr Vlk
Microsoft MVP
Microsoft 365 Enterprise Security Architect @ KPCS CZ
KPCS vlk@kpcs.cz

Statistika úvodem

Hesla nejsou unikátní napříč službami

63 %

pracovníků přiznává používání stejných hesel

Hesla jsou obecně slabou ochranou

80 %

útoků spočívalo v kompromitaci hesla uživatele / správce

Hesla stojí za finančními škodami

3 mil. Kč

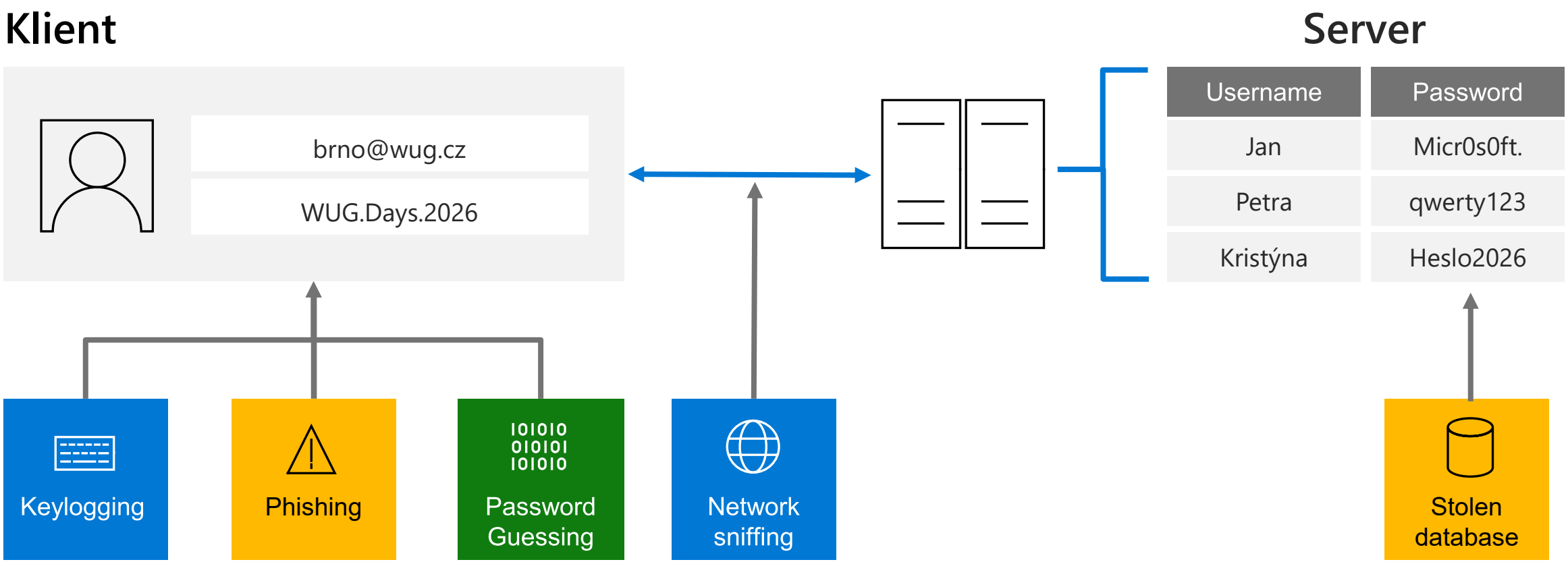
Průměrná cena narušení bezpečnosti po útoku

Hesla generují zbytečnou zátěž IT podpory

25 %

tiketů na podpoře se týká resetů hesel

Záleží na heslu, nebo na druhém faktoru?



Útoky na identitu jsou útokem na hesla

- **99 % útoků na identitu jsou útokem na heslo**
  - Breach Replay
  - Password Spray
  - Phishing
- **1 % útoků jsou útokem na pověření uživatele**
  - MFA
    - Swim Swapping
    - MFA Fatigue
    - Adversary in the Middle (AitM)
  - Post-Authentication
    - Token Theft
    - Consent Phishing
  - Infrastructure Compromise
- *PS: Tato statistika se i brzy obrátí, viz práce Michael Grafnetter.* 😉

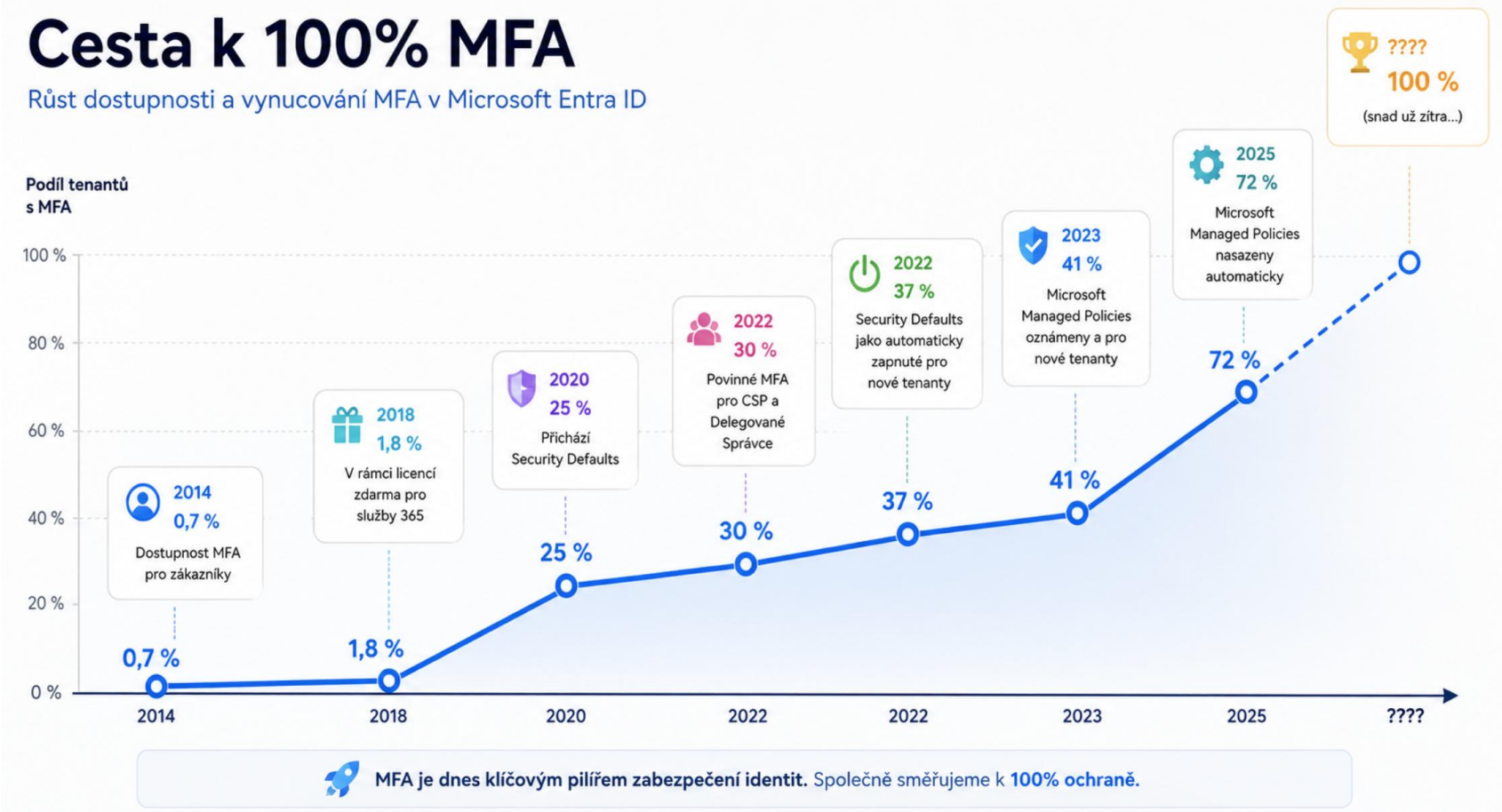
Inovace hesel

- Diskutabilní dopad pravidelné změny hesel
- Komplexita negeneruje bezpečná nebo unikátní hesla
- Kontroly neobsahují uniklá a organizačně nebezpečná hesla
  - WUG2026!
  - Heslo123.
- NIST Password Guidance
  - Lepší délka než komplexita, minimálně 12, lépe 16 znaků
  - Eliminace povinné expirace hesel
  - Heslo obratem změňte v případě kompromitace
  - Podpora pro všechny ASCII a Unicode znaky
  - Zakázání nápověd pro hesel
  - Podpora pro využití správců hesel

Adopce MFA

- 2014 – 0,7 % (dostupnost MFA pro zákazníky)
- 2018 – 1,8 % (v rámci licencí zdarma pro služby 365)
- 2020 – 25 % (přichází Security Defaults)
- 2022 – 30 % (Povinné MFA pro CSP a Delegované Správce)
- 2022 – 37 % (Security Defaults jako automaticky zapnuté pro nové tenanty)
- 2023 – 41 % (Microsoft Managed Policies oznámeny a pro nové tenanty)
- 2025 – 72 % (Microsoft Managed Policies nasazeny automaticky)
- ???? – 100 %?(snad už zítra…)

Adopce MFA


Cesta k 100% MFA
Růst dostupnosti a vynucování MFA v Microsoft Entra ID
Podíl tenantů s MFA
100 %
80 %
60 %
40 %
20 %
0 %
2014
0,7 %
Dostupnost MFA pro zákazníky
2018
1,8 %
V rámci licencí zdarma pro služby 365
2020
25 %
Přichází Security Defaults
2022
30 %
Povinné MFA pro CSP a Delegované Správce
2022
37 %
Security Defaults jako automaticky zapnuté pro nové tenanty
2023
41 %
Microsoft Managed Policies oznámeny a pro nové tenanty
2025
72 %
Microsoft Managed Policies nasazeny automaticky
????
100 %
(snad už zítra...)
0,7 %
1,8 %
25 %
30 %
37 %
41 %
72 %
2014
2018
2020
2022
2022
2023
2025
????
MFA je dnes klíčovým pilířem zabezpečení identit. Společně směřujeme k 100% ochraně.

Silné MFA nebo Phishing Resistant MFA

- Ne všechny faktory jsou si rovny svoji kvalitou a lze je ze zařízení zcizit
  - Telefonát
  - SMS
  - TOTP
  - OATH
- Silné MFA
  - Nevyžaduje manuální dodatečné zadání znalostního faktoru od uživatele
  - Authenticator (Push ovšem s Number Matching)
- Phishing Resistant
  - Návrhově odolné proti phishing útoku a podvržení ověřovatele
  - PKI / CBA
  - FIDO2 / Passkeys
  - Windows Hello for Business

Než jsme to nasadili…

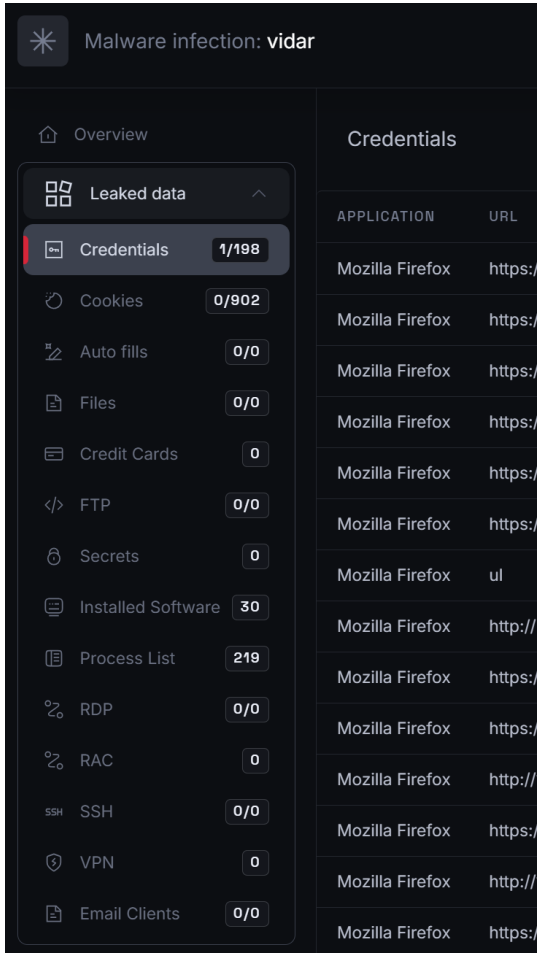
- Útočníci už se adaptovali.
  - 146 % nárůst AitM kampaní
- MFA Bypass
  - AitM Phishing
  - Device Code Flow
- Token Theft
  - PRT a Cookies
  - Vynucení kryptografického otisku TPM
  - Entra ID: Token Protection
  - Chrome: Device Bound Session Credentials

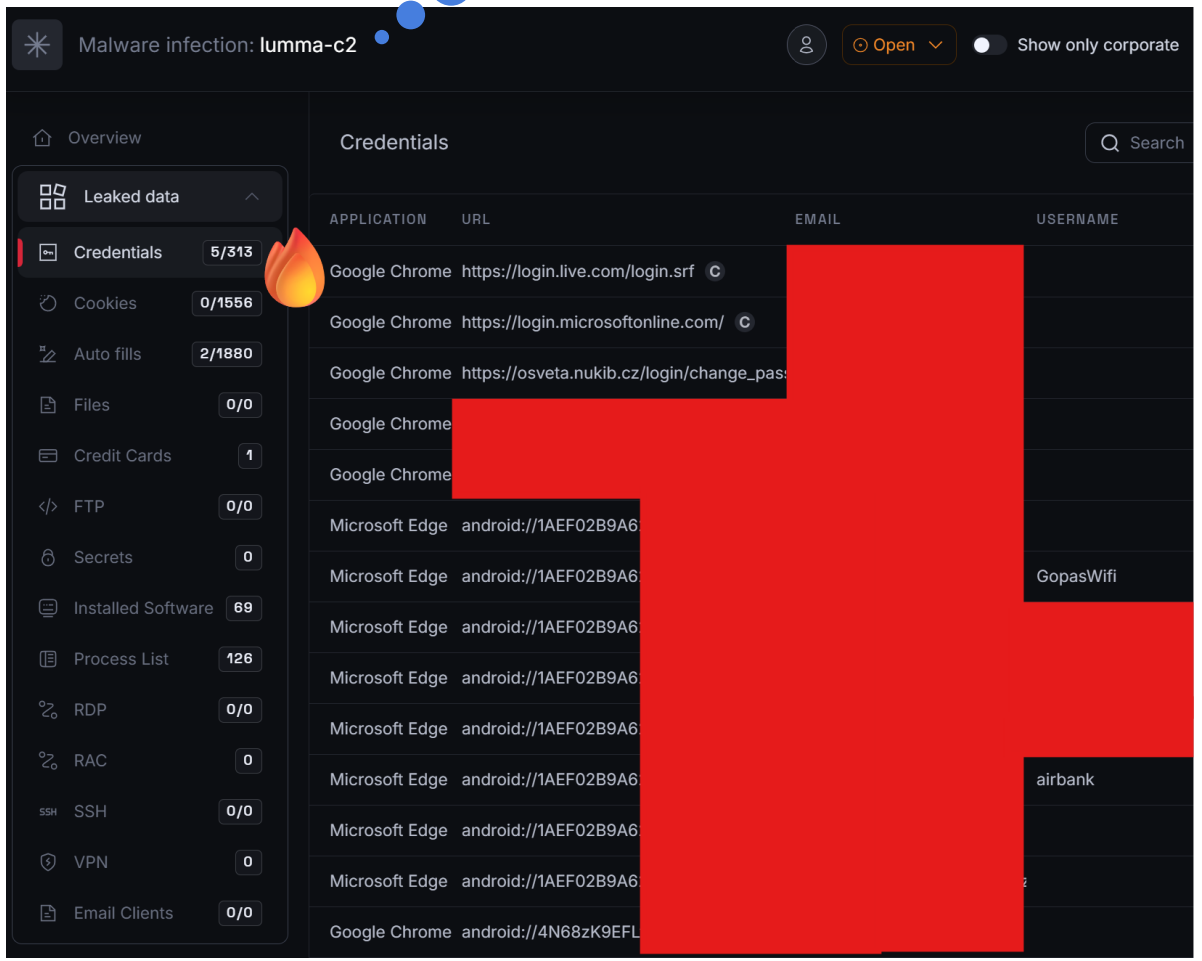
Odbočka: Infostealer

Chcete vědět, jak to vypadá ve vaší organizaci? Dejte vědět KPCS.

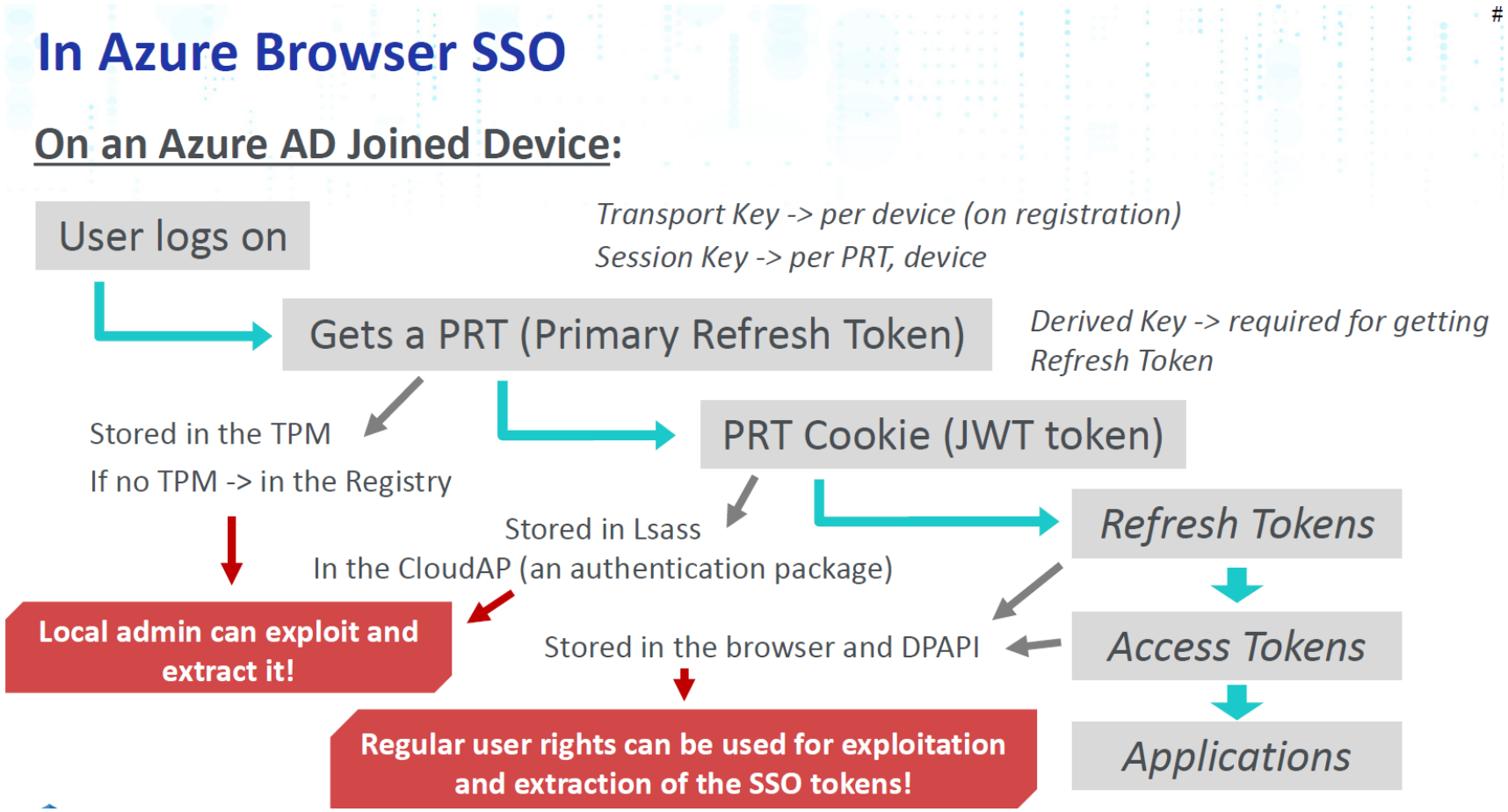
- Edge
- Chrome
- Firefox

- Credentials
- Cookies
- Auto Fill





Odbočka: Lokální správci a eskalace



Proč tedy nyní?

- Protože chceme zvýšit úroveň zabezpečení přihlašování
  - Zvýšit odolnost proti phishing útokům na základě analýzy rizik…
- Protože se na nás řítí regulace
  - ZokB: Povinná osoba při ověření identity administrátorů, uživatelů a technických aktiv
    - a) využívá autentizační mechanismus, který je založen na vícefaktorové autentizaci s alespoň dvěma různými typy faktorů, nebo využívá autentizační mechanismus, který je založen na aktuálně odolné kontinuální autentizaci založené na modelu nulové důvěry,
    - b) a do doby splnění požadavků podle písmene a) využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.
  - DORA: Metody ověřování zahrnující všechny tyto prvky:
    - i) používání metod ověřování, které jsou úměrné klasifikaci stanovené v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554 a celkovému rizikovému profilu aktiv v oblasti IKT a zohledňují osvědčené postupy;
    - ii) používání metod silného ověření v souladu s osvědčenými postupy a technikami pro vzdálený přístup do sítě finančního subjektu, pro privilegovaný přístup, pro přístup k aktivům v oblasti IKT podporujícím zásadní nebo důležité funkce nebo k veřejně přístupným aktivům v oblasti IKT;

Proč tedy nyní?

- nZoKB
  - Když nemáte MFA…
  - … a i když ho máte…
  - … musí být hesla lepší.

(4) Povinná osoba do doby splnění požadavku podle odstavce 2 využívá nástroj založený na autentizaci pomocí identifikátoru účtu a hesla, kdy tento nástroj musí vynucovat pravidlo

a) délky hesla alespoň

1. 12 znaků pro účty uživatelů,

2. 17 znaků pro účty administrátorů,

3. 22 znaků pro účty technických aktiv,

b) umožňující zadat heslo o délce alespoň 64 znaků,

c) neomezující použití malých a velkých písmen, číslic a speciálních znaků,

d) umožňující uživatelům a administrátorům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut,

e) povinné změny hesla v intervalu alespoň jednou za 18 měsíců a

f) neumožňující uživatelům a administrátorům

1. zvolit si jednoduchá a často používaná hesla,

2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, adresy elektronické pošty, názvu systému nebo obdobným způsobem a

3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.

(5) Povinná osoba v souladu s odstavcem 4 zajistí

a) bezodkladné vynucení změny výchozího hesla uživatelů a administrátorů po prvním přihlášení,

b) bezodkladné vynucení změny výchozího hesla technického aktiva,

c) vytváření hesla účtu technického aktiva složeného z náhodného řetězce malých a velkých písmen, číslic a speciálních znaků,

d) bezodkladné vynucení změny přístupového hesla v případě důvodného podezření na narušení jeho důvěrnosti,

e) vytvoření náhodného výchozího hesla nebo identifikátoru sloužícího k vytvoření nebo k obnovení přístupu a zajistí jeho důvěrnost a

f) bezodkladné zneplatnění hesla nebo identifikátoru sloužícího k vytvoření nebo k obnovení přístupu po jeho prvním použití nebo uplynutí nejvýše 24 hodin od jeho vytvoření.

(6) Povinná osoba u administrátorského účtu zejména určeného pro případ obnovy po kybernetickém bezpečnostním incidentu musí zajistit

a) bezodkladnou změnu výchozího hesla,

b) vytvoření hesla náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,

c) délku hesla složeného alespoň z 22 znaků,

d) bezpečné uložení hesla,

e) omezení manipulace s účtem a jeho heslem, kdy s tímto účtem a jeho heslem mohou manipulovat pouze pověřené osoby, a to v nezbytně nutných případech,

f) změnu hesla po jeho použití, při jakékoli změně pověřených osob, v případě důvodného podezření na jeho kompromitaci nebo v intervalu alespoň jednou za 18 měsíců a

g) evidování manipulace a pokusy o manipulaci s tímto účtem a jeho heslem.

Proč tedy nyní?

- Protože Passkeys preferují výrobci webových stránek a aplikací
  - Slevomat
  - Salesforce
- Protože Passkeys preferují výrobci platforem
  - Microsoft na Windows
  - Google na Android
  - Apple na iOS a také macOS
- Ale především protože Passkeys preferují poskytovatelé identit (IdP)
  - Microsoft Account v rámci Microsoft 365 Personal a Family
  - Entra ID v rámci Microsoft 365 Business a Enterprise
    - Výchozí preferovaný faktor k registraci (Authenticator)
    - Registrační kampaň pro stávající uživatele (Authenticator)
  - Apple ID v rámci iCloud

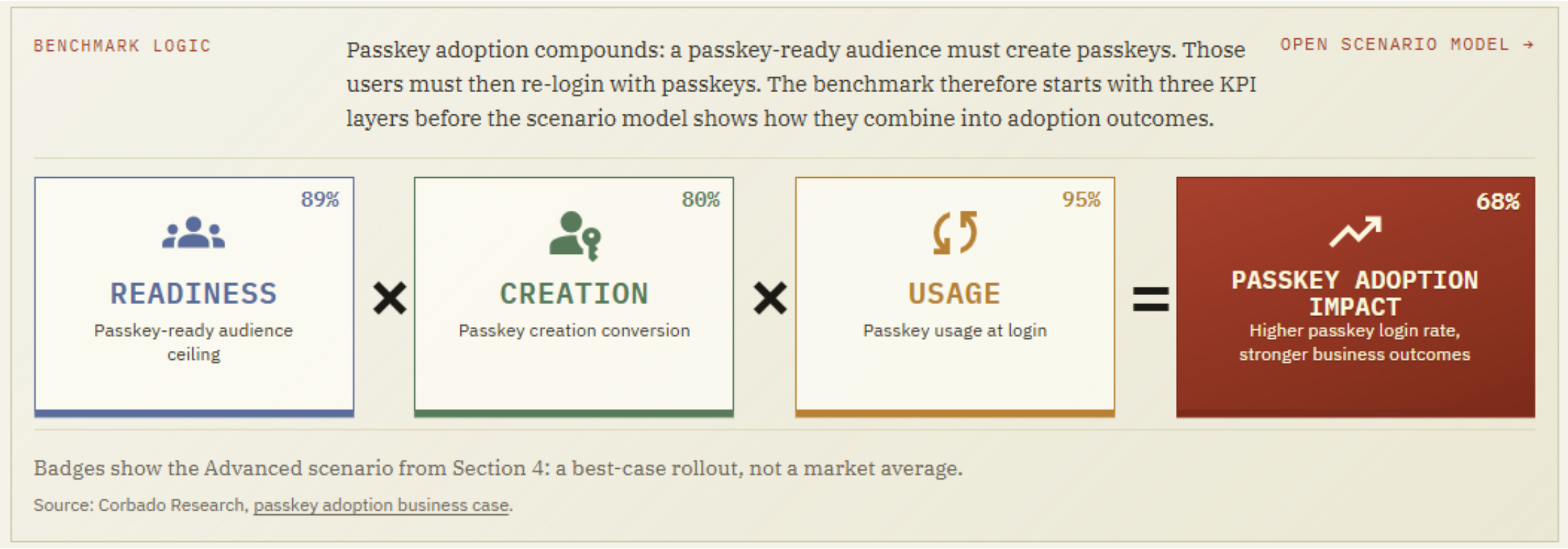
Proč tedy nyní?

- Protože s námi hesla dost pravděpodobně ještě dlouho zůstanou.
- Protože hesla jsou přímočará, jednoduchá a i tak se nepoužívají správně.
- Protože Passwordless i Passkeys se nestanou jen tak bez adopce.
- Protože chceme být připraveni, co se na nás a uživatele řítí.
- Protože máme šanci s Passkeys začít lépe po všech stránkách.

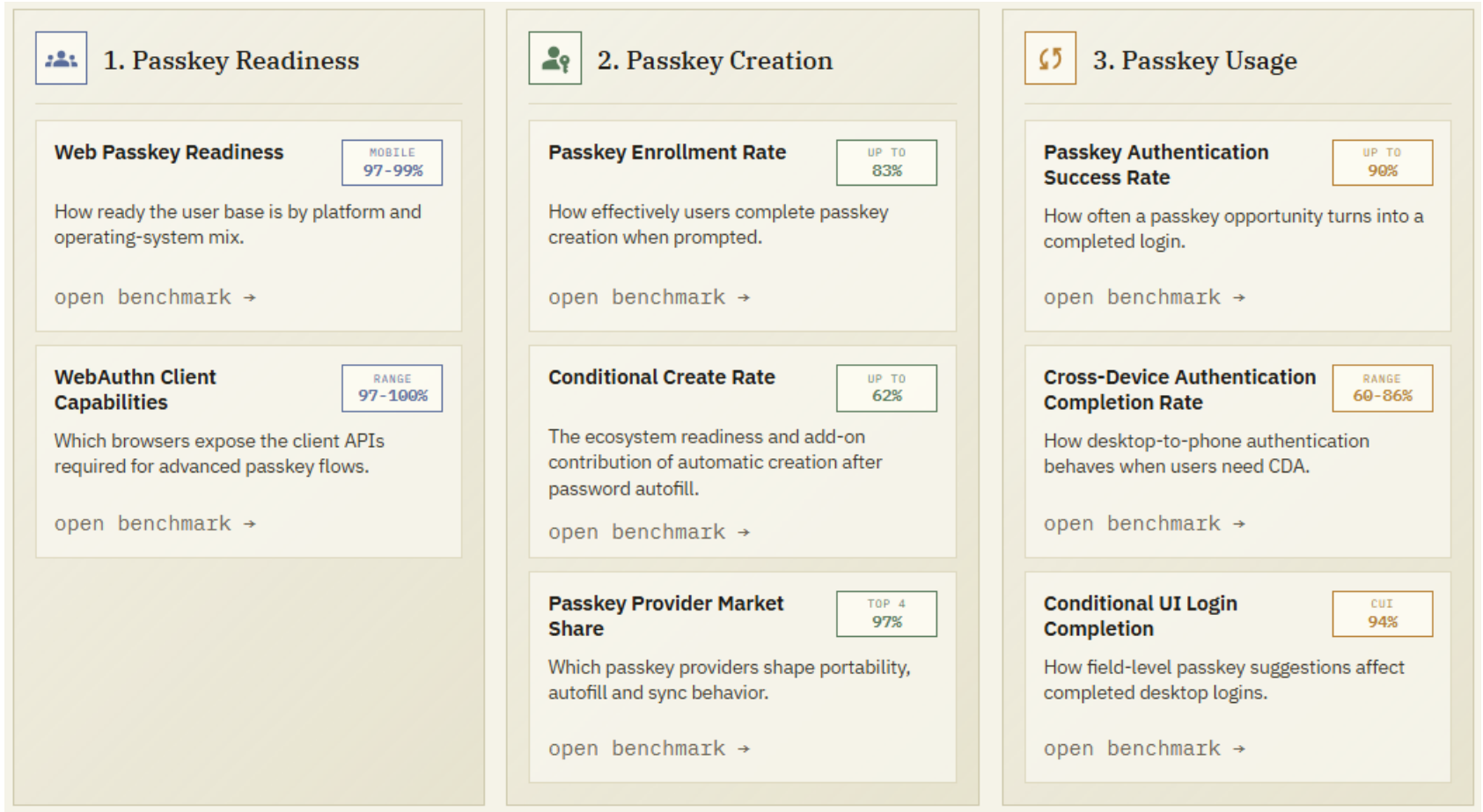
Proč tedy nyní?

- Protože Microsoft ukončuje podporu pro nativní SMS v rámci MFA v Entra ID a pro služby Microsoft 365 k únoru 2027.
- Protože Microsoft bude preferovat Passkeys pro MFA i přihlašování od září 2026 a spouští registrační kampaň pro jejich používání.

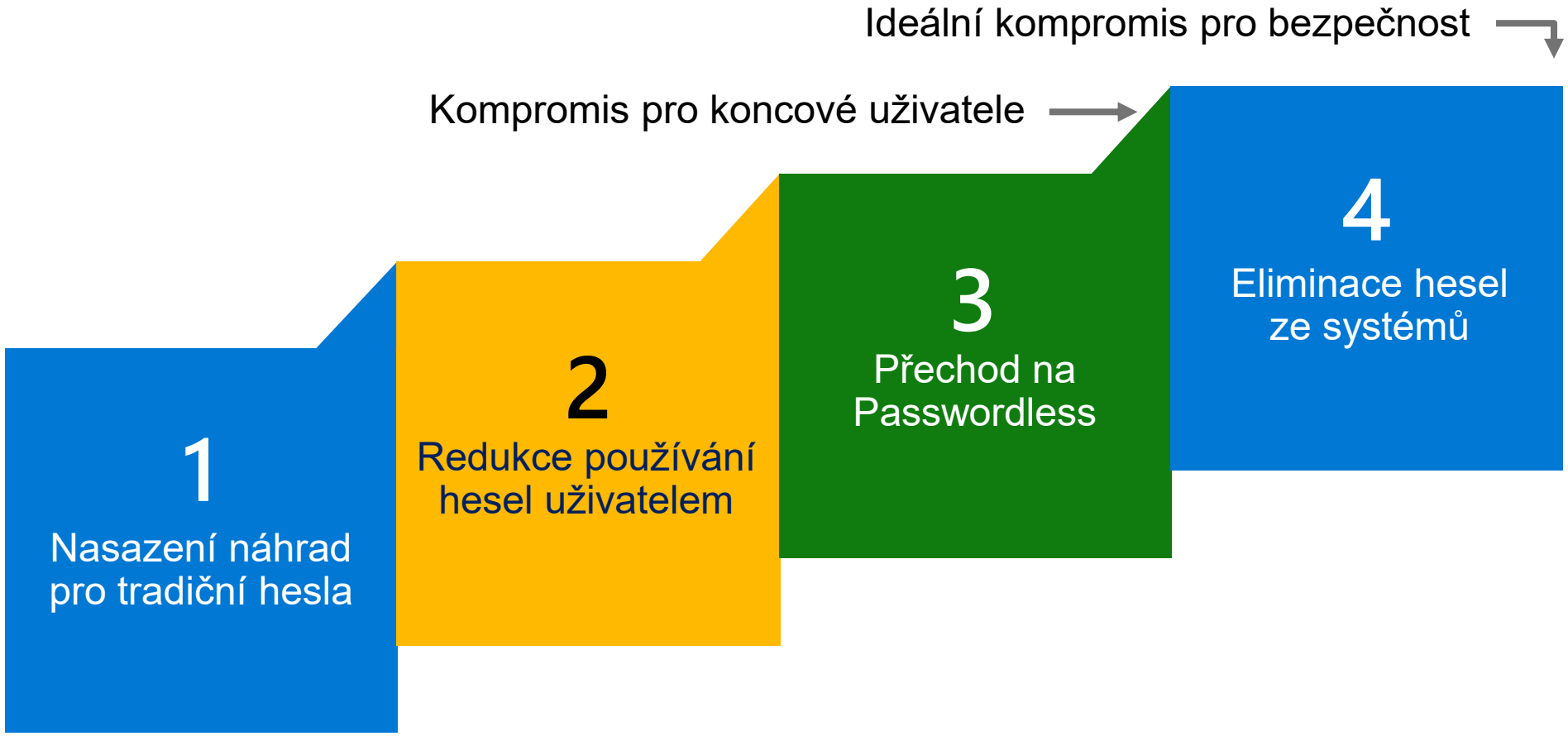
Statistika nuda je...



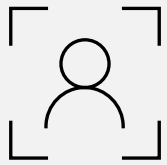
… má však cenné údaje



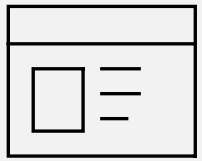
Cesta k Passwordless / Passkeys



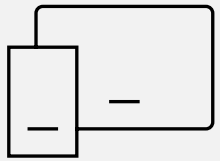
Jak bude naše cesta náročná



Přítomnost a nastavení v Entra ID

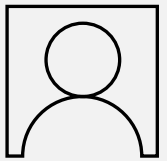


Aplikace podporující moderní ověřování

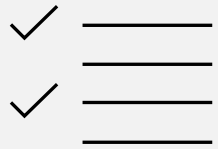


Připravenost zařízení a platformem

Zabezpečení pověření vůči útokům

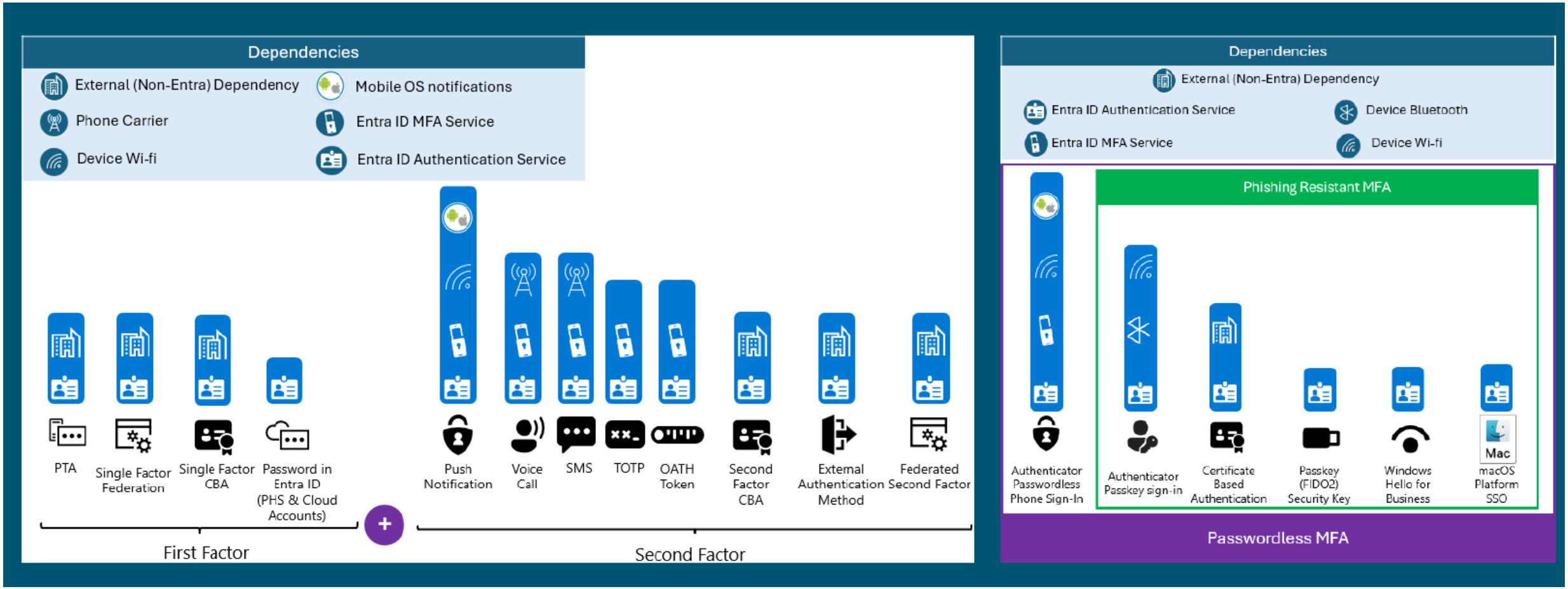


Registrace uživatelem a při změnách zařízení



Reporty užití i bezpečnostní politiky

Technické závislosti faktoru



Passkeys jako budoucnost Passwordless

- Evoluce využití FIDO2 a WebAuthN pro zabezpečenou výměnu ověřovacích informací mezi klientem a aplikací (čili webovou stránkou)

Špatné: Heslo | **Dobré:** Heslo a… | **Lepší:** Heslo a… | **Nejlepší:** Passwordless

Abcd123.

qwerty

password

TechEd2026!

Heslo123

SMS

Voice

Microsoft Authenticator

Software Tokens OTP

Hardware Tokens OTP

Windows Hello for Business

Microsoft Authenticator

Passkey

FIDO2 security key

Certificate Based Authentication

Passkeys

- Evoluce FIDO2 aneb bezpečnější ověřování uživatele vůči aplikacím

Proč jsou passkeys bezpečnější metodou ověření?

Nativně jsou odolné vůči phishing útokům

Nativně jsou odolné vůči útokům na komunikaci mezi serverem a ověřovací aplikací (klientem)

Neexistují hesla, která by mohla uniknout ze serveru nebo klienta

Jsou generována automaticky a jsou automaticky unikátní k dané službě nebo aplikaci

Jsou bezpečně uložena na hardware zařízení a chráněna účtem uživatele

Jsou přívětivější pro uživatele (Přihlaste se obličejem, prstem nebo Vaším PIN)

Volitelně mohou být zálohována nebo synchronizována mezi zařízeními uživatele

Jak funguje poskytovatel ověření

- Může být vestavěn v platformě, spjat se zařízením, nebo v dané aplikaci, například správci hesel nebo prohlížeči

Passkeys are stored on Authenticators

- ***Roaming*** **Authenticator**
  also called *cross-platform* authenticator
  example: a USB security key

- Roaming authenticators can use different *transports*: USB, NFC, BLE, hybrid

- ***Platform*** **Authenticator**
  Built into user's device
  example: a built-in fingerprint sensor

FaceID

TouchID

Windows Hello

- Note: a single authenticator can store multiple passkeys!

Different types of passkeys

Hardware-bound

- Single-device
- Hardware attestation
- Ideal for high assurance use cases
- FIPS eligible
- Example: passkey stored on a security key

Synced | Copyable passkeys

- Multi-device
- Backed up and synced across devices via a cloud provider
- No need to re-enroll a new device on every account!
- Synced across *devices* but not across *ecosystems*
  (Apple iCloud and Google Password Manager)

Syncable passkeys

- Multi-device passkeys je FIDO2 metoda bezpečně synchronizovaná poskytovatelem ověřovacího prostředku pomocí vlastní služby mezi zařízeními uživatele.

Apple iOS (Keychain)

Chráněno zabezpečením účtu uživatele v rámci cloudové synchronizace mezi Apple zařízeními iOS a macOS a biometrií uživatele nebo PIN

Na úrovni hardware chráněno bezpečnostním čipem

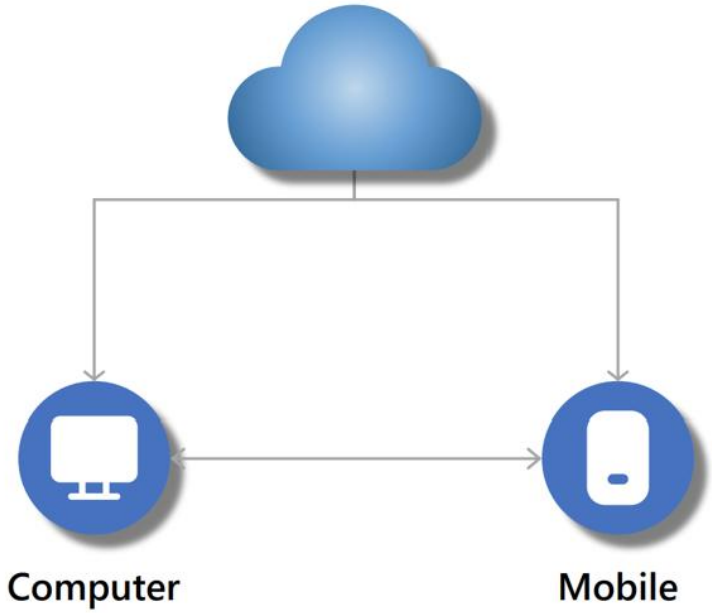
Google Android (Keystore)

Chráněno zabezpečením účtu uživatele v rámci cloudové synchronizace mezi Google zařízeními s Android a biometrií uživatele nebo PIN

Na úrovni hardware chráněno bezpečnostním čipem dle dostupnosti na daném modelu zařízení

Microsoft Authenticator

K dispozici po aktualizacích na iOS i Android



Device-bound passkeys

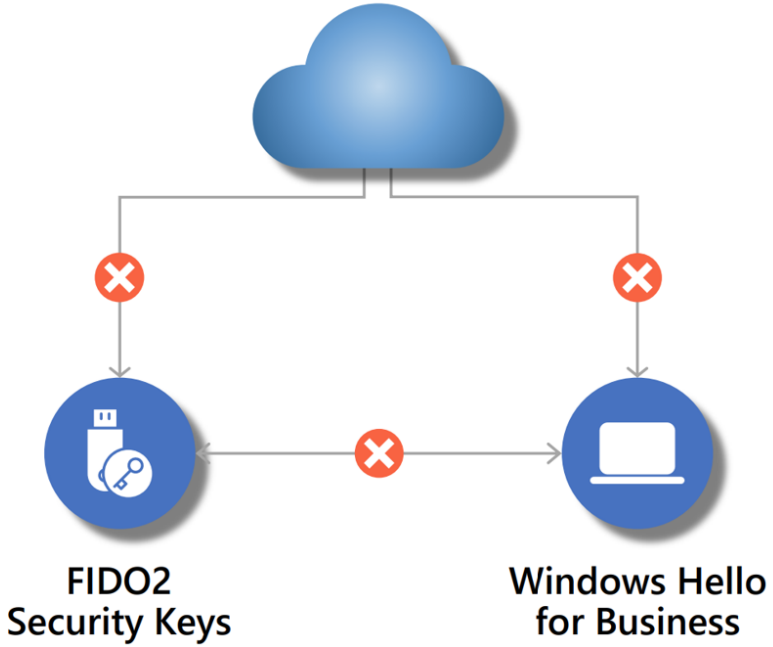
- Single-device passkeys je FIDO2 metoda, která technicky nedokáže opustit dané zařízení, na kterém byla vytvořena.

Windows Hello for Business

Chráněno TPM čipem a operačním systémem a PIN nebo biometrickým signálem uživatele

FIDO2

Chráněno na úrovni hardware a volitelně PIN nebo biometrií dle nastavení uživatele, možnostmi zařízení nebo dle stanovené politiky

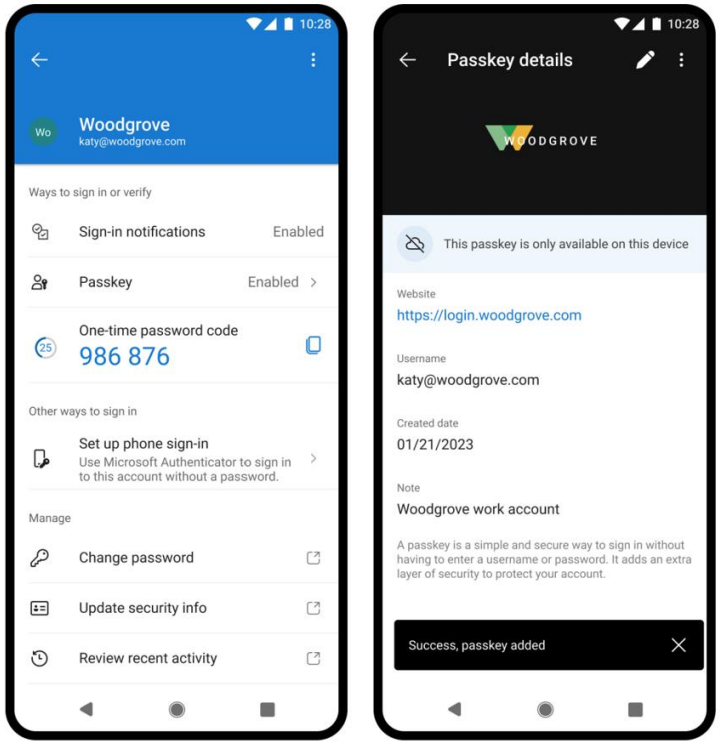


Passkeys management

- Jednotlivé passkeys mohou být spravovány samotnou platformou, operačním systémem, poskytovatelem ověření, například správcem hesel nebo ověřovací aplikací či prohlížečem

Microsoft Authenticator

Využívá vlastního poskytovatele

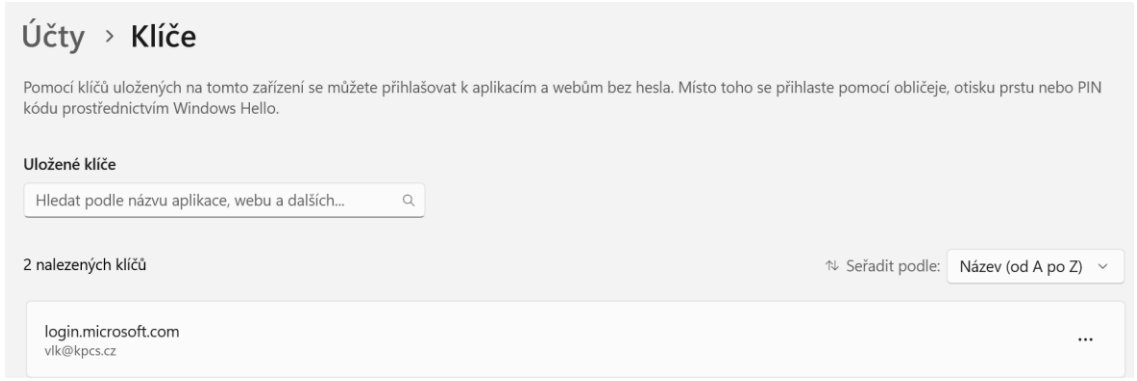


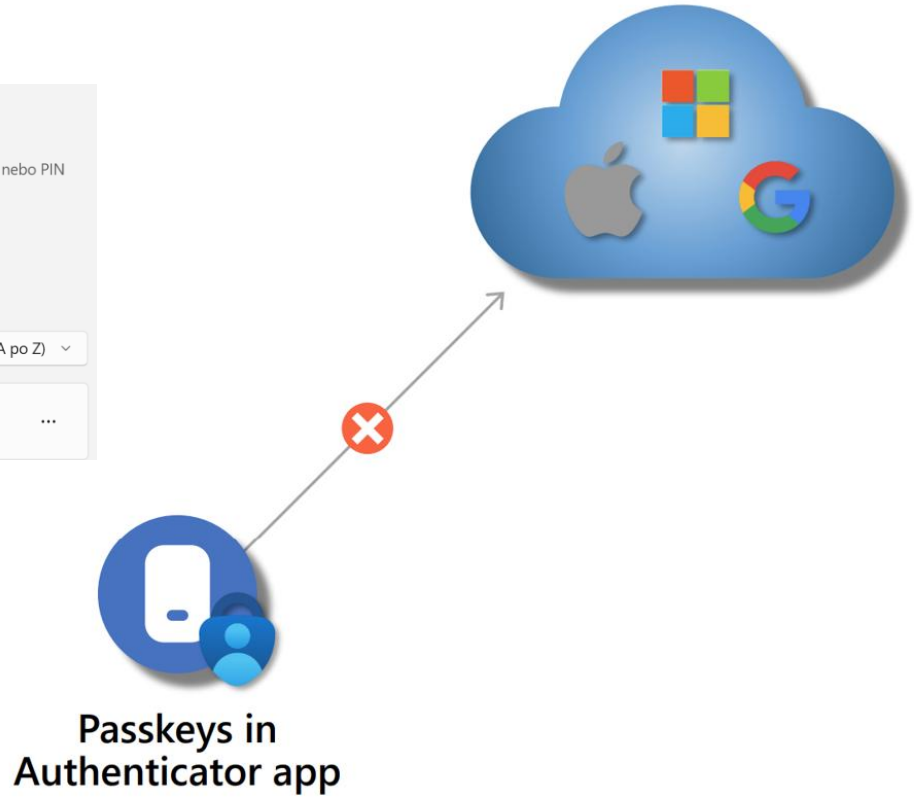
Passkeys management

- Jednotlivé passkeys mohou být spravovány samotnou platformou, operačním systémem, poskytovatelem ověření, například správcem hesel nebo ověřovací aplikací či prohlížečem

Windows 11

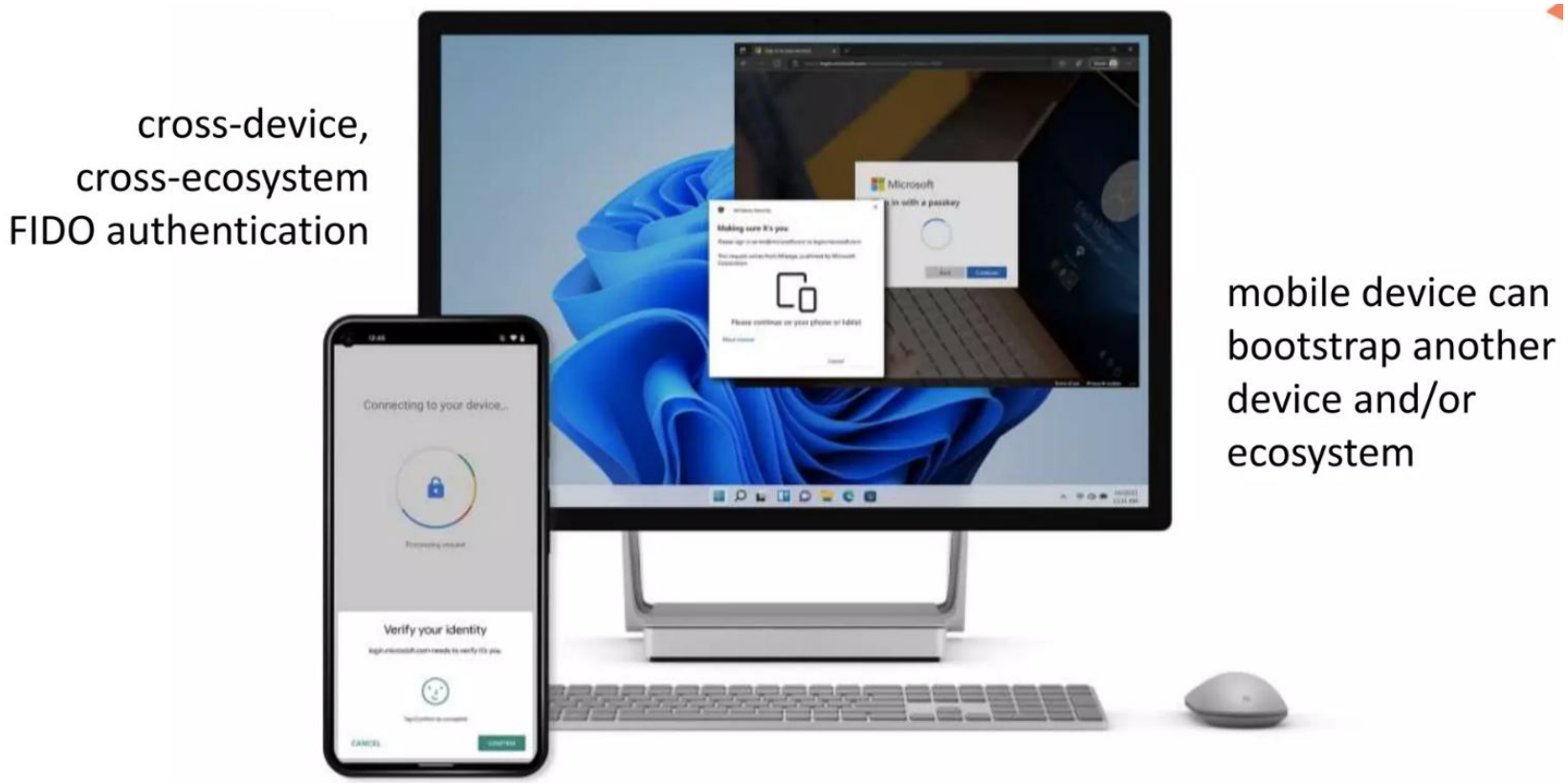
Využívají Windows Hello jako FIDO2 metodu





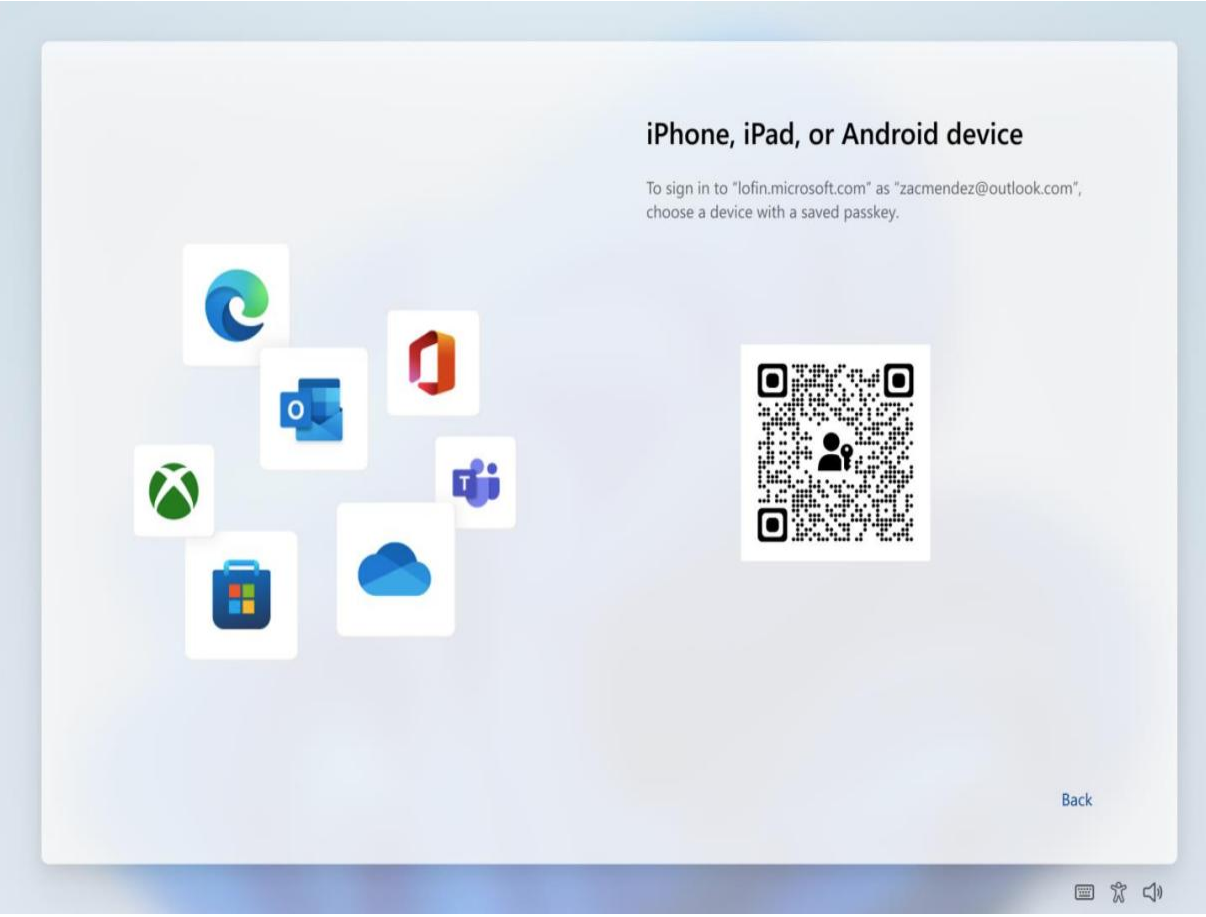
Passkeys ecosystem

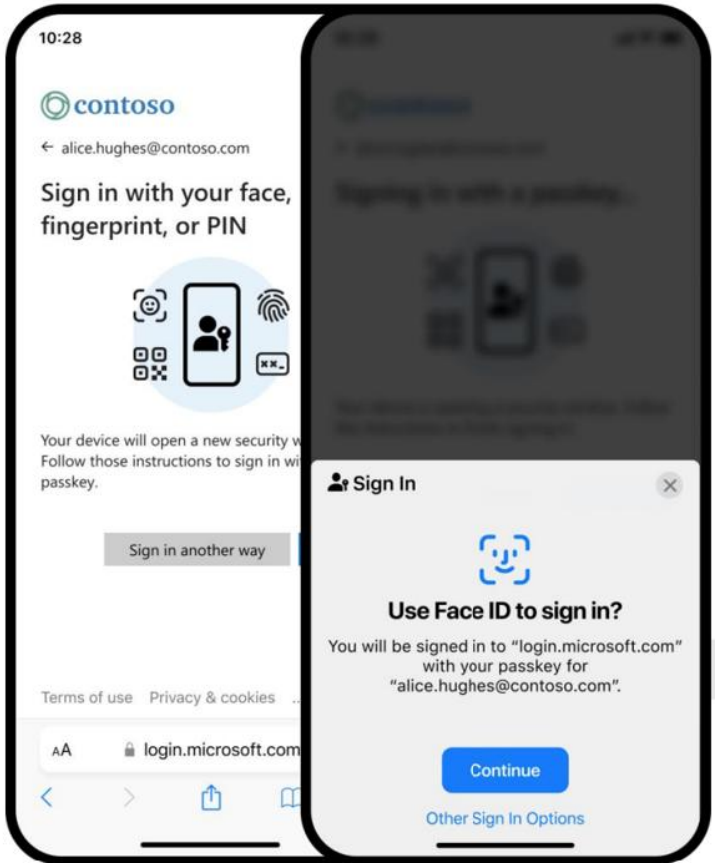
- V rámci ověřování může být využito i externího zařízení, které disponuje správným passkey ke konkrétní službě, pokud je ověřena identita uživatele poskytovatelem



Jak to vypadá

- Uživatel nastaví Windows Hello nebo Microsoft Authenticator jako passkey metodu na svém zařízení a může ji využít k jednotlivým aplikacím nebo ověřením napříč zařízeními.





Co je tedy otázkou?

- Vynucení device-bound passkeys i pro mobilní zařízení a pro které aplikace?
- Povolení cross-device ověřování pro Windows Hello a Authenticator?

Výhody

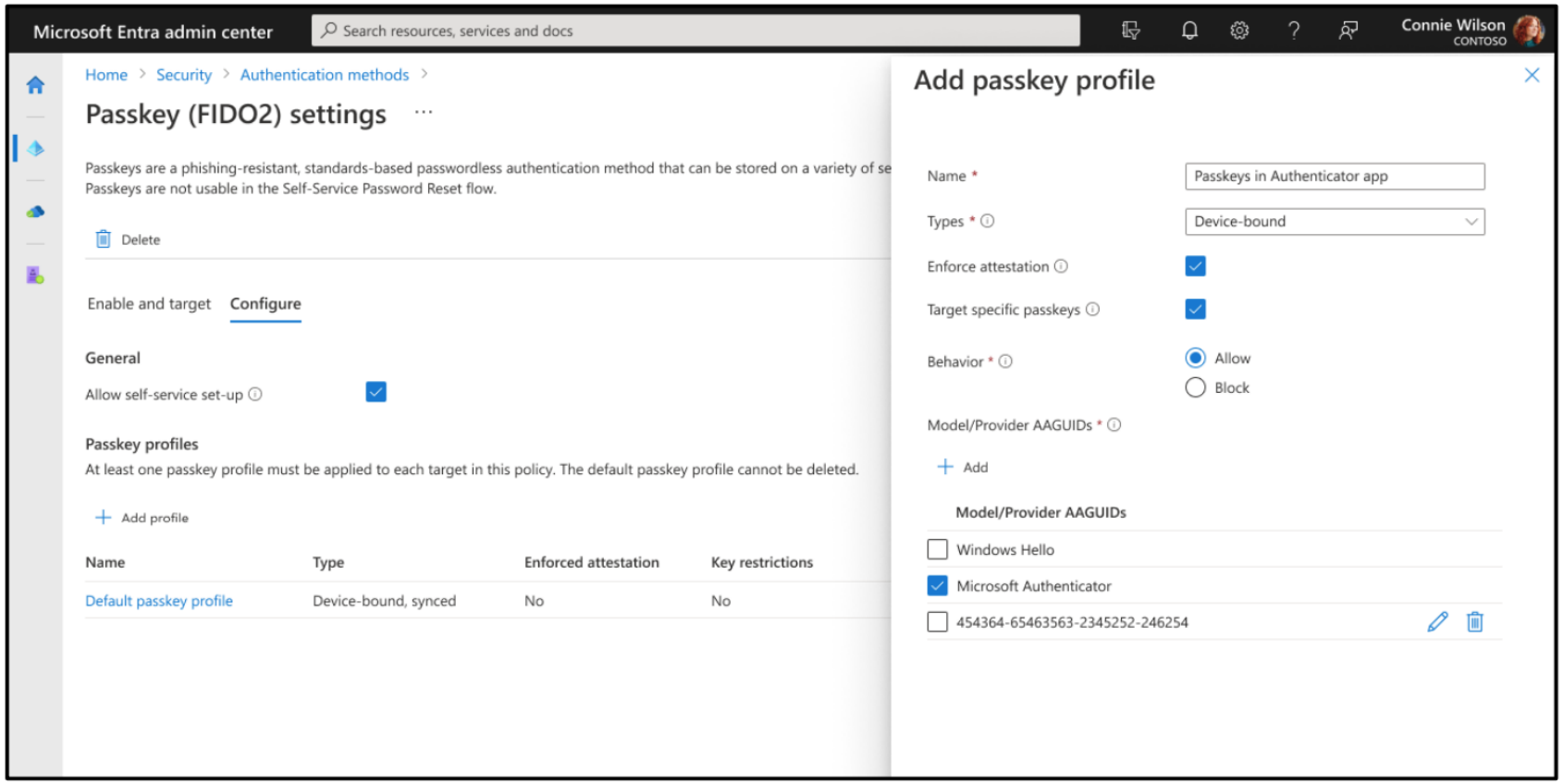
- Nativní podpora odolných přihlašovacích údajů na mobilu
- Brzy všudypřítomný uživatelský zážitek
- Žádný drahý hardware ani správa navíc
- Vestavěné mechanismy obnovy přístupu

Nevýhody

- Klíče zálohovány přes spotřebitelskou identitu/obnovu
- Nelze zaručit atestaci autentizátoru
- Sdílení = nelze zaručit identitu uživatele
- Minimální administrátorská kontrola přístupových klíčů na mobilu

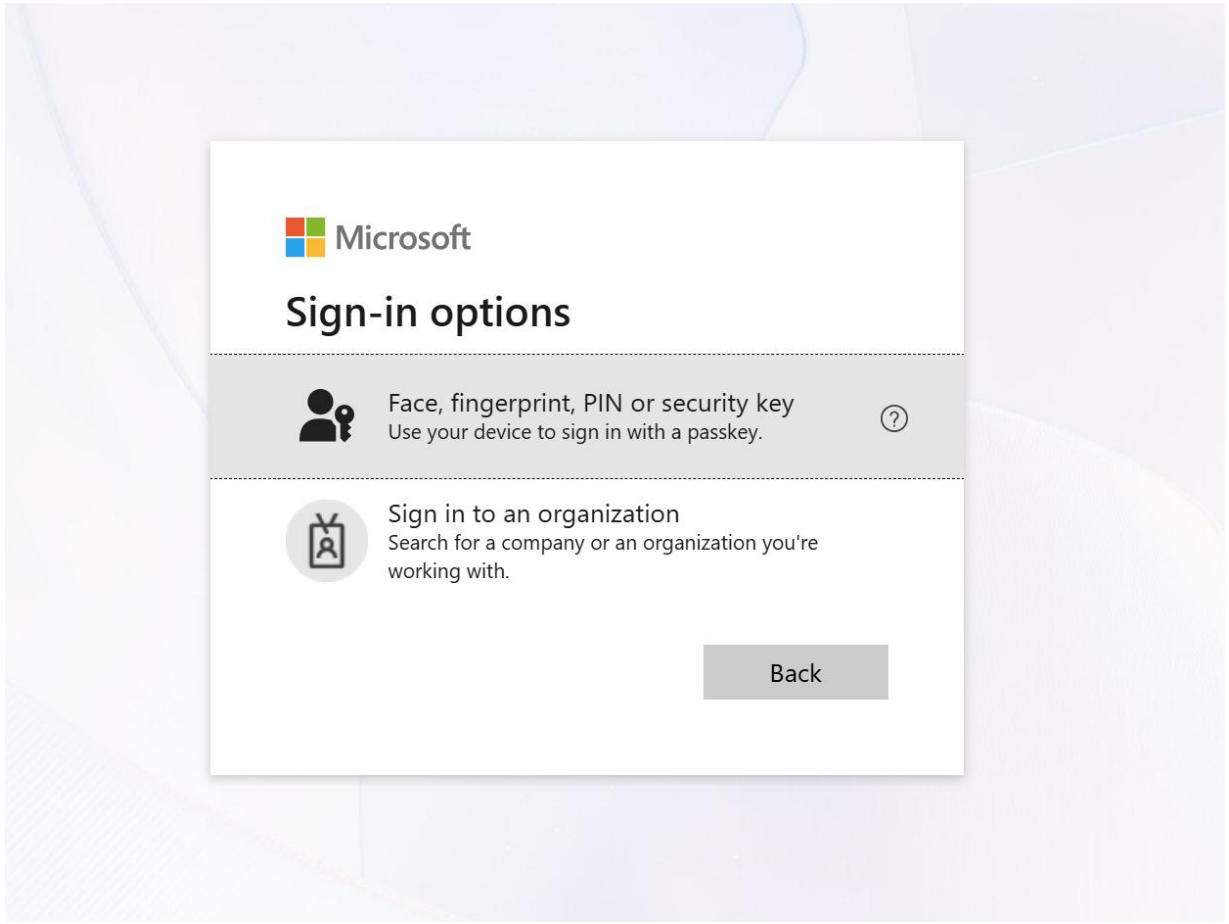
Co je tedy otázkou?

- iOS / Android / Windows Hello (a které) / Microsoft Authenticator / FIDO2 / a další ?
- Povolení cross-device ověřování pro Windows Hello a Authenticator?



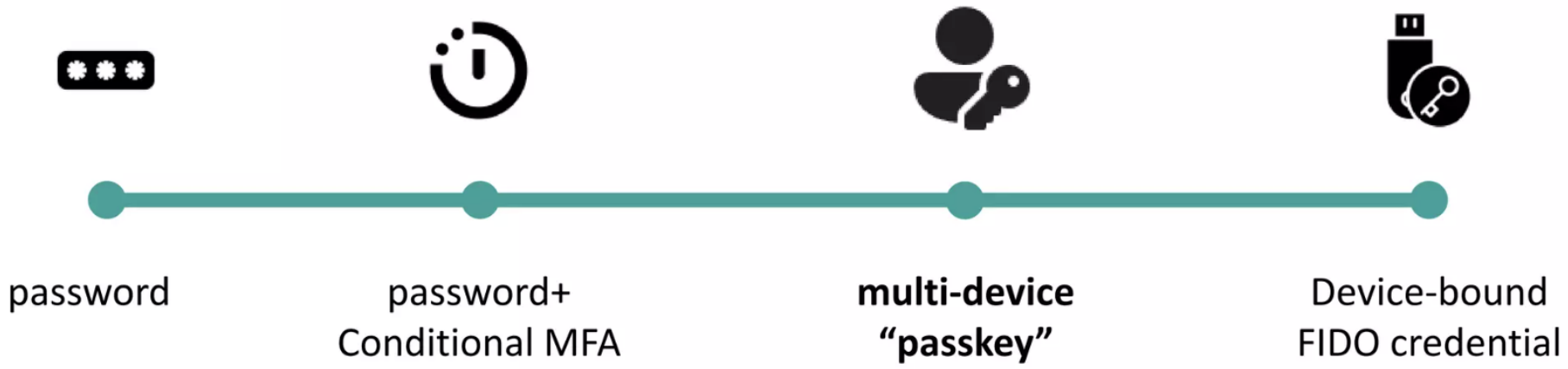
Dopad na uživatele

- Změna přihlašovacích dialogů pro Windows Hello (for Business) a v Entra ID



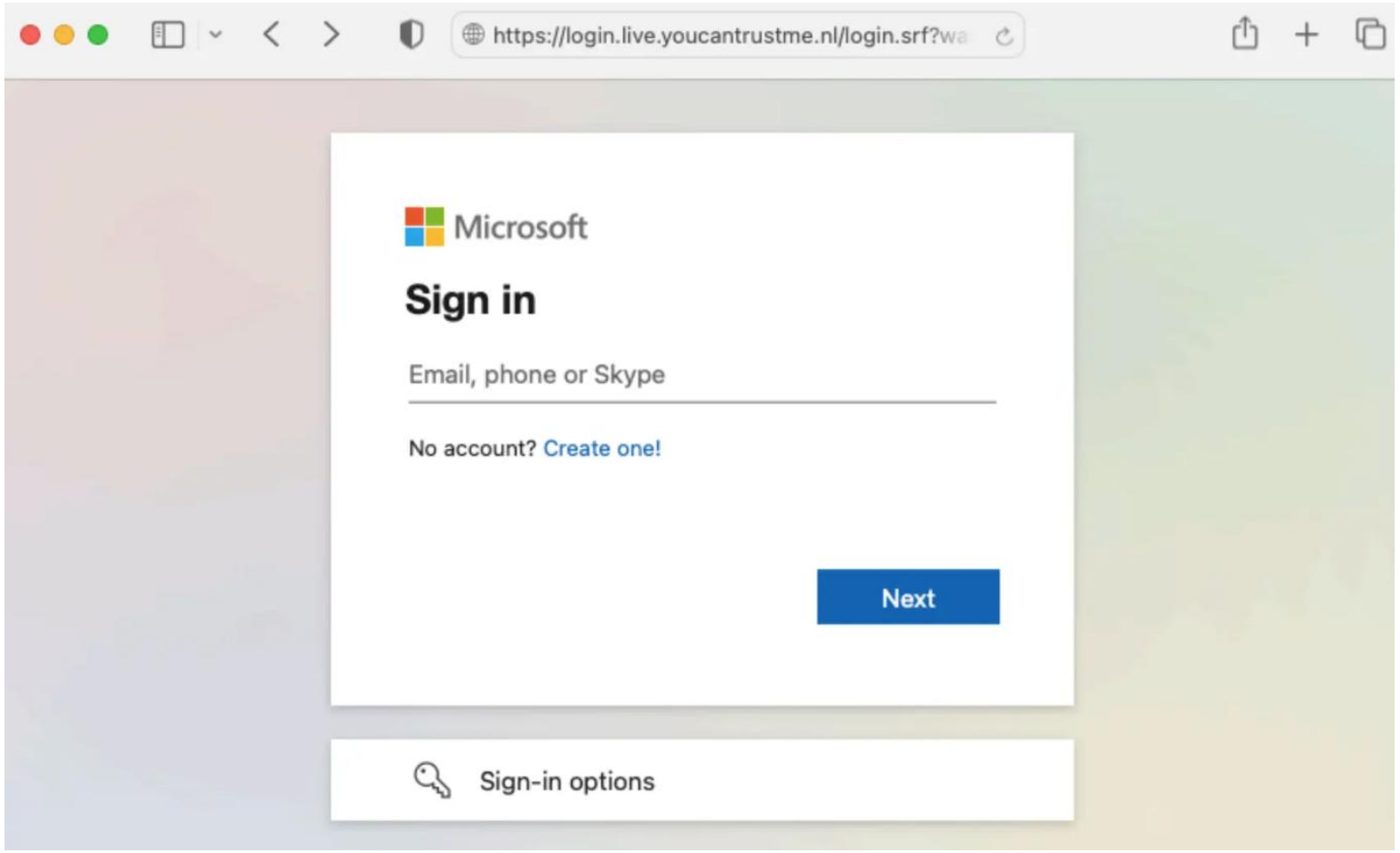
Passkeys jako budoucnost Passwordless

- Device-bound FIDO2 passkey bráno jako dnes nejvíce bezpečná metoda ověření



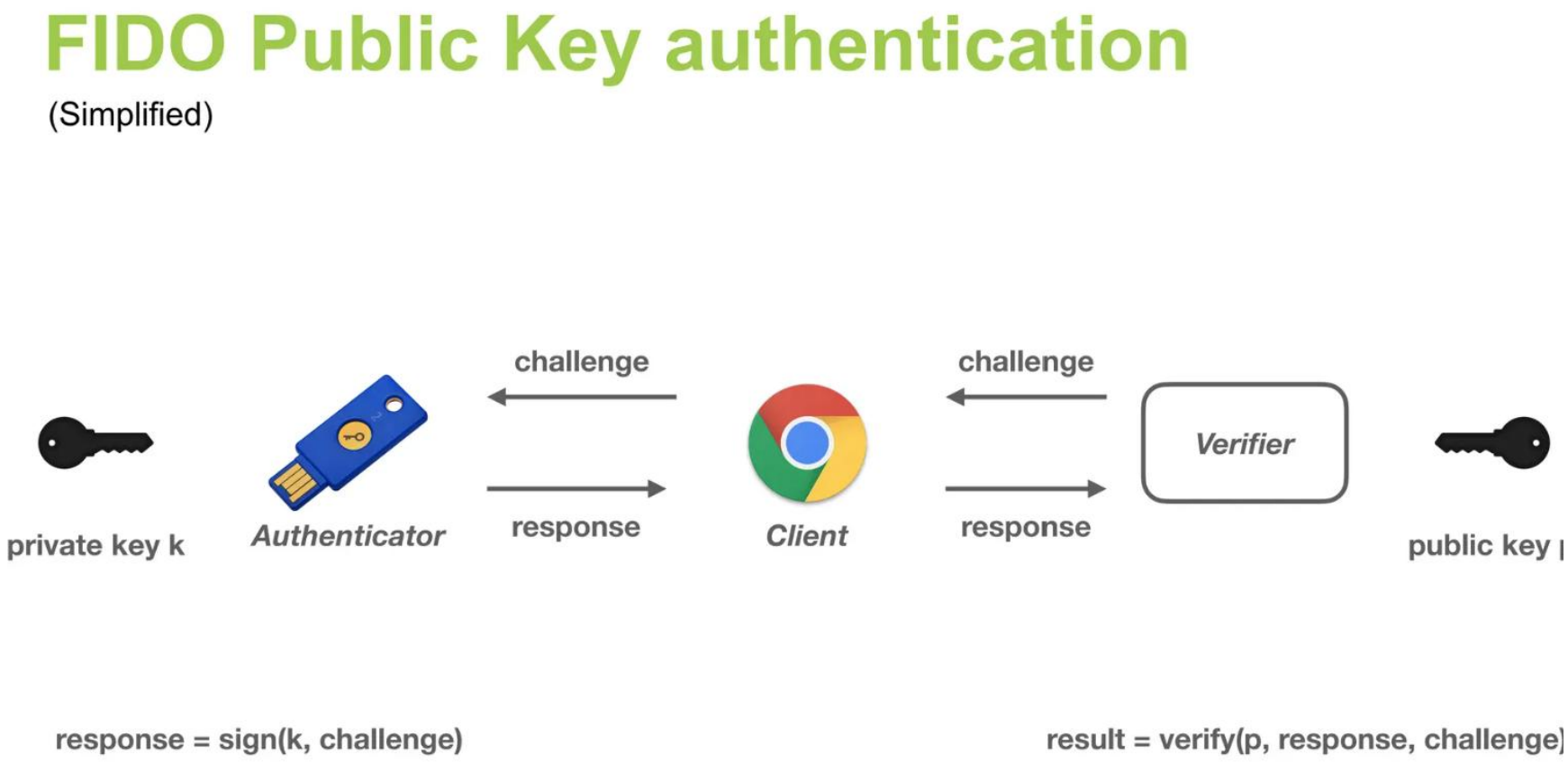
Passkeys ecosystem

- V rámci ověřování může být využito i externího zařízení, které disponuje správným passkey ke konkrétní službě, pokud je ověřena identita uživatele poskytovatelem



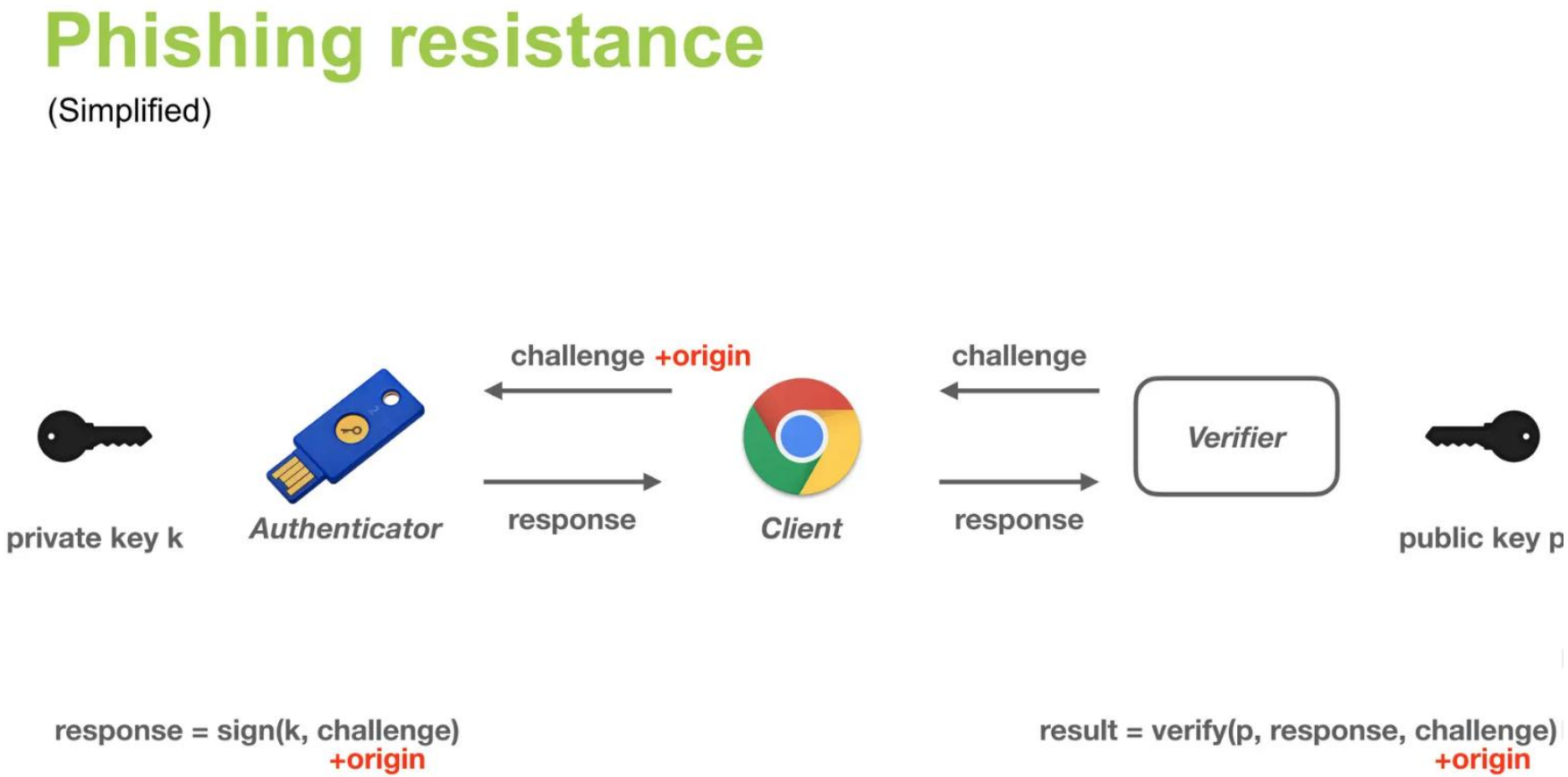
FIDO2

- Současná specifikace a funkčnost ověření moderní metodou a kryptografií



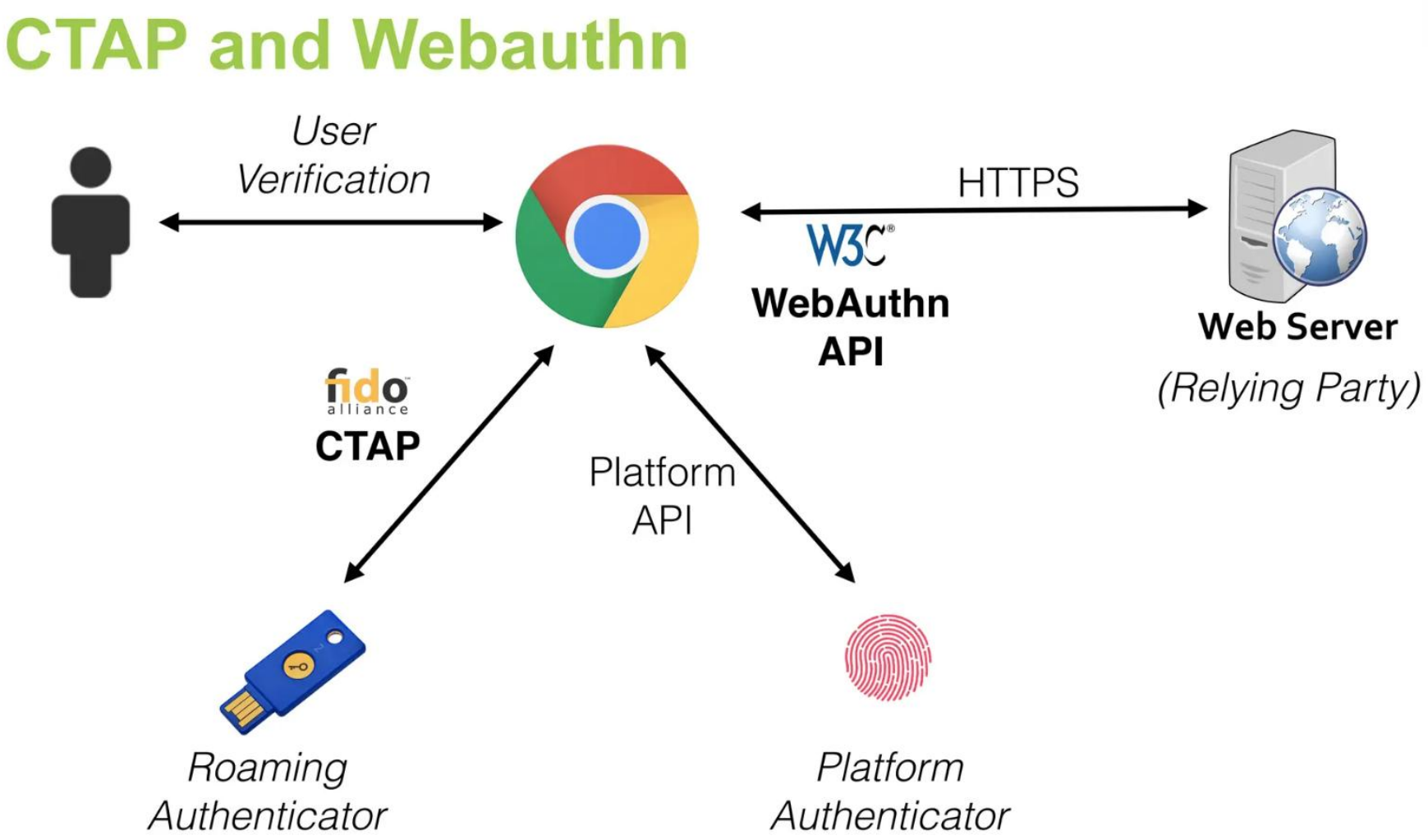
FIDO2

- Rozšíření o ověření identity aplikace/serveru a klienta vzájemnou kryptografickou operací



CTAP a WebAuthN

- Funkčnost zajištěna na úrovni platformy, API, operačního systému, prohlížeče

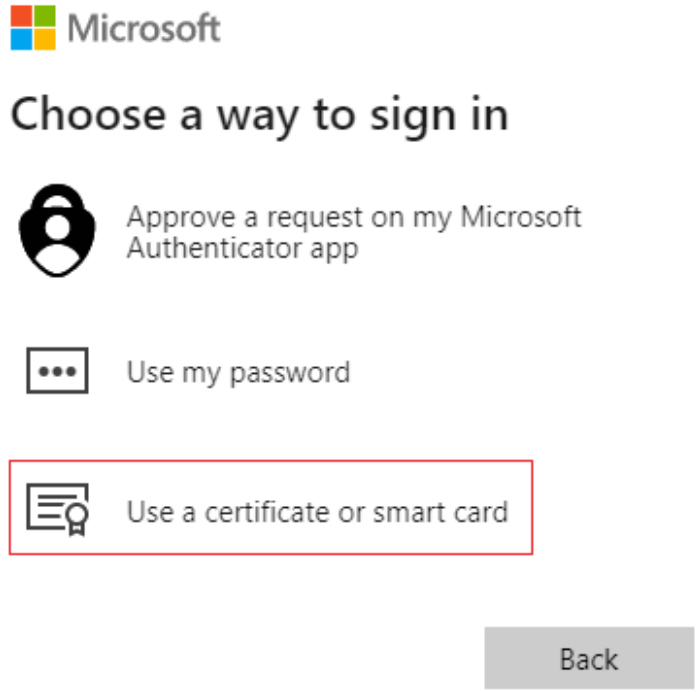


Poznámky z praxe

Aneb jak na skryté detaily nasazení Passkeys

Entra CBA

- Certifikáty
- Kdo je vydá? Cloud PKI!
- Jak je doručení zařízením? Intune!
- Stále validní princip
- Podpora na mobilních platformách a aplikacích



Podpora v rámci operačních systémů

- Podpora FIDO2 v koncovém OS
  - Windows 10 a 11 od verze 22H2
  - macOS od verze 13
  - iOS od verze 17
  - Android od verze 13
- Ale až s novějšími verzemi obdržíme nejen FIDO2, ale také Passkeys
- GUI v jednotlivým OS se mění i s použitým prohlížečem (nativní prohlížeč)
- Vzhled pro uživatele a rozsah podpory se liší s každou další novou verzí, např.
  - Windows 11 24H2 po aktualizacích nabízí Passkeys i pro Windows Hello
  - macOS 26 s podporou Entra ID při přihlášení a Secure Enclave v rámci Platform SSO
  - iOS 26 odstraňuje limitace na počet Passkeys Providers
  - Android 14 odstraňuje limitace využití Google Password Manager
  - Automatický upgrade hesla od iOS 18 a Android 15

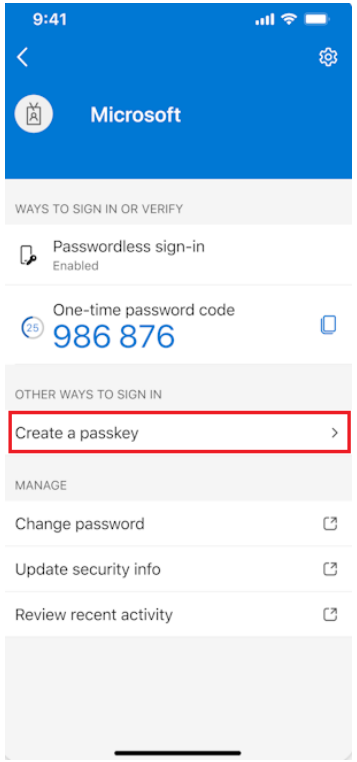
Microsoft Authenticator

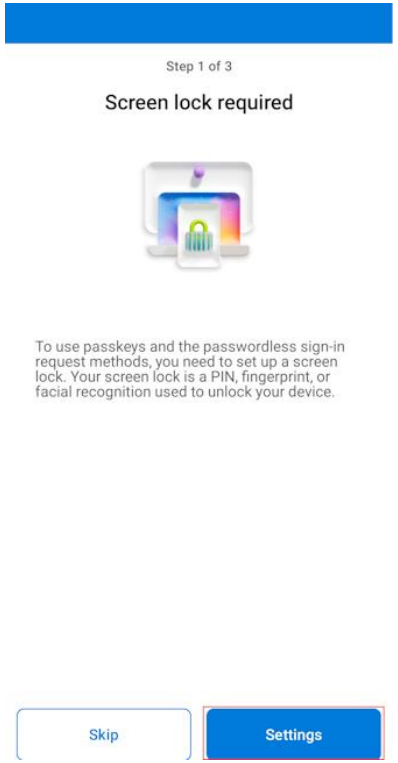
Scenario	iOS	Android
Same-device registration by signing into Authenticator	✅	✅
Same-device registration in a browser	✅	✅[1]
Cross-device registration	✅	✅

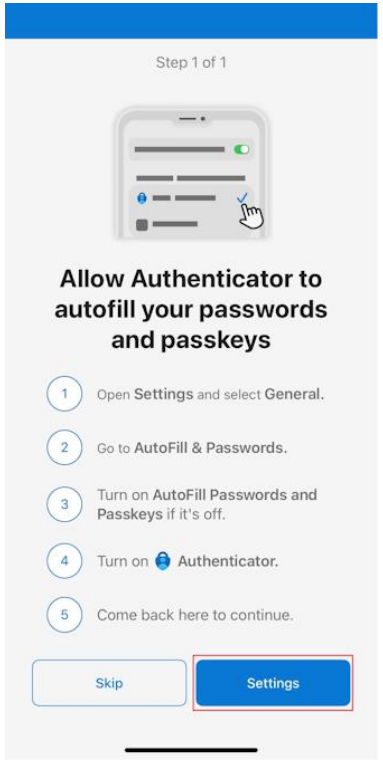
[1]Support for same-device registration in Microsoft Edge on Android is coming soon.

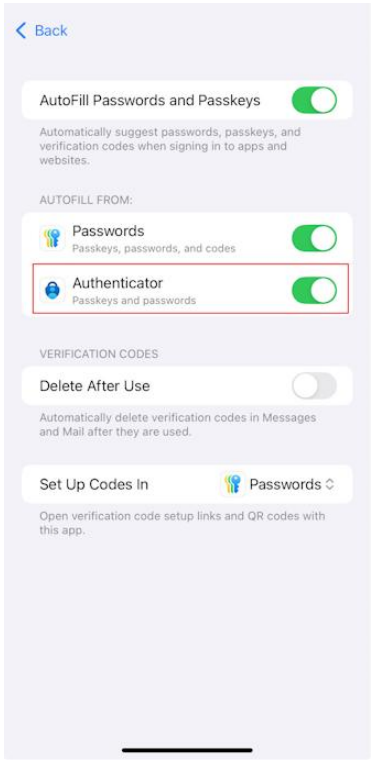
- Preferovaná a přímočará metoda
- Device Bound jako výchozí
- Syncable jako možnost dle politiky
- Minimálně iOS version 6.8.37 nebo Android version 6.2507.4749 a aktualizace
- Users must complete multifactor authentication (MFA) within the past five minutes before they can register a passkey (FIDO2).

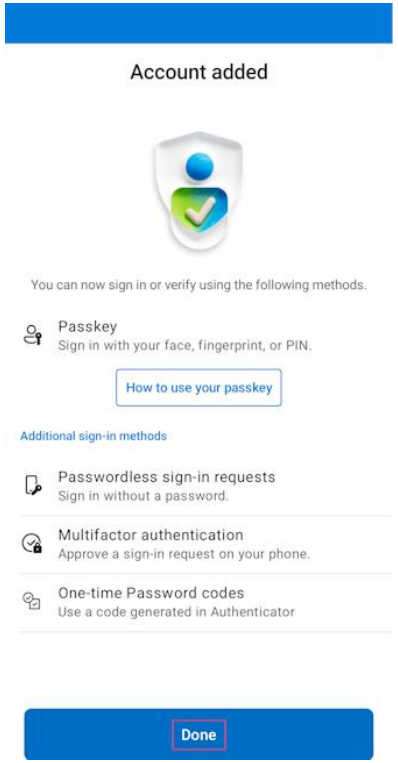
Microsoft Authenticator



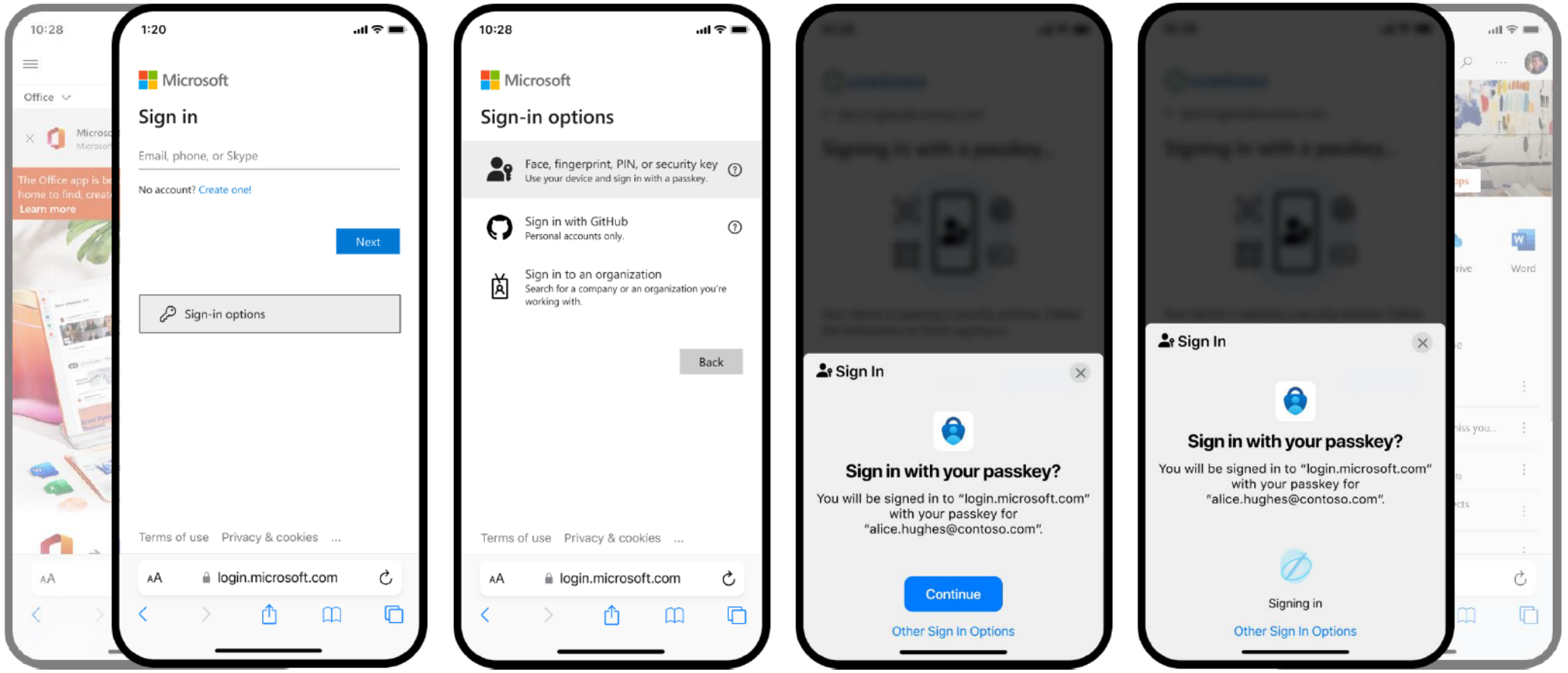






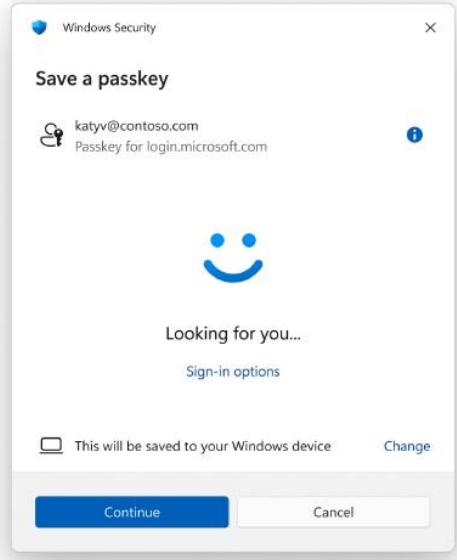


Microsoft Authenticator



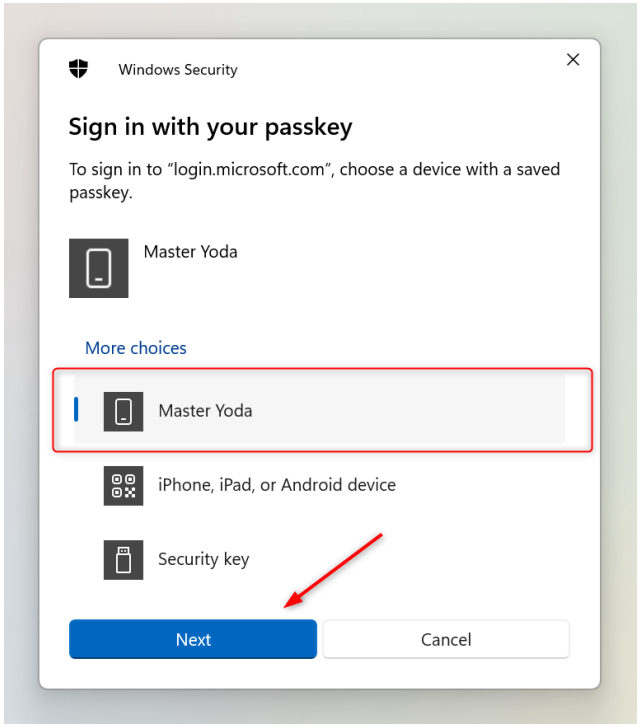
Windows

- Windows 10 s podporou FIDO2
- Windows 11 24H2 s podporou Passkeys
- Windows 11 25H2 s podporou Passkeys Manager (1Password)
- Microsoft Edge a Microsoft Password Manager



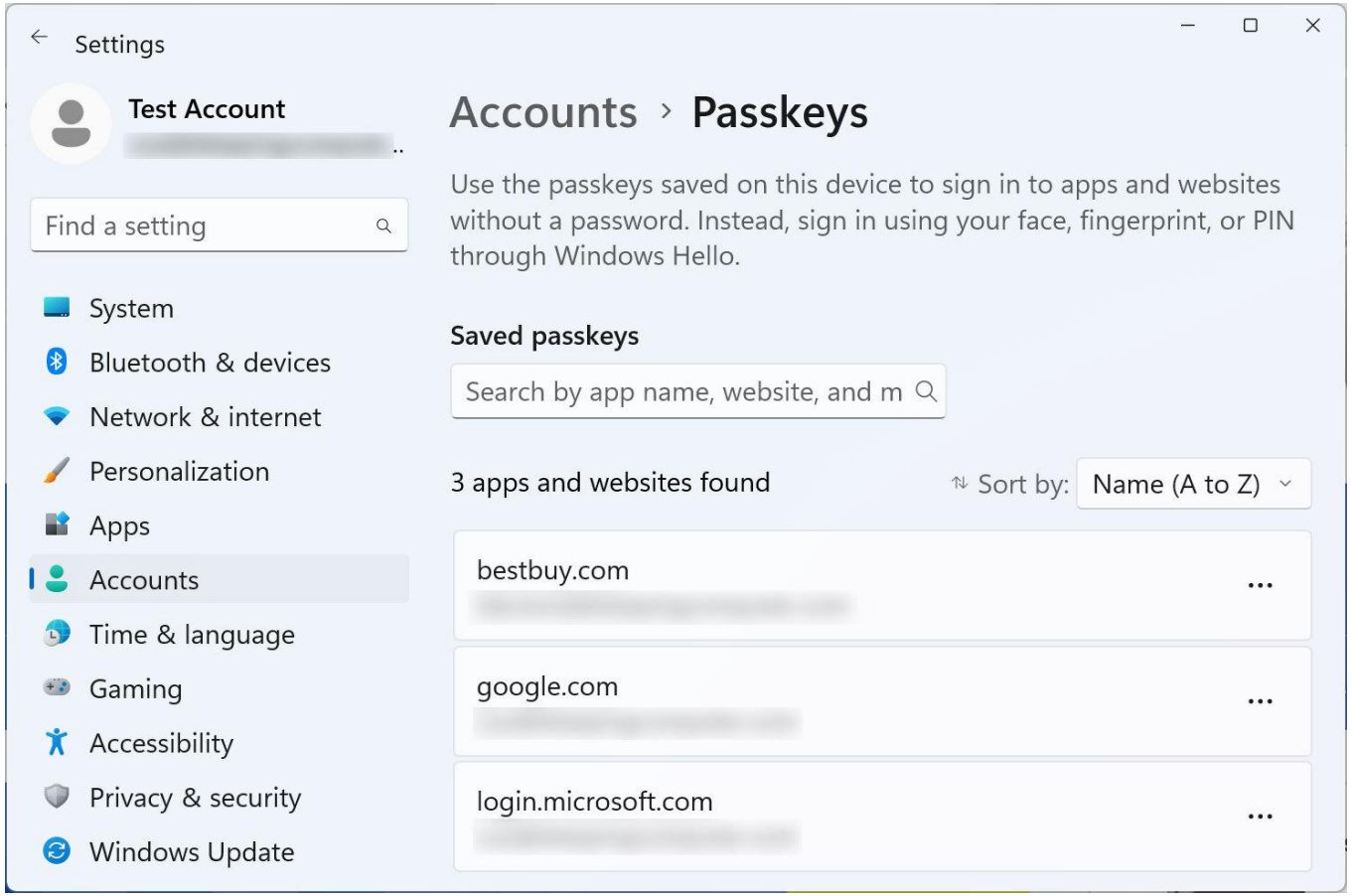
Windows

- Integrováno s Windows Hello výzvou (Hello / Cross-Device / Security-Key)

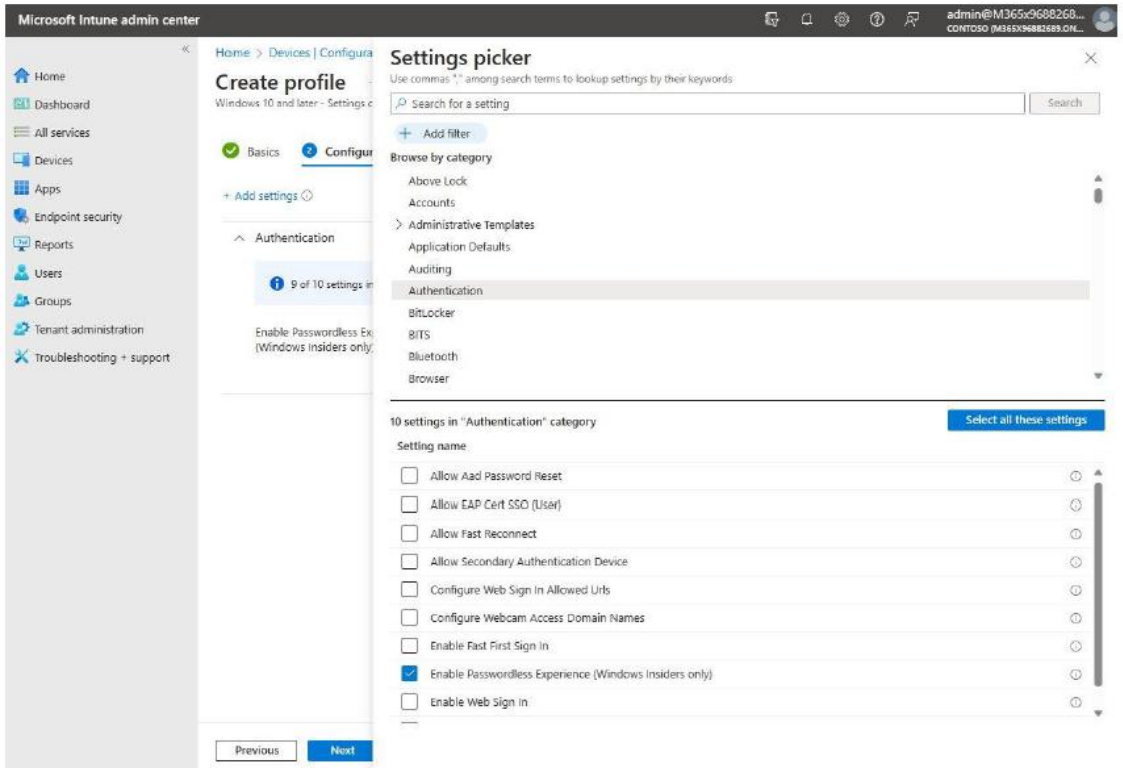


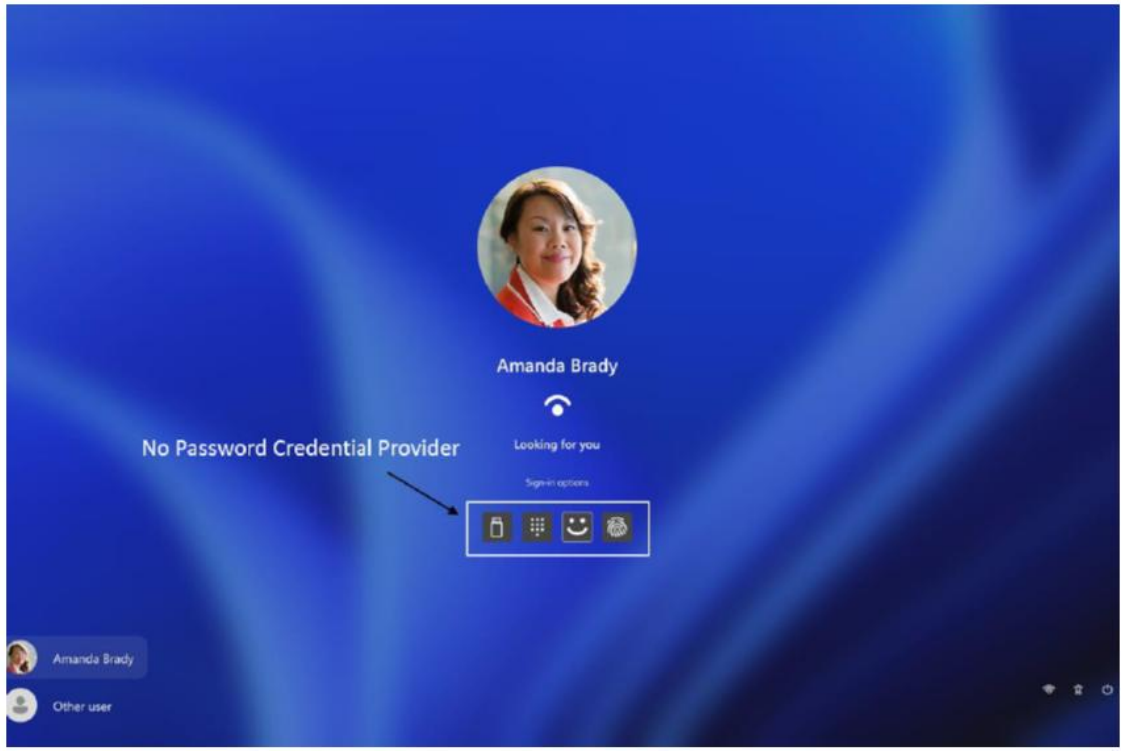
Windows

- Nastavení a Účty
- Microsoft Edge

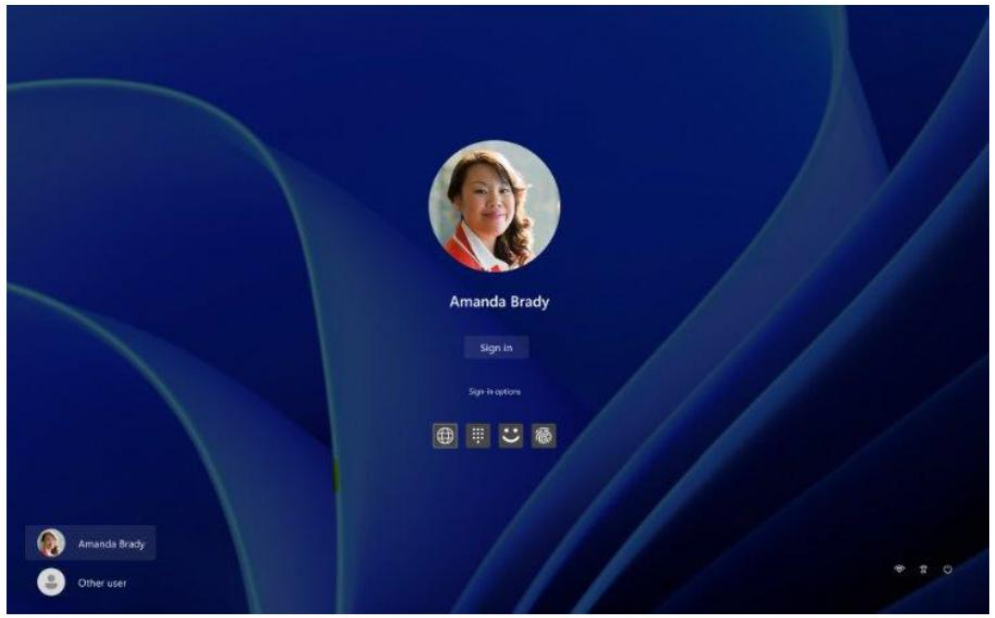


Windows Passwordless

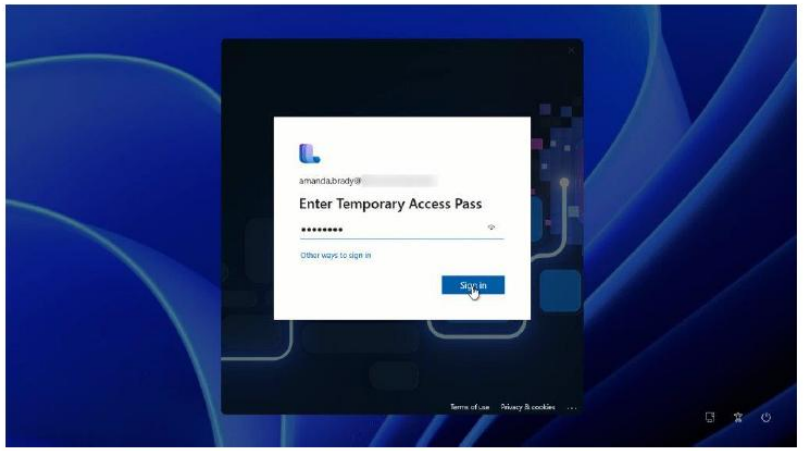


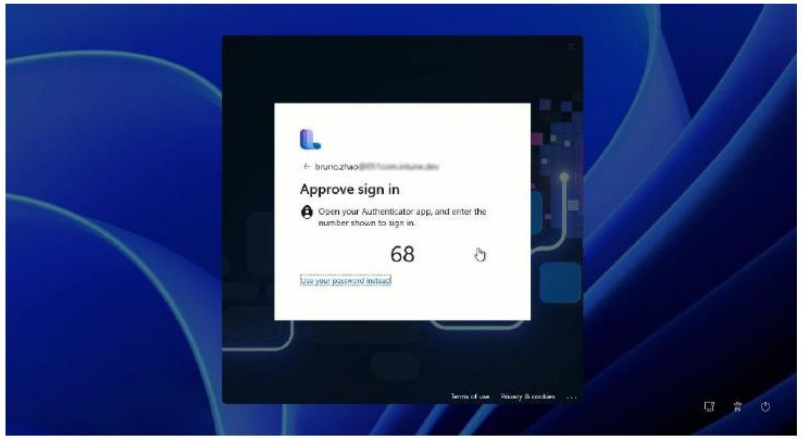


Windows Web Sign-In



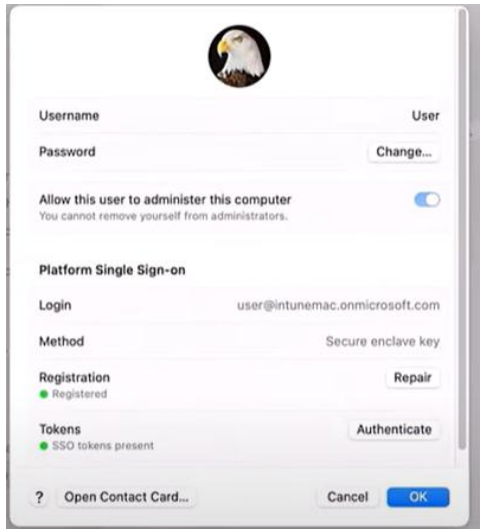
Web Sign-in is now opened to all authentication methods
(in addition to TAP)





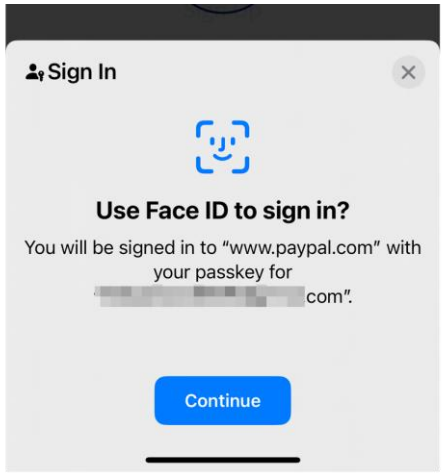
macOS

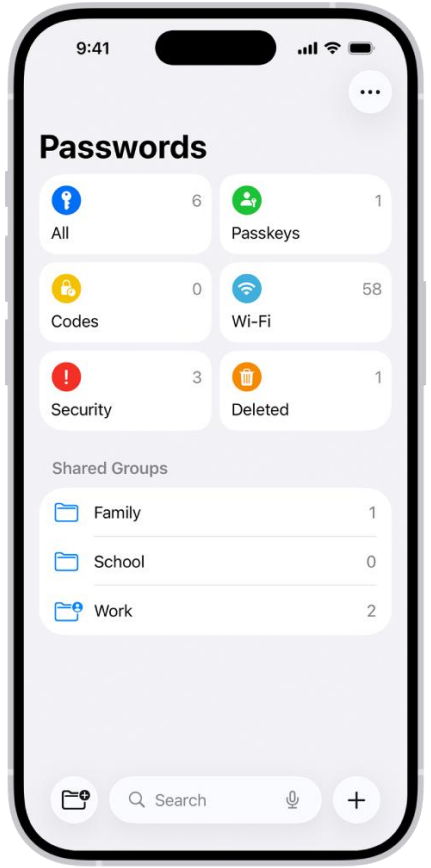
- macOS Ventura 13 nebo novější
- Ale až verze 14 s potřebnými dialogy a politikami
- K dispozici Platform SSO se všemi aktualizacemi ve verzi 26
- Entra ID účet se Secure Enclave jako Windows Hello for Business

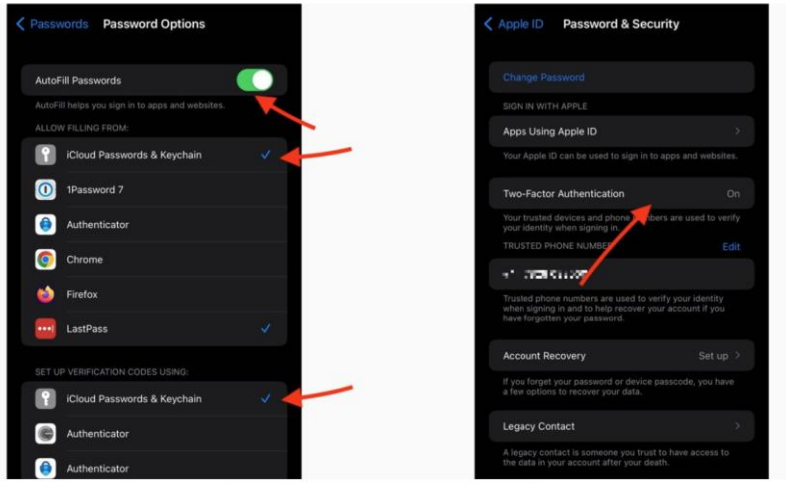


iOS

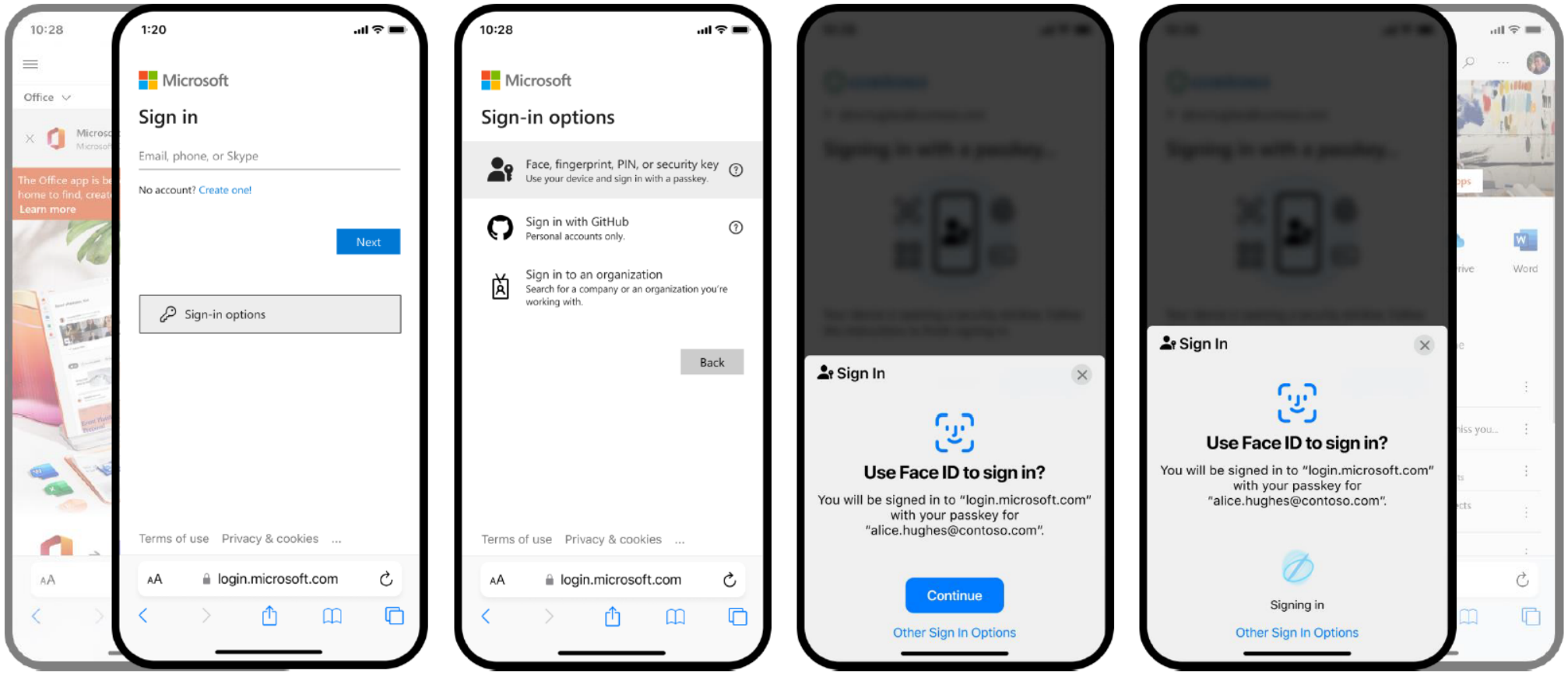
- iCloud Keychain od verze 16
- iCloud je svázán s konkrétním Apple ID
- iOS 18 představil aplikaci Hesla (Passwords)
- iOS 26 zvýšil počet správců hesel
- Výchozí prohlížeč?





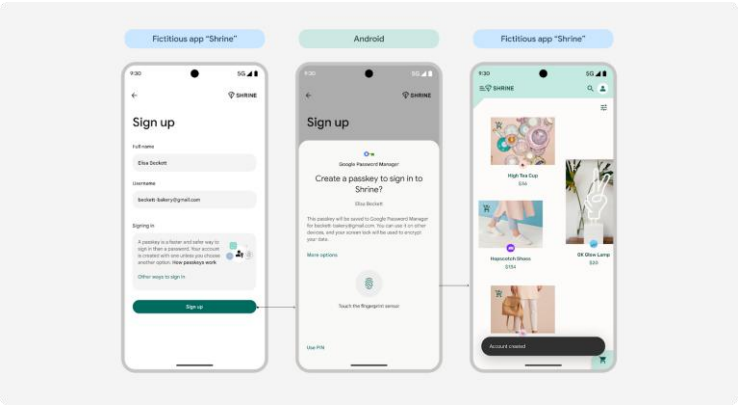


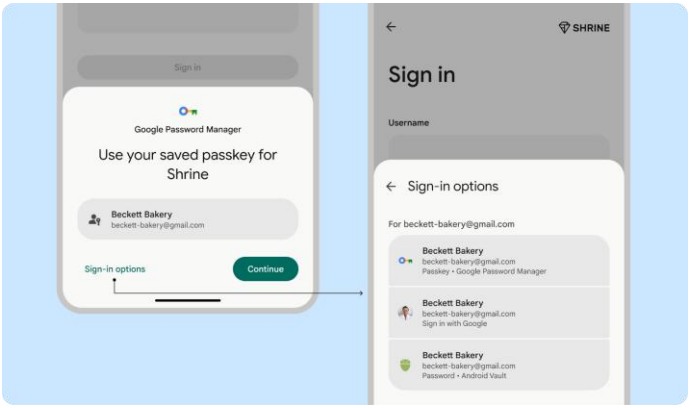
iOS


10:28
1:20
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Next
Sign-in options
Terms of use
Privacy & cookies
...
AA
login.microsoft.com
10:28
Microsoft
Sign-in options
Face, fingerprint, PIN, or security key
Use your device and sign in with a passkey.
Sign in with GitHub
Personal accounts only.
Sign in to an organization
Search for a company or an organization you're working with.
Back
Terms of use
Privacy & cookies
...
AA
login.microsoft.com
Sign In
Use Face ID to sign in?
You will be signed in to "login.microsoft.com" with your passkey for "alice.hughes@contoso.com".
Continue
Other Sign In Options
Sign In
Use Face ID to sign in?
You will be signed in to "login.microsoft.com" with your passkey for "alice.hughes@contoso.com".
Signing in
Other Sign In Options

Android

- Android 9 podporuje Credential Manager API
- Vydání vyžaduje podporovanou verzi Google Play Services
- Vydání požaduje nastavení zámku obrazovky
- Vydání vyžaduje využití API nebo nativního prohlížeče (WebView / SystemView)
- Android 14 s nativní podporou Passkey a 15 s úpravami dialogů





Třetí strany

- 1Password
- Keeper
- A další poskytovatelé správců hesel…

Internetové prohlížeče a aplikace

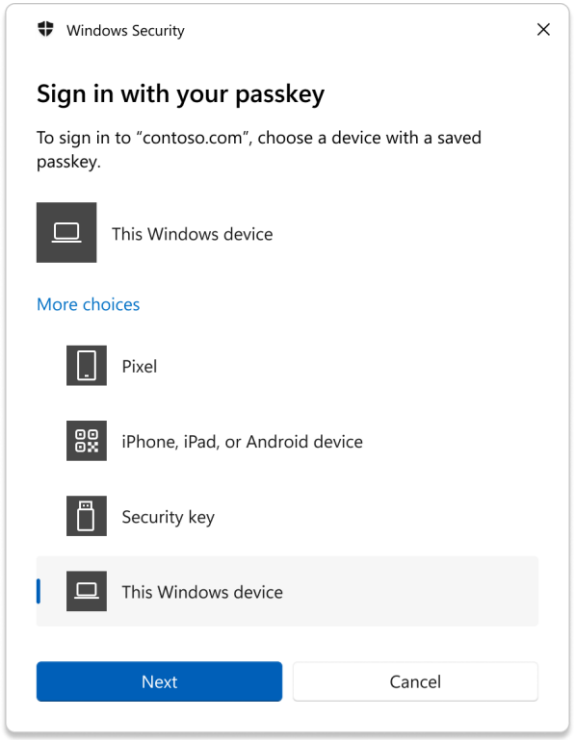
OS	Chrome	Edge	Firefox	Safari
Windows	✅	✅	✅	N/A
macOS	✅	✅	✅	✅
ChromeOS	✅	N/A	N/A	N/A
Linux	✅	✅	✅	N/A
iOS	✅	✅	✅	✅
Android	✅	✅	❌	N/A

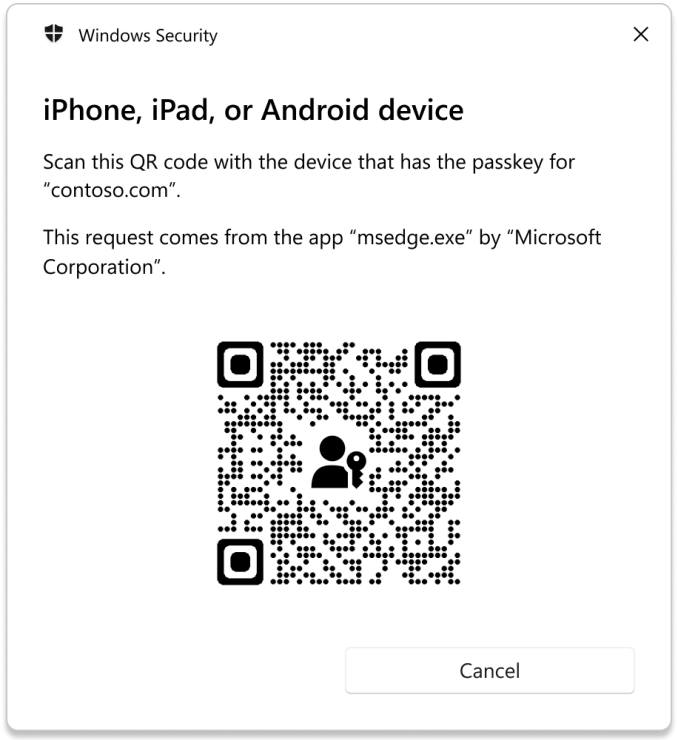
Internetové prohlížeče a aplikace

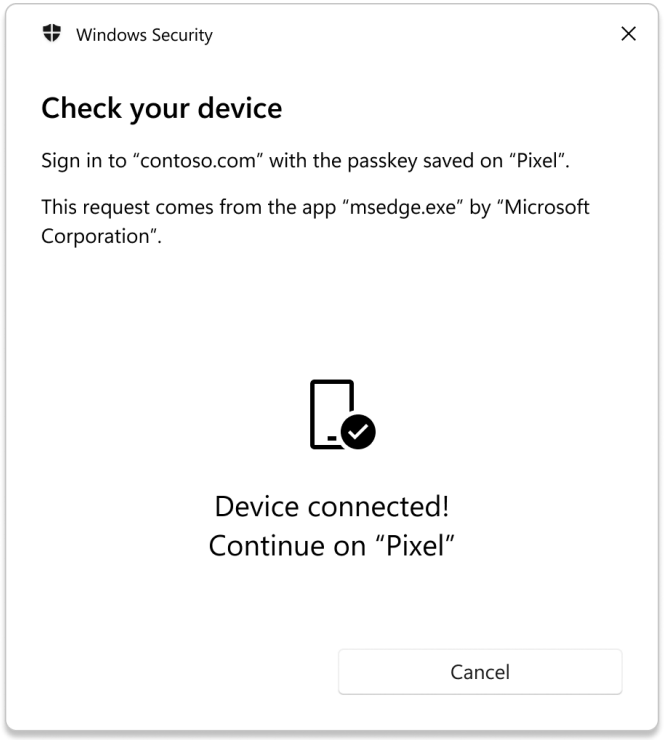
Browser / OS	iOS	macOS	Android	Windows	Linux
Safari	✓ Safari 16.1+	✓ Safari 16.1+	— n/a	— n/a	— n/a
Chrome	✓ Chrome, Brave, Edge	✓ Chrome 108+	✓ Chrome 108+	✓ Chrome 108+	✓
Edge	✓ Chrome, Brave, Edge	✓ Chrome 108+	✓ Chrome, Brave, Edge	✓ Chrome 108+	✓
Firefox	✓	✓ Firefox 122+	✓ Firefox 122+	✓ Firefox 122+	✓
Native app	✓ iOS apps	✓ Mac apps	✓ Android apps	✓ Windows apps	— Phone passkeys (QR code flow) and security keys only

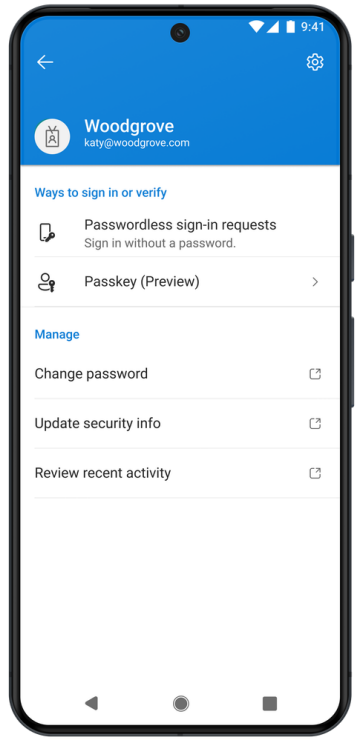
Cross-Device Authentication

- Dokončení procesu na jiném zařízení pomocí QR kódu a Bluetooth









Na co si dát pozor

- Adopce koncovými uživateli
  - Měnící se vzhled na jednotlivých platformách a aplikacích
- Využití hesla versus Passkey
  - Našeptávač hesel a správce hesel
  - Záleží na službě či aplikaci (další faktor, primární faktor, jediný faktor)
- Změny URL aplikací pro přihlášení
  - Vzpomeňte na Twitter a jeho přejmenování na X
  - login.onmicrosoft.com
- Dostupnost Bluetooth spojení
  - Vypnuté nebo není k dispozici
  - Vypršení časového limitu pro aktivaci
- Záložní metody pro obnovení přístupu a nástup do organizace
  - Temporary Access Pass

Hardware

- Biometrické sensory pro Windows Hello
- Biometrické sensory pro FaceID a TouchID
- Biometrické sensory pro Android a jejich různorodost
- Dostupnost kamery pro Cross-Device ověření
- Dostupnost Bluetooth pro Cross-Device ověření
  - Zakázané párování s BT
  - Bluetooth Low Energy

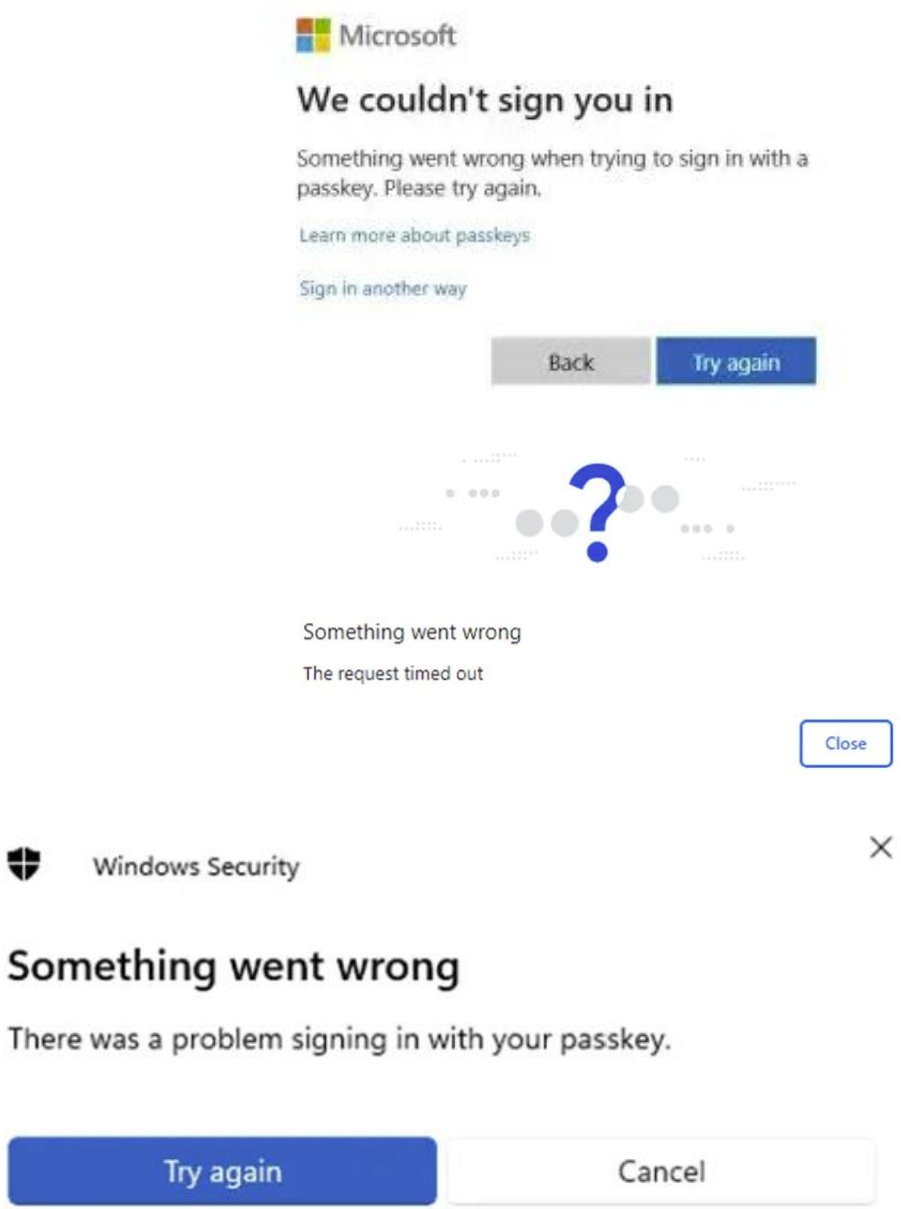
- OMA-URI: `./Device/Vendor/MSFT/Policy/Config/Bluetooth/`ServicesAllowedList
- Data type: **String**
- Value: `{0000FFFD-0000-1000-8000-00805F9B34FB};{0000FFF9-0000-1000-8000-00805F9B34FB}`

Set a list of allowable Bluetooth services and profiles:
- FIDO Alliance Universal Second Factor Authenticator service (`0000fffd-0000-1000-8000-00805f9b34fb`)
- FIDO2 secure client-to-authenticator transport service (`0000FFF9-0000-1000-8000-00805F9B34FB`)

For more information, see FIDO CTAP 2.1 standard specification and Bluetooth Assigned Numbers document.

A ještě pár drobností

- Když je uživatel pomalý
  - 60 sekund WebAuthN v Google Chrome
- Když je uživatelovo internet pomalý
  - 600 sekund dle specifikace
- Když je nedostupná atestace
  - Registrace se nezdařila
- Když je vyžadována atestace
  - Registrace se nezdařila



Atestace

- Preferovaná bezpečností
- Problémová pro uživatele
- Blokuje Cross-Device požadavky
- Attestation Requirements
  - Microsoft relies on the FIDO Alliance Metadata Service (MDS) to determine passkey authenticator compatibility with Windows, Microsoft Edge browser, and online Microsoft accounts. Vendors report data to the FIDO MDS.
  - FIDO2 standards (WebAuthn and CTAP) require providers to return a valid attestation statement.
  - The specific requirements vary based on how an administrator configures attestation requirements in the Passkeys (FIDO2) policy.

Internetová konektivita

- Neblokujeme některá URL?
- Služby Apple
- Služby Microsoft
- Atestační služby

Requirements

- Microsoft Entra multifactor authentication (MFA).
- Android 14 and later or iOS 17 and later.
- For cross-device registration and authentication:
  - Make sure that Bluetooth and an active internet connection are enabled on both devices. If your organization restricts Bluetooth usage, you can permit Bluetooth pairing exclusively with passkey-enabled FIDO2 authenticators to allow cross-device passkey sign-in and registration. Your organization needs to allow connectivity to endpoints in the following table to enable cross-device registration and authentication. Devices must be allowed to reach these URLs. For more information about requirements for Apple devices, see Use Apple products on enterprise networks.

Expand table

Platform	URL
Android	`cable.ua5v.com`

iOS	`cable.auth.com`
	`app-site-association.cdn-apple.com`
	`app-site-association.networking.apple`

Note

Users can't use cross-device registration if you enable attestation.

V neposlední řadě

- Politiky podmíněného přístupu
  - Require Compliant Device
  - Require Application Protection

> ⓘ Note
>
> If you grant the **Require device to be marked as compliant** control as part of a Conditional Access policy, it doesn't block Microsoft Authenticator app access to the UserAuthenticationMethod.Read scope. Authenticator needs access to the UserAuthenticationMethod.Read scope during Authenticator registration to determine which credentials a user can configure. Authenticator needs access to UserAuthenticationMethod.ReadWrite to register credentials, which doesn't bypass the **Require device to be marked as compliant** check.

A tedy hlavně!

- Co když se nám někdo rozhodne vdát nebo změnit pohlaví?
- Změna UPN není plně podporována
  - If a user's UPN changes, you can no longer modify passkeys (FIDO2) to account for the change. If the user has a passkey (FIDO2), they need to sign in to Security info, delete the old passkey (FIDO2), and add a new one.

Ke zvážení a zamyšlení

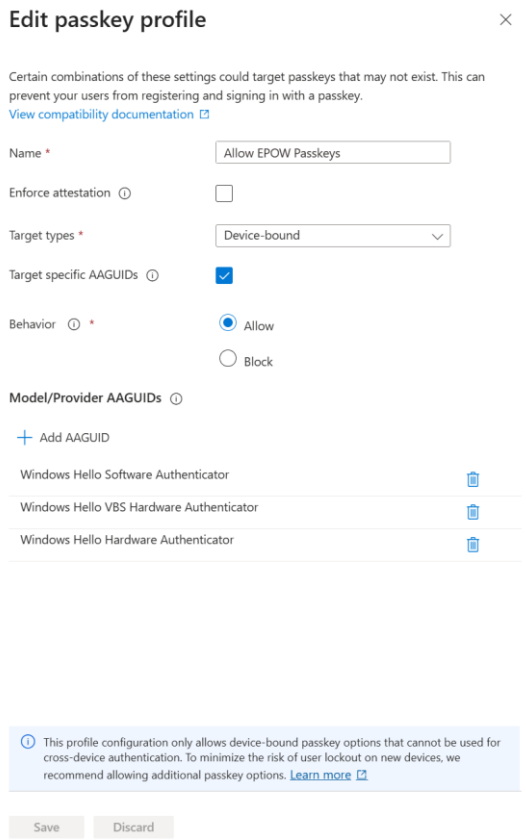
- macOS jen v rámci MDM pro nejlepší uživatelskou zkušenost
- Záložní metody a problémová atestace (TAP)
- Device-Bound nebo Syncable
- Virtualizovaná prostředí
- Procesy spojené s Passkeys
- Registrace metody neznamená nutnost ji používat
- Registrace metody neznamená, že nemám jinou metodu
- Downgrade Attacks
- Conditional Access Strenghts…

Nastavení

Rychlé intro do Entra ID a Passkeys

Nastavení ve zkratce

- Povolení profilu pro Passkey v autentizační politice
  - Passkey Enabled
- Vytvoření profilu pro Passkey (atestace, typ, skupiny)
  - Passkey Profile
- Povolení registrační kampaně
  - Registration Campaign
- Vynucení Passkeys přes autentizační síly v autentizační politice
  - Conditional Access Authentication Strengths



Zdroje a další postup

- Chcete Passkeys pochopit?
  - What is a Passkey? Secure Signins | Microsoft Security
  - FIDO Passkeys: Passwordless Authentication | FIDO Alliance
  - Passkeys (FIDO2) authentication method in Microsoft Entra ID | Microsoft Learn
- Chcete Passkeys nasadit vlastními silami?
  - How to enable passkeys (FIDO2) in Microsoft Entra ID | Microsoft Learn
  - Enable passkeys in Authenticator for Microsoft Entra ID | Microsoft Learn
  - Support for Passkeys in Windows | Microsoft Learn
  - Seriál FIDO2 Passkeys | SAMURAJ-cz.com 😍
- Chcete Passkeys nasadit externími silami?
  - Kontakt | KPCS 👷

Dotazy a diskuse

Petr Vlk
Microsoft MVP
Microsoft 365 Enterprise Security Architect @ KPCS CZ
KPCS vlk@kpcs.cz

Že nevíte, jak to vlastně v organizaci máte s MFA?
Nechte si ověřit skutečný stav nastavení našimi experty.

Definujte priority bezpečnosti: Zero Trust Workshop by KPCS

Ověřte si realitu IT prostředí: Security Risk Assessment by KPCS