YubiKey C Bio FIDO Edition uživatelský manuál

verze 1.00

Biometrický bezpečnostní token s USB-C rozhraním a podporou passwordless protokolu FIDO2 (bezheslové ověřování), pomocí kterého maximálně zabezpečíte e-mail, sociální sítě či kryptoburzu podporující FIDO2, a to pouhým otiskem prstu. Mechanická odolnost, voděodolnost a bezbateriový provoz, ideální na svazek klíčů.

Popis YubiKey C Bio FIDO Edition

Co je to YubiKey

YubiKey jsou univerzální bezpečnostní tokeny vyrobené švédskou společností Yubico. Nejčastěji se používají k zabezpečení přihlašování do služeb a aplikací na internetu (například emailové služby, sociální sítě, kryptoměnové směnárny) a to pomocí dodatečného stisknutí tlačítka, kterým je token vybaven. Pokud daná služba podporuje tokeny YubiKey jako tzv. *"druhý faktor ověření"*, útočníci se nemají šanci nabourat k datům uživatele (emaily, fotky, kryptoměny). V opačném případě lze informace odcizit a to pomocí jednoduchých nebo sofistikovaných technik, které mohou překvapit i profesionální uživatele internetu. Stačí, aby si útočník vybral vhodnou chvíli k útoku.

Dnes stále populární SMS kódy s omezenou platností, které musí uživatel opisovat do přihlašovacího formuláře, jsou jednou z mnoha oblíbených ověřovacích metod. Bohužel všechny tyto starší metody jsou zcela bezradné proti útočné technice zvané *"phishing"*. Spolehlivým nástupcem jsou bezpečnostní tokeny a specializované aplikace v mobilním telefonu (často již využívané některými bankami). Bezpečnostní tokeny ale narozdíl od mobilních aplikací nepotřebují ke svému fungování telefon, nemusí se instalovat a aktualizovat a jsou znovupoužitelné pro libovolné množství služeb, nikoliv pouze pro jednu konkrétní.

YubiKey tokeny podporují několik způsobů moderního ověřování (neboli *"autentizace"*), záleží vždy na konkrétní službě, jakou variantu FIDO2 protokolu nabídne.

Silný druhý faktor

Uživatel zadává jméno a heslo a poté odemyká a potvrzuje otiskem prstu na senzoru tokenu

Silný multi-faktor

Uživatel zadává jméno a heslo a poté odemyká a potvrzuje otiskem prstu na senzoru tokenu

Bezheslové ověřování

Uživatel bez zadání přihlašovacích údajů rovnou odemyká a potvrzuje otiskem prstu na senzoru tokenu

YubiKey modely se od sebe mírně liší, v prvé řadě konektorem, kterým se připojují do počítačů, notebooků či tabletů a potom také drobně funkční výbavou a principem potvrzování. Tomu také odpovídá odlišná cena.

V čem se Yubikey liší od ostatních tokenů

Na trhu je k dispozici celá řada produktů od různých výrobců. Vzhledem k tomu, že uživatel zabezpečuje své soukromí a citlivá data, měl by si zodpovědět na následující otázky:

- Chci si tokenem zabezpečit co největší počet služeb a aplikací?
- Chci mít jistotu, že token, na kterém bude záviset má bezpečnost, nemá zadní vrátka, která se dají zneužít?
- Potřebuji, aby token fungoval za každého počasí a byl vyroben z prověřených a kvalitních čipů a součástek?
- Když už investuji čas a usílí do používání bezpečnostního tokenu, existuje nějaké další jeho využití?

Pro uživatele, kteří si na všechny tyto otázky odpoví **"ano"**, neexistuje jiná volba než tokeny YubiKey.

Čísla a fakta

- **9 z 10** top IT firem na světě zavedlo YubiKey tokeny k ověřování svých zaměstnanců (Google, Facebook, Microsoft)
- Společnost Yubico založená v roce **2007** je spoluautorem standardu U2F (Universal 2nd Factor) a protokolu CTAP v rámci **FIDO Alliance** a standardu WebAuthn v rámci konsorcia **W3C**
- S YubiKey je proces ověřování **4x rychlejší** ve srovnání se SMS a OTP kódy
- Firmám, které YubiKey zavedly, klesl počet incidentů spojených s hesly průměrně o **92%**

Co YubiKey token naopak není?

YubiKey **není** flash disk. Nelze na něj nahrávat uživatelské soubory (fotky, videa, hudbu, dokumenty).

YubiKey **není** ani kryptopeněženka a nelze v něm držet ani bitcoin, ani jiné kryptoměny.

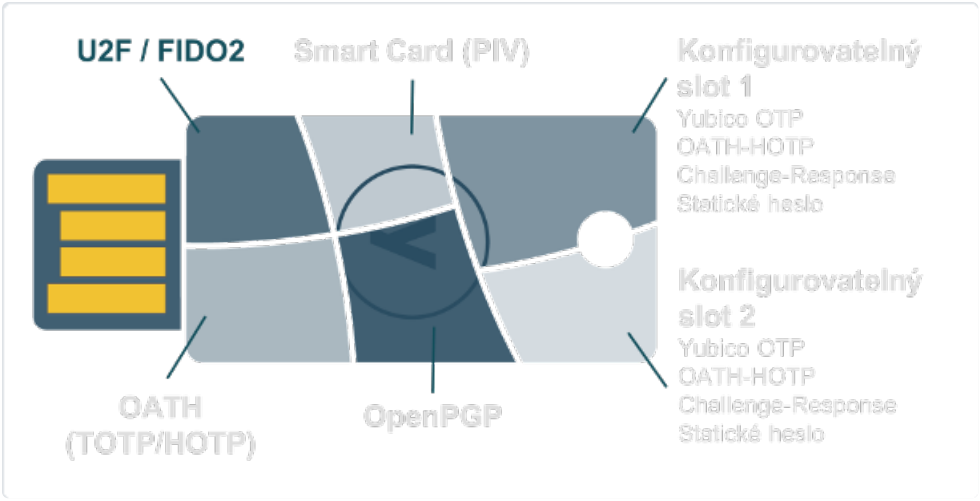
Princip potvrzování

YubiKey C Bio FIDO Edition disponuje tlačítkem, které uživatel stiskne a tím potvrdí prováděnou operaci (nemusí být vždy vyžadováno). Tlačítko je navíc i senzor, který snímá otisk prstu. U YubiKey 5 tokenů uživatel vedle stisku tlačítka zadává i číselný PIN, pokud je to potřeba (analogie je platební karta při výběru z bankomatu). S YubiKey C Bio FIDO Edition tento krok odpadá a PIN plně nahrazuje platný otisk prstu. Teprve ve chvíli, kdy se nepodaří otisk rozpoznat, token se uzamkne na biometrické úrovni a uživatel je vyzván k zadání PINu, kterým biometrii opět odemkne pro další použití.

Technické parametry

Základní parametry	
Název produktu	YubiKey C Bio FIDO Edition
Rozhraní	USB 2.0 (USB-C)
Princip potvrzování	Biometrický otisk prstu, mechanický dotek tlačítka
Funkcionalita	
Autentizační metody	Passwordless, Strong Two Factor, Strong Multi-Factor
Funkce	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F)
Certifikace	FIDO 2 Certified, FIDO Universal 2nd Factor (U2F) Certified
Typ zařízení	FIDO HID Device
Biometrie	
Počet otisků	5
Proces přiřazení otisku ve Windows	Yubico stránky (anglicky)
Proces přiřazení otisku v Chrome	Yubico stránky (anglicky)
Technické vlastnosti	
Stupeň krytí	IP68
Odolnost	neobsahuje baterie, neobsahuje pohyblivé částice, vysoká mechanická odolnost, voděodolnost
Barva	černá
Rozměry	18mm x 45mm x 3.75mm
Hmotnost	5g
Pracovní teplota	0°C - 40°C
Skladovací teplota	-20°C - 85°C
Rozměry obalu	55mm x 85mm x 5mm
Hmotnost včetně obalu	8g
Obsah balení	1 token
Další informace	
EAN	5060408464175
Země původu	Made in USA & Sweden
Výrobce	Yubico
Záruka	24 měsíců
Odkazy	
"YubiKey Bio FIDO Edition" Technický manuál výrobce (anglicky)	

Funkce



YubiKey C Bio FIDO Edition disponuje funkčním modulem FIDO2 s podporou U2F protokolu. S počítačem, tabletem nebo telefonem tento modul komunikuje skrze rozhraní:

- **FIDO** rozhraní se také hlásí jako HID klávesnice, nicméně je zde potřeba navíc podpora speciálního FIDO protokolu. Tím disponují všechny zařízení s prohlížečem podporující protokol WebAuthn (na iOS od verze 13)

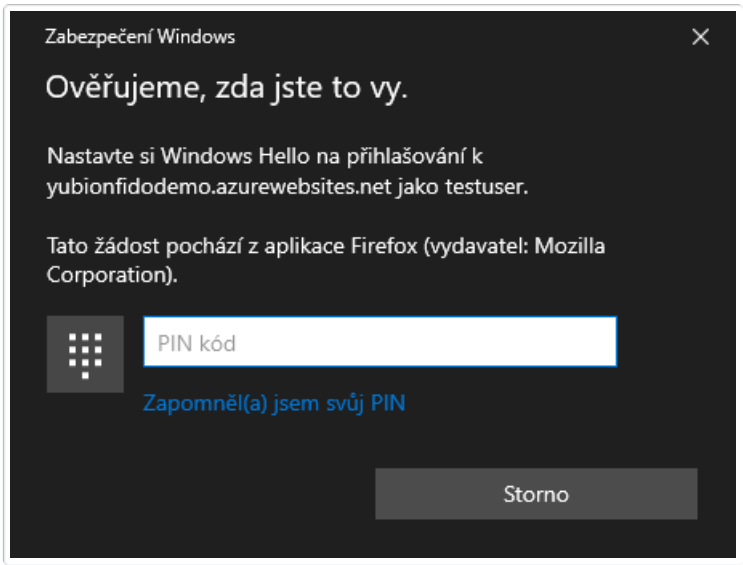
Ostatní protokoly nejsou dostupné, narozdíl od tokenů YubiKey 5.

FIDO2

FIDO2 projekt představuje společné úsilí FIDO Alliance a sdružení W3C a výsledkem tohoto je silný autentizační protokol, jehož základy tvoří standard WebAuthn (standardizuje autentizaci na webu) a protokol CTAP2 (zajišťuje komunikaci mezi klientem, typicky webovým prohlížečem a ověřovacím prostředkem, např. bezpečnostním tokenem, u kterého je navíc definovaná nutnost potvrzení akce, tj. například stisknutí tlačítka, zadání PINu nebo potvrzení otisku prstu). FIDO2 je následovníkem standardu U2F a je zpětně kompatibilní.

YubiKey C Bio FIDO Edition podporuje všechny scénáře FIDO2 podporované řadou YubiKey 5. Token lze použít ve scénáři bezheslového přihlašování i ve scénáři s heslem. V obou případech se místo PINu použije otisk prstu, podobně jako se používá biometrie na chytrém telefonu. Existují však případy, kdy je PIN vyžadován a to při registraci služby nebo jiné správě otisků prstů, stejně jako u chytrého telefonu. Jediná možnost jak zadat PIN je však po 3 neúspěšných pokusech snímání otisku prstu.

FIDO2 přihlašovací proces je konfigurovatelný a záleží na provozovateli dané služby, kterou variantu zvolí. Pro lepší představu uvádíme několik možných scénářů. Pokud máte na svém Windows PC aktivní Windows Hello, bude na vás pravděpodobně před výzvou k zapojení YubiKey vyskakovat výzva, kterou je potřeba **stornovat**.

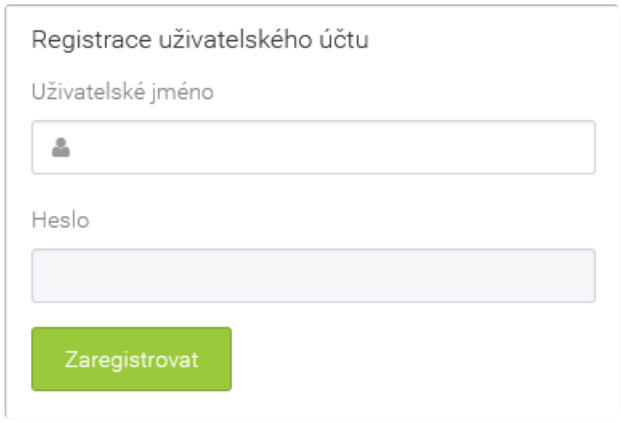


Tradiční 2FA

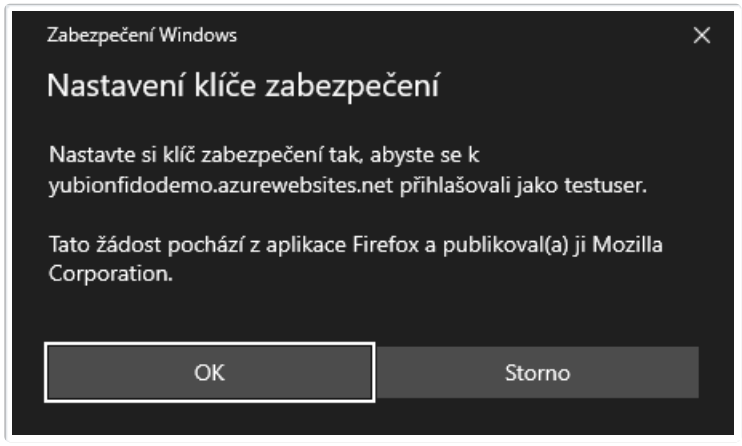
Klasické přihlašování s heslem, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě).

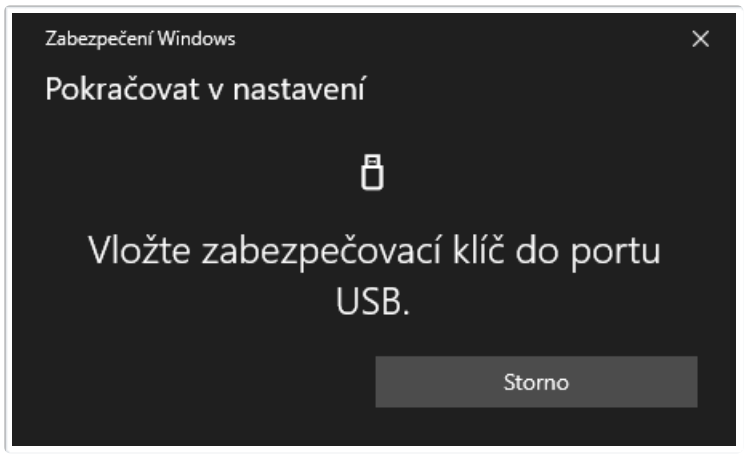
Fáze registrace

1. Uživatel zvolí uživatelské jméno a heslo

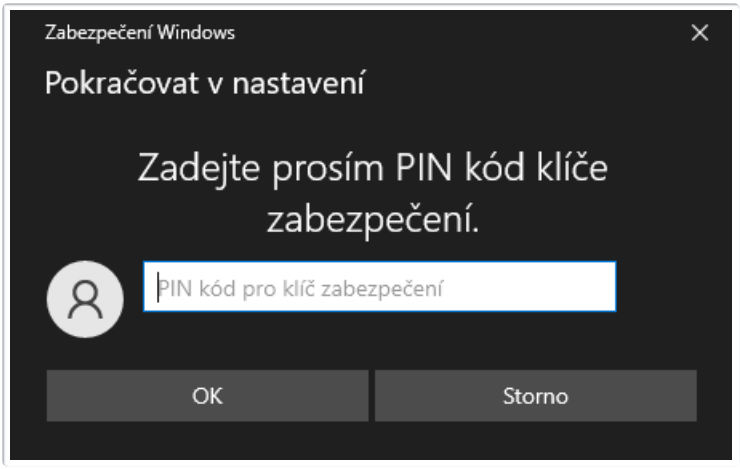


2. Uživatel je vyzván, aby připojil YubiKey

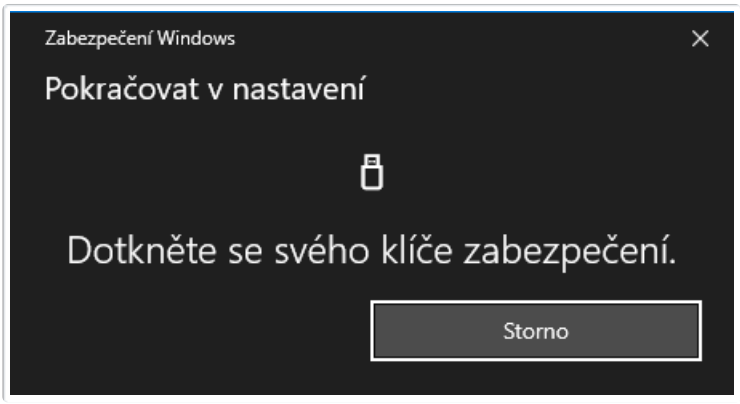




3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání (jinak se tento krok přeskočí)

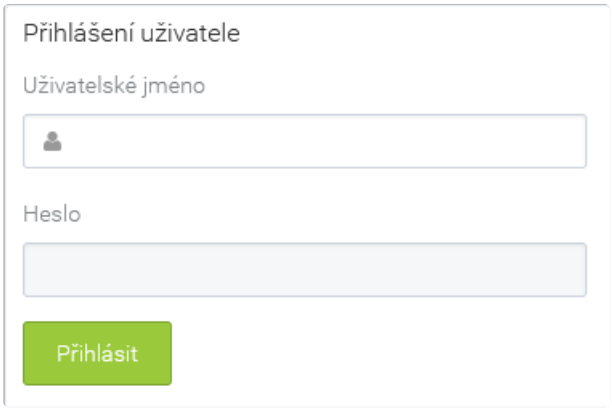


4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey

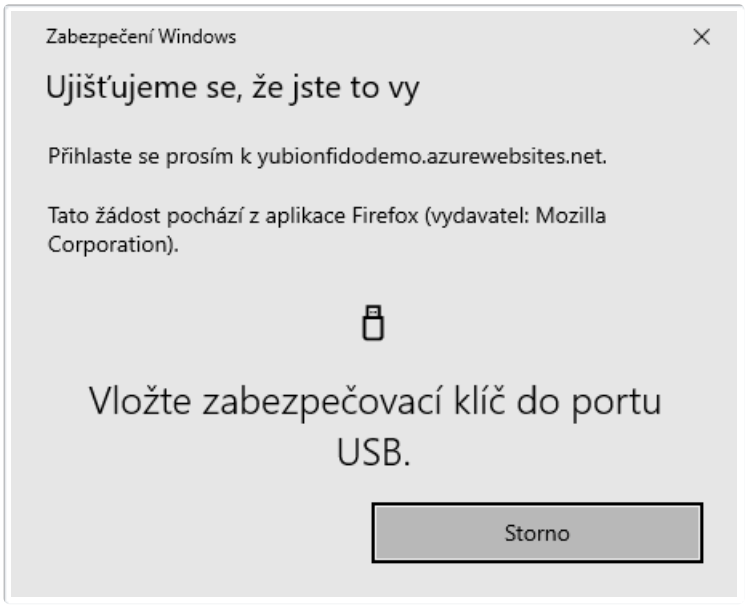


Fáze přihlášení

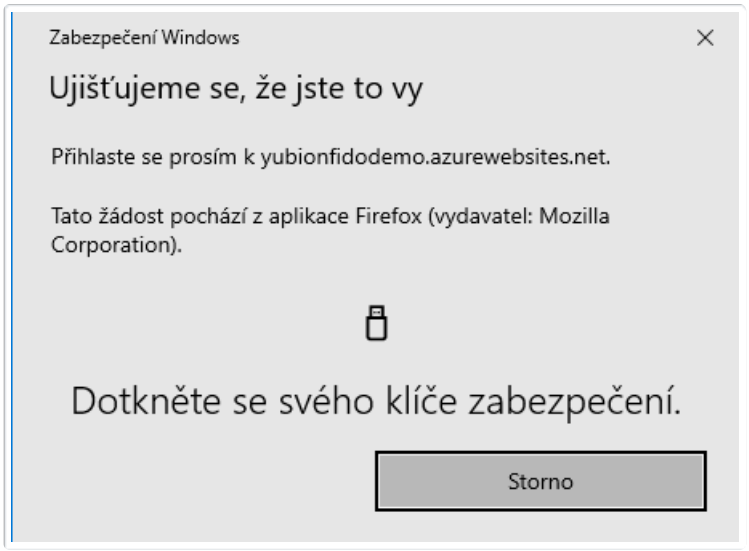
1. Uživatel zadá uživatelské jméno a heslo



2. Uživatel je vyzván, aby připojil YubiKey



3. Uživatel dokončí přihlašování stisknutím tlačítka na YubiKey

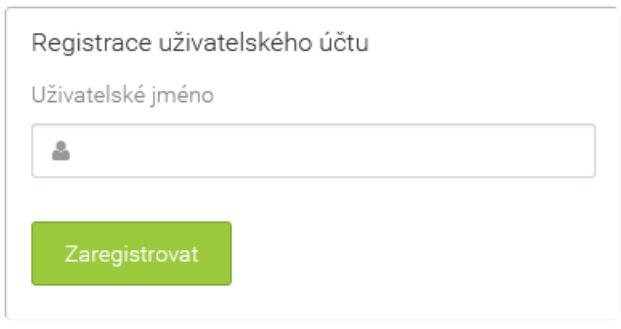


Bezheslové (passwordless) přihlášení s uživatelským jménem

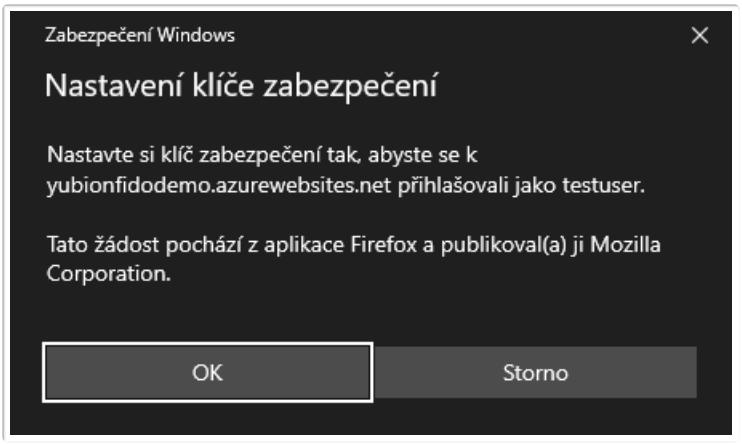
Bezheslové přihlašování s uživatelským jménem, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě)

Fáze registrace

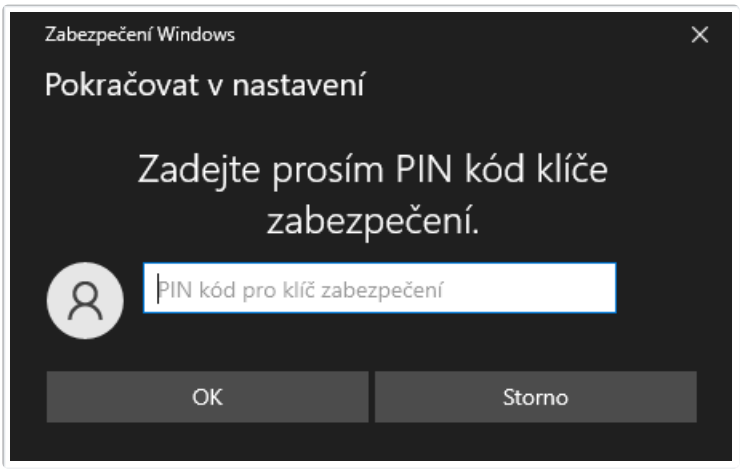
1. Uživatel zvolí uživatelské jméno



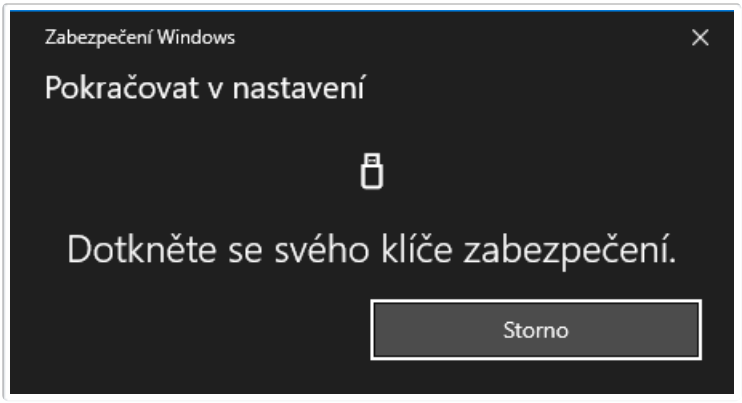
2. Uživatel je vyzván, aby připojil YubiKey



3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání (jinak se tento krok přeskočí)



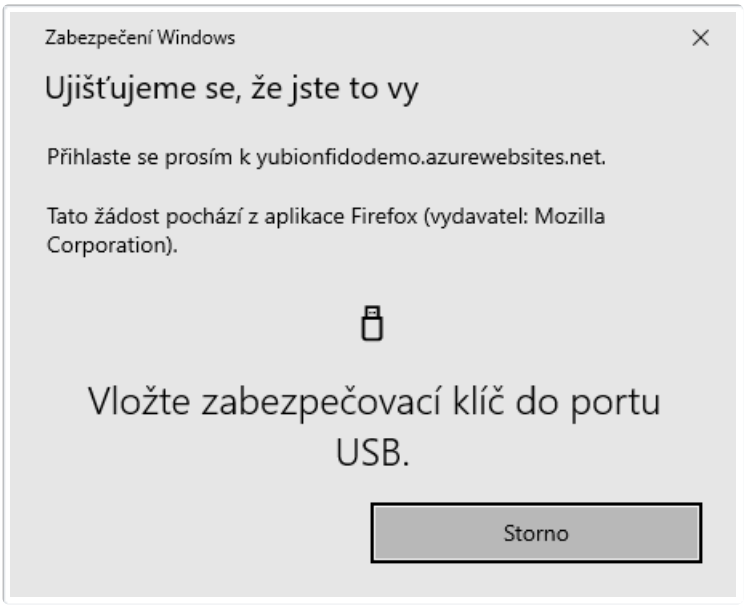
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



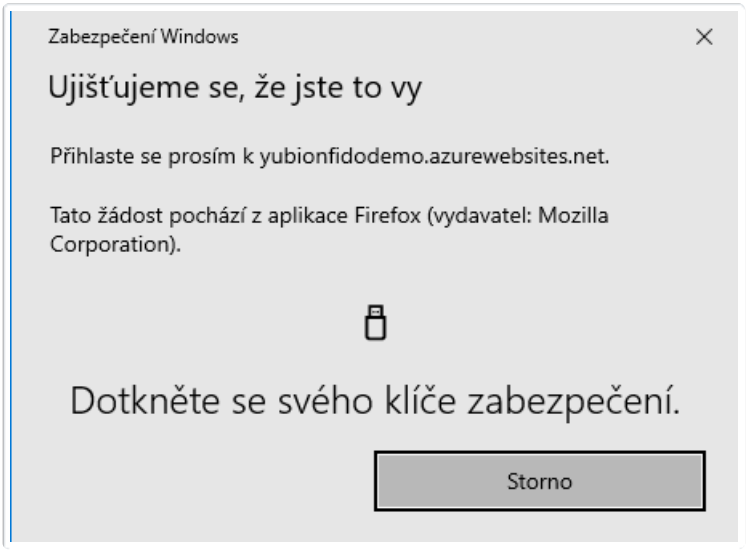
Fáze přihlášení

1. Uživatel zadá uživatelské jméno

2. Uživatel je vyzván, aby připojil YubiKey



3. Uživatel dokončí přihlašování stisknutím tlačítka na YubiKey

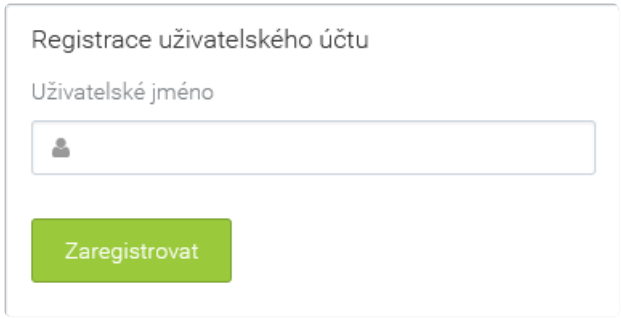


Bezheslové (passwordless) přihlášení bez uživatelského jména

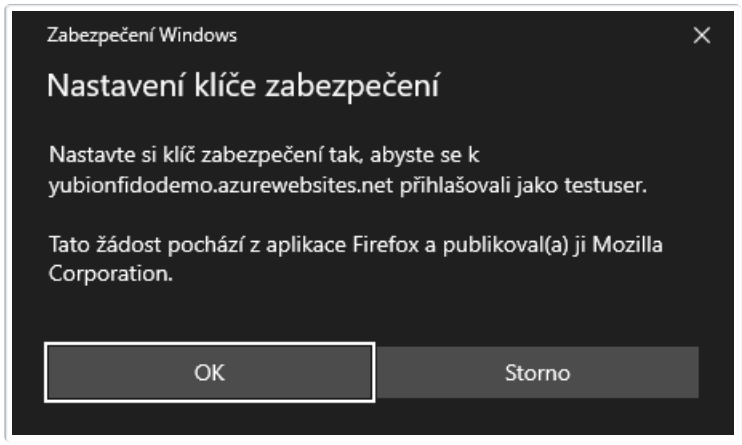
Bezheslové přihlašování bez uživatelského jména, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto scénářem je omezen kapacitou tokenu na 25 (v tokenu se ukládá uživatelské jméno a obecné informace ke službě).

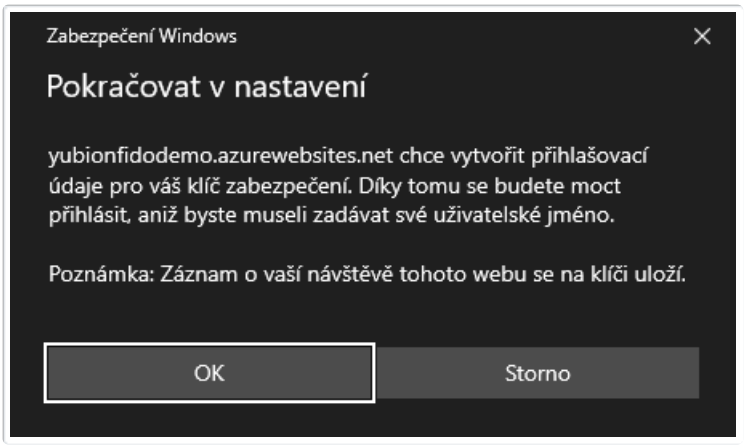
Fáze registrace

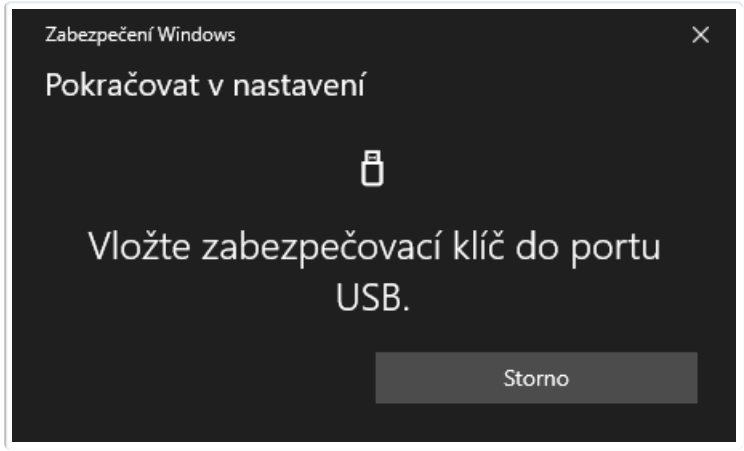
1. Uživatel zvolí uživatelské jméno



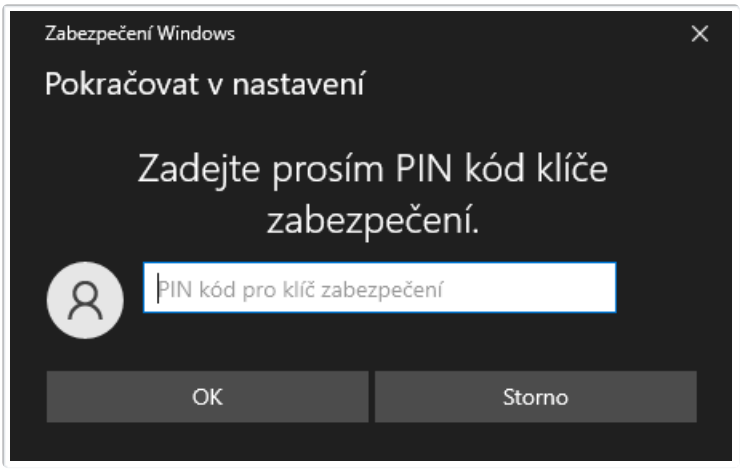
2. Uživatel je vyzván, aby připojil YubiKey



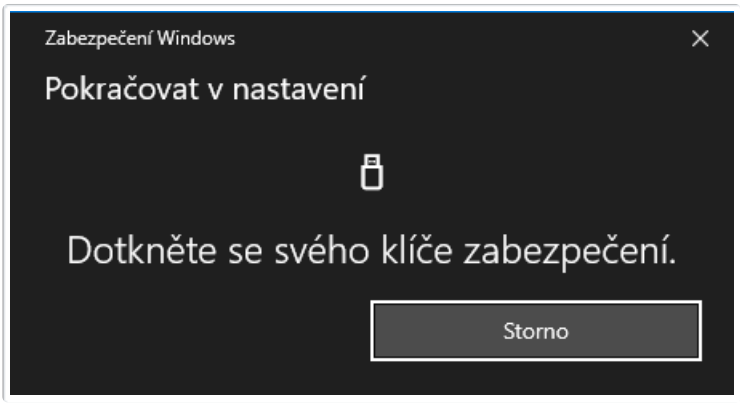




3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání (jinak se tento krok přeskočí)



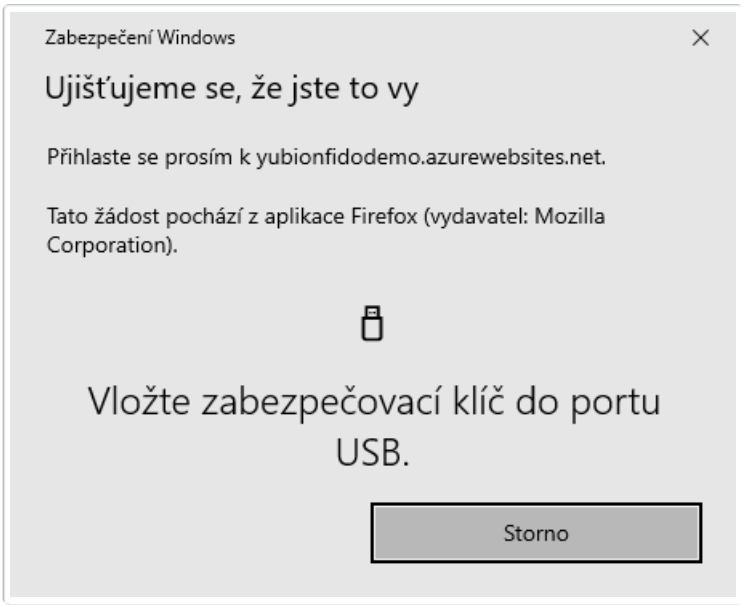
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



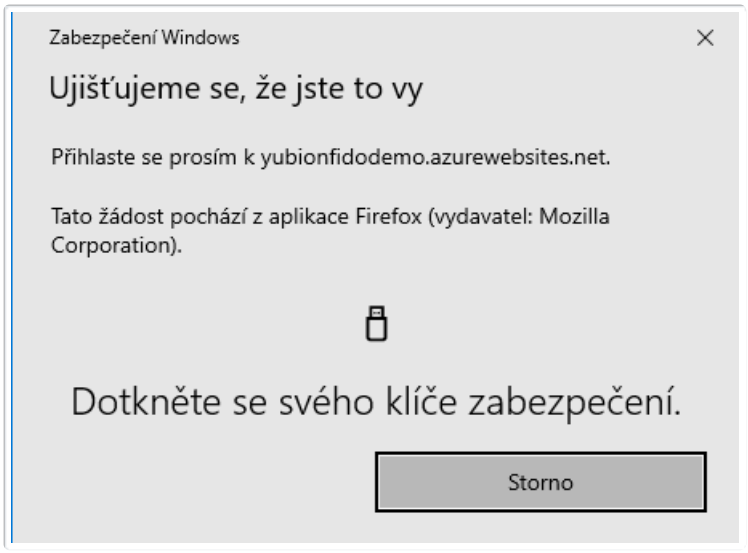
Fáze přihlášení

1. Uživatel nezadává žádné přihlašovací údaje a rovnou stiskne tlačítko přihlásit

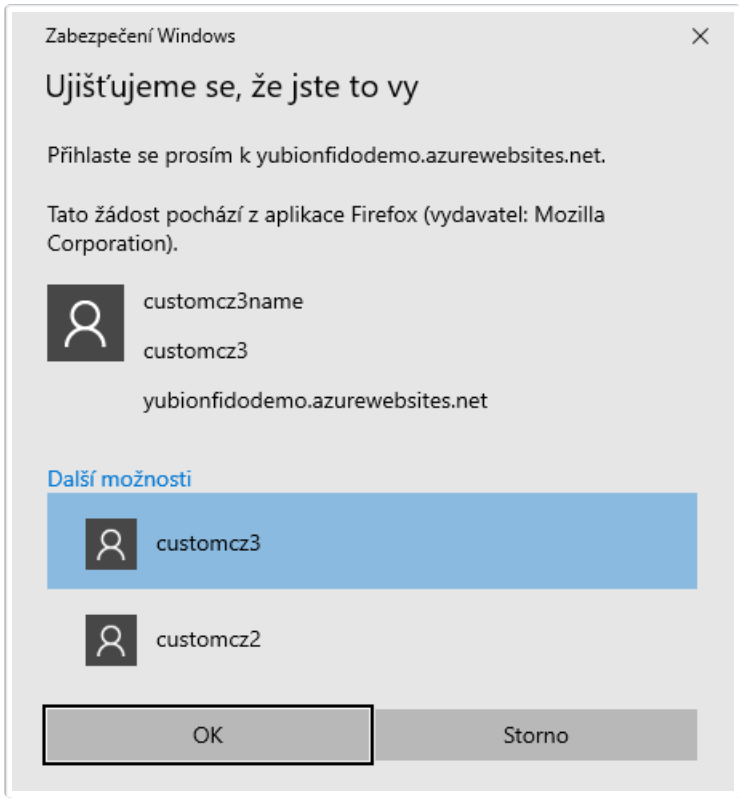
2. Uživatel je vyzván, aby připojil YubiKey



3. Uživatel potvrdí přihlašování stisknutím tlačítka na YubiKey



4. Pakliže existuje více registrovaných uživatelských jmen k danému YubiKey, je uživatel vyzván k výběru jednoho z nich (jinak se tento krok přeskočí)

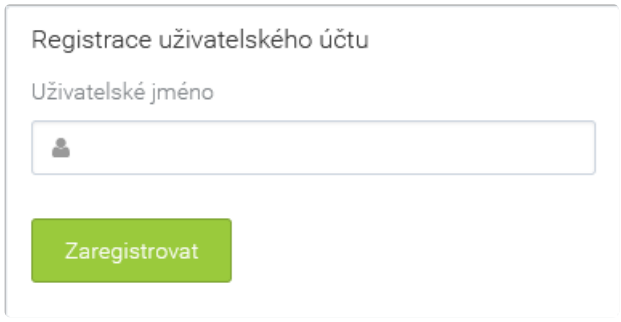


MFA bezheslové (passwordless) přihlášení s uživatelským jménem

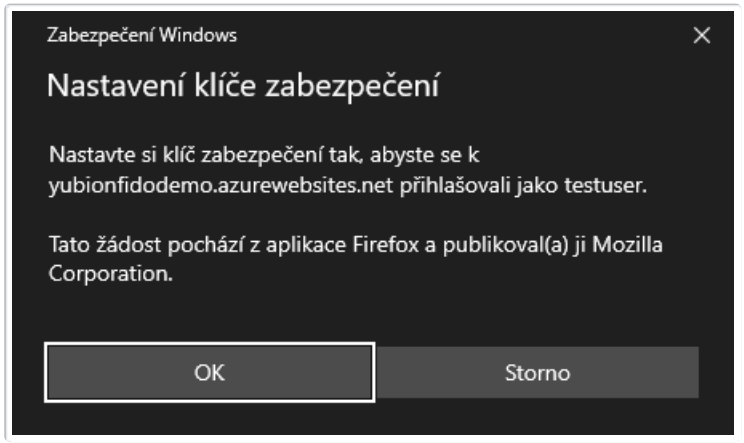
Bezheslové přihlašování s uživatelským jménem, kdy token slouží jako multi-faktor k ověření (zadává se i PIN). Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě).

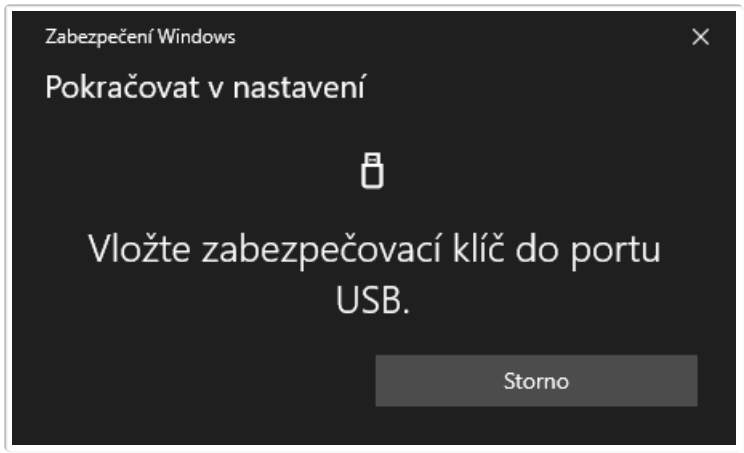
Fáze registrace

1. Uživatel zvolí uživatelské jméno

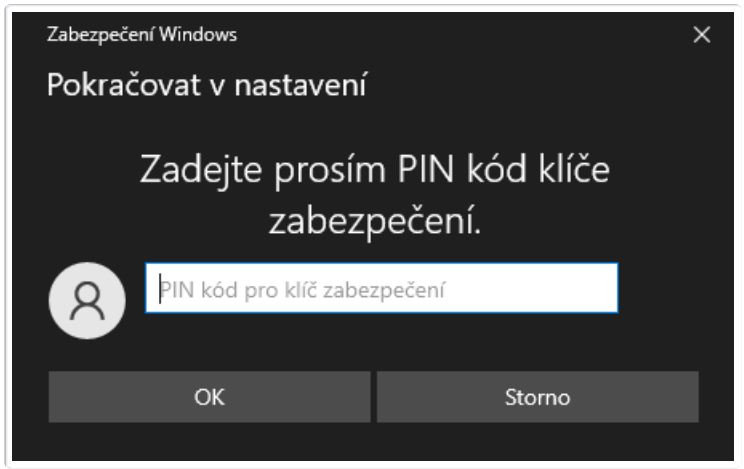


2. Uživatel je vyzván, aby připojil YubiKey

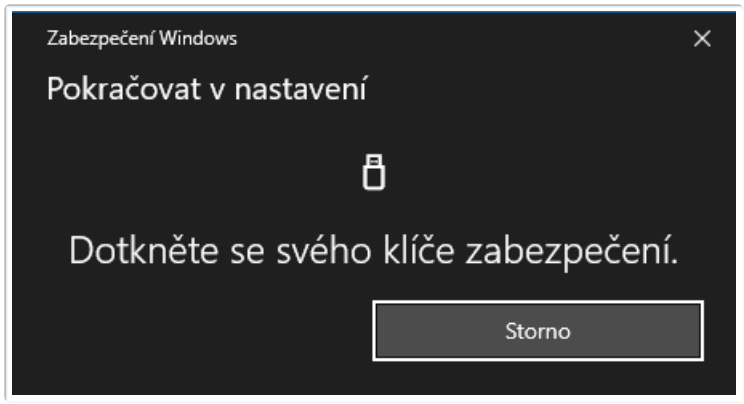




3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání, pokud nikoliv, je vyzván k jeho vytvoření (včetně dodatečného stisku YubiKey tlačítka)



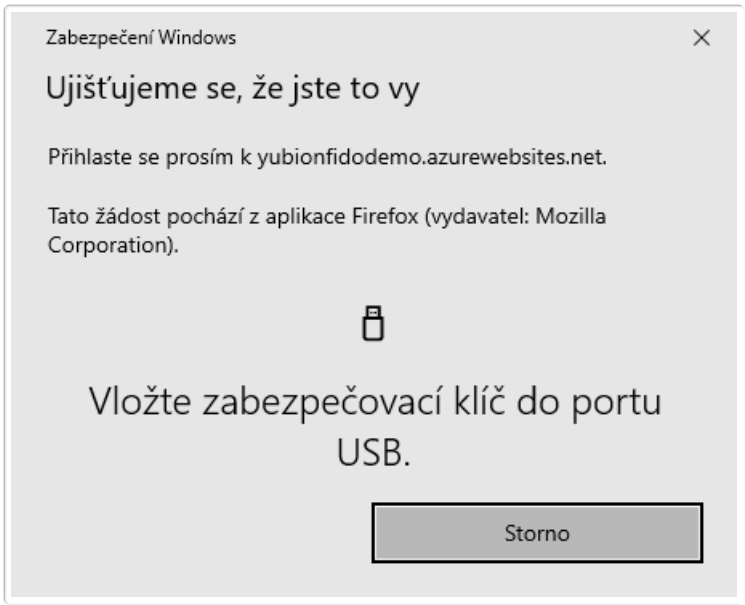
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



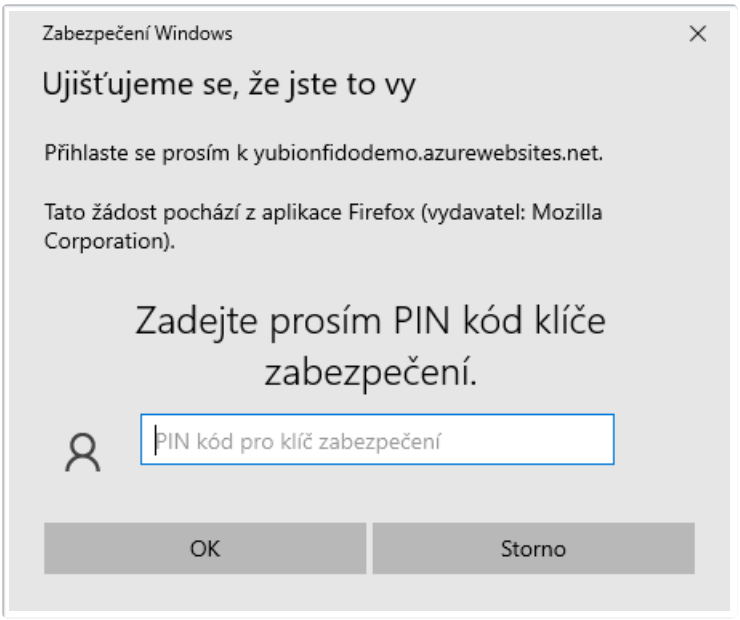
Fáze přihlášení

1. Uživatel zadá uživatelské jméno

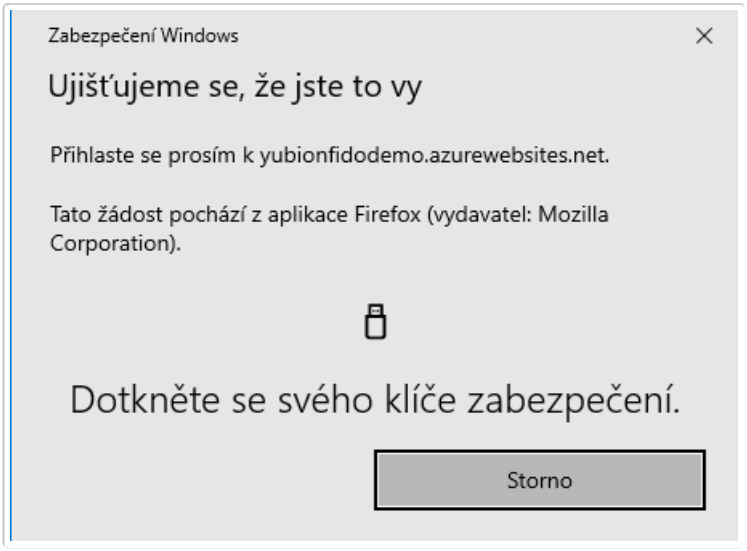
2. Uživatel je vyzván, aby připojil YubiKey



3. Uživatel je vyzván, aby zadal PIN kód k YubiKey



4. Uživatel potvrdí přihlašování stisknutím tlačítka na YubiKey

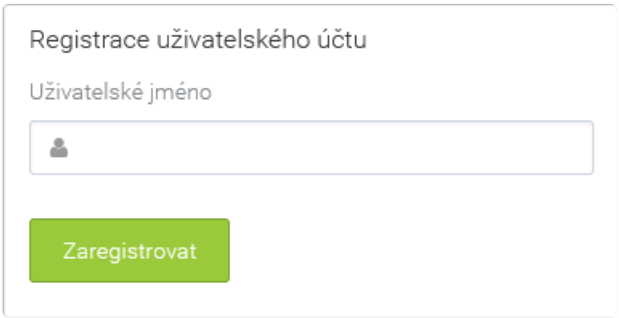


MFA bezheslové (passwordless) přihlášení bez uživatelského jména

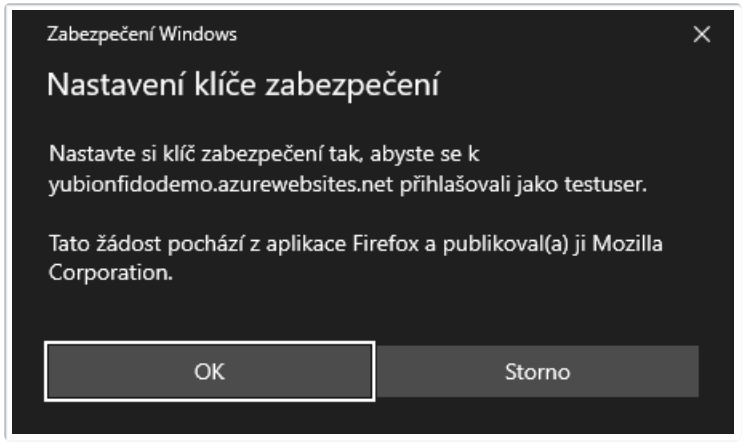
Bezheslové přihlašování bez uživatelského jména, kdy token slouží jako multi-faktor k ověření (zadává se i PIN). Lze vyzkoušet demo (zaškrtnout u registrace *requireResidentKey* a zvolit *userVerification: required* u registrace i autentizace). Počet spárovaných služeb využívající token tímto scénářem je omezen kapacitou tokenu na 25 (v tokenu se ukládá uživatelské jméno a obecné informace ke službě).

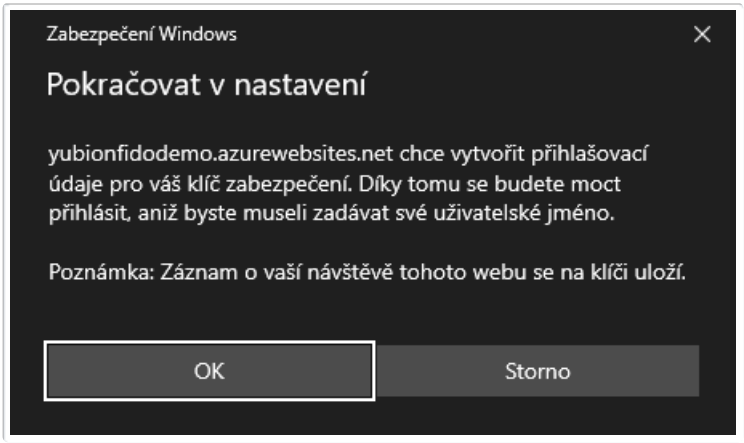
Fáze registrace

1. Uživatel zvolí uživatelské jméno

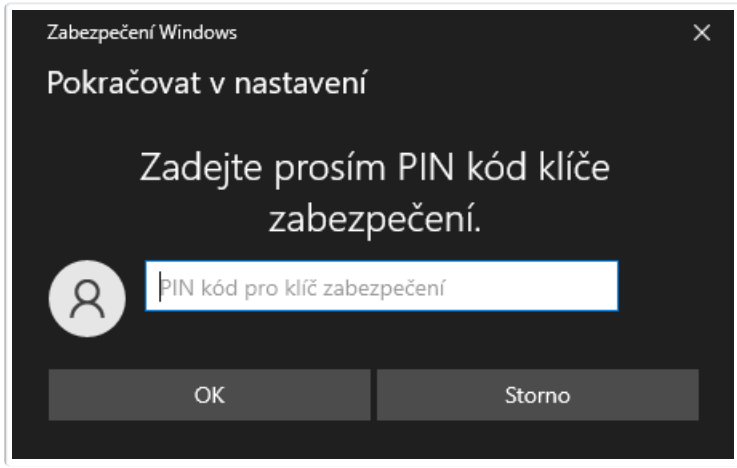


2. Uživatel je vyzván, aby připojil YubiKey

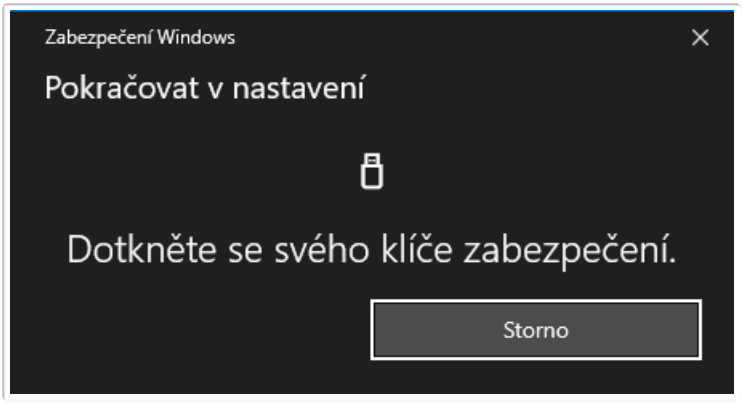




3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání, pokud nikoliv, je vyzván k jeho vytvoření (včetně dodatečného stisku YubiKey tlačítka)



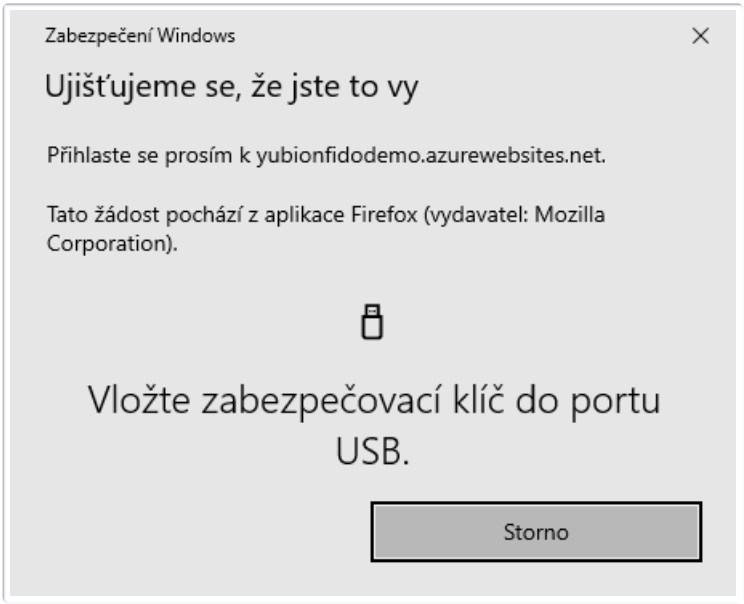
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



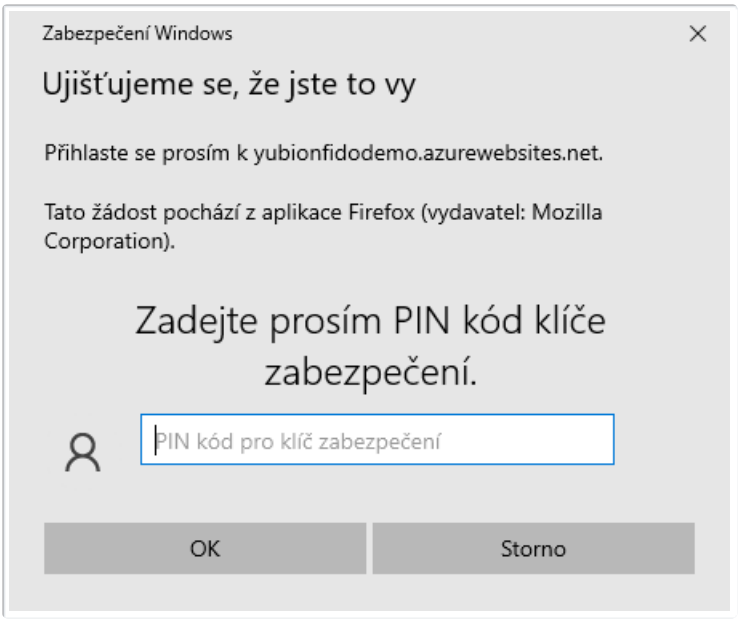
Fáze přihlášení

1. Uživatel nezadává žádné přihlašovací údaje a rovnou stiskne tlačítko přihlásit

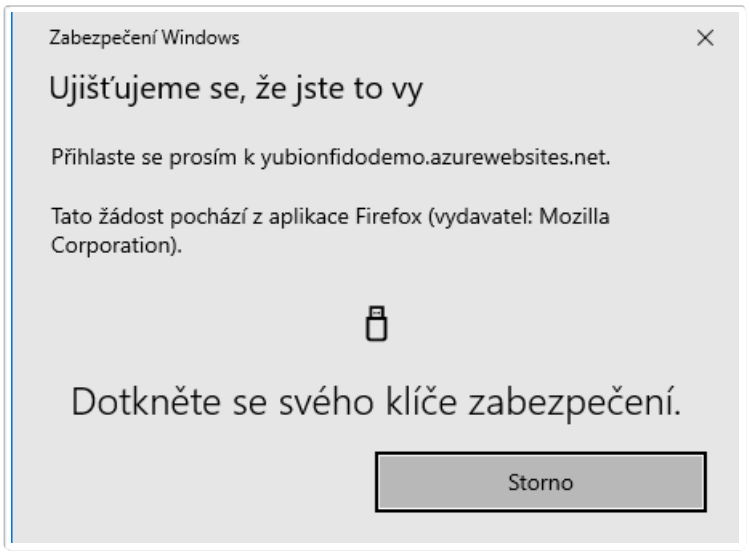
2. Uživatel je vyzván, aby připojil YubiKey



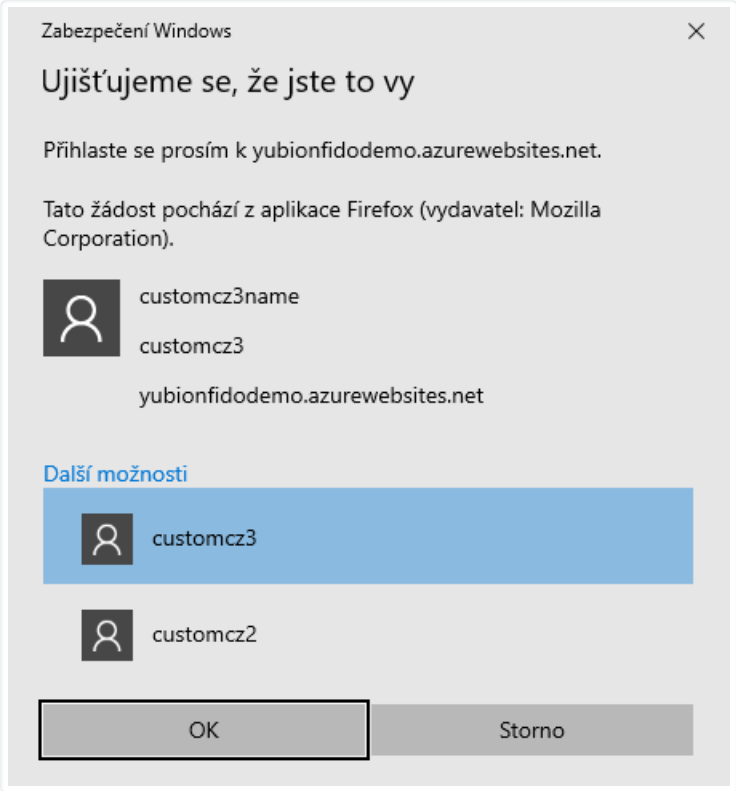
3. Uživatel je vyzván, aby zadal PIN kód k YubiKey



4. Uživatel potvrdí přihlašování stisknutím tlačítka na YubiKey



5. Pakliže existuje více registrovaných uživatelských jmen k danému YubiKey, je uživatel vyzván k výběru jednoho z nich (jinak se tento krok přeskočí)



FIDO2 technické informace	
USB Interface	FIDO
Maximální počet spárovaných služeb	neomezeně, 25 s uloženým uživatelským jménem
PIN	defaultní hodnota: není 4-63 znaků jakmile je jednou nastaven, lze ho změnit po jeho zadání lze ho odstranit resetem celého FIDO2 modulu pokud je PIN 3x po sobě zadán chybně, je potřeba token vyndat a znovu zandat do USB, neúspěšné pokusy jsou započítány pokud je PIN 8x po sobě zadán chybně, FIDO2 modul se zamkne a je nutné ho vyresetovat počet zbývajících pokusů lze zobrazit skrze YubiKey Manager
Reset	lze provést skrze YubiKey Manager token bude potřeba znovu zaregistrovat u všech služeb neprovádět bez záložního tokenu, nebo dojde ke ztrátě přístupu k registrovaným službám automaticky vyresetuje i všechny U2F zaregistrované služby
Certifikace	FIDO 2 Level 1 (FIDO® Certified)
Yubico testovací stránka na vyzkoušení protokolu	Yubico FIDO2 test
Nejznámější globální služby podporující FIDO2	Zobrazit aplikace
Nejznámější české služby podporující FIDO2	mojeID - úroveň **značná**
Postup registrace záložního tokenu	doporučeno ihned při registraci primárního tokenu, ale lze kdykoliv později bez omezení
Kompatibilita	
Podpora v prohlížeči	Yubico stránky (anglicky)

Podpora v prohlížeči	přehled (anglicky)
Odkazy	
Technický manuál - FIDO2	Yubico stránky (anglicky)
Technický manuál - WebAuthn	Yubico stránky (anglicky)
Domovská stránka FIDO2	FIDO Alliance (anglicky)
WebAuthn popis	Yubico stránky (anglicky)

U2F

U2F je zkratkou pro Universal 2nd Factor a představuje otevřený standard navržený FIDO Aliancí v roce 2014. Standard byl nahrazen mnohem robustnějším standardem FIDO2.

U2F proces se stejně jako u FIDO2 rozděluje na dvě fáze, registrační a přihlašovací. Narozdíl od FIDO2 není tak variabilní a nepoužívá vůbec PIN.

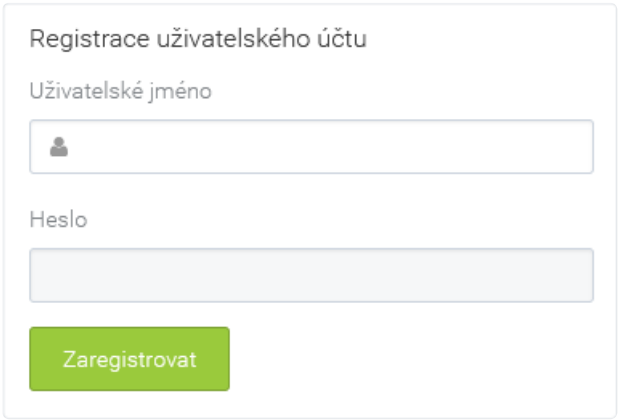
Pokud uživatel 3x potvrdí token neznámým otiskem prstu, token se uzamkne na biometrické úrovni a je potřeba ho odemknout PINem. Ten ale u U2F protokolu není podporovaný, služba zadání PINu nenabídne a vznikne trochu nekomfortní situaci, kdy je potřeba zadat PIN jiným způsobem (např. přes YubiKey Manager).

Tradiční 2FA

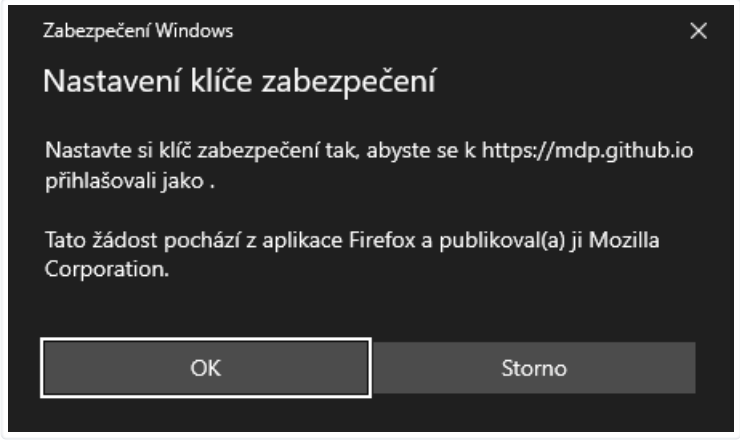
Klasické přihlašování s heslem, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet na demo nebo na demo. Počet spárovaných služeb využívající token tímto scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě).

Fáze registrace

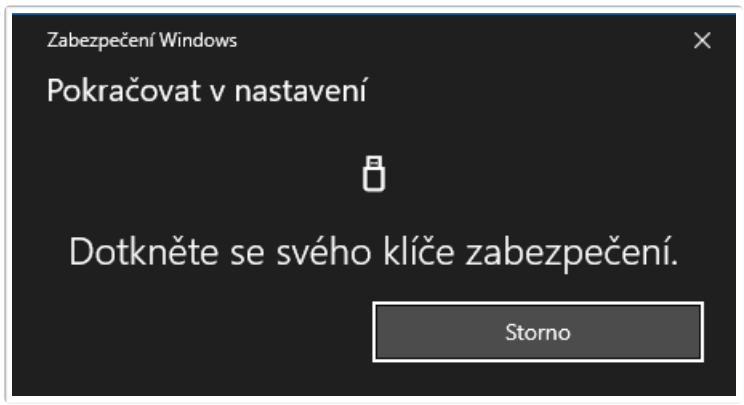
1. Uživatel zvolí uživatelské jméno a heslo



2. Uživatel je vyzván, aby připojil YubiKey

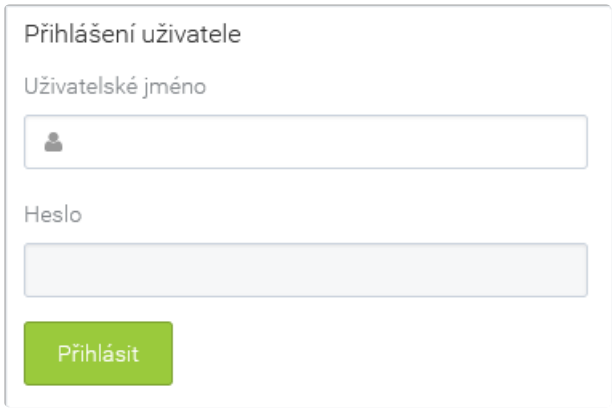


3. Uživatel dokončí registraci stisknutím tlačítka na YubiKey

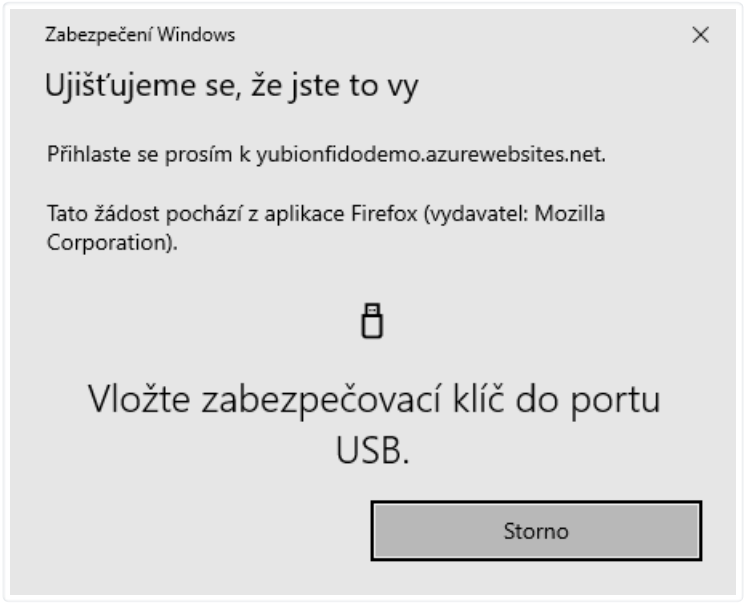


Fáze přihlášení

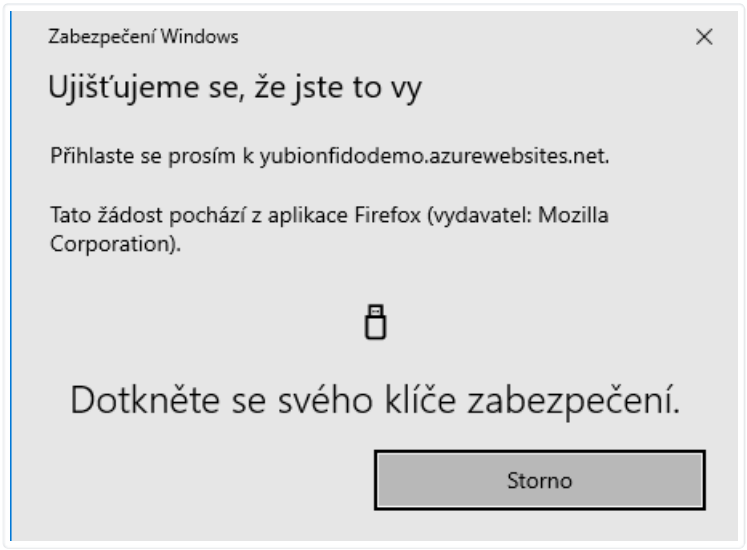
1. Uživatel zadá uživatelské jméno a heslo



2. Uživatel je vyzván, aby připojil YubiKey



3. Uživatel dokončí přihlašování stisknutím tlačítka na YubiKey



U2F technické informace	
USB Interface	FIDO
Maximální počet spárovaných služeb	neomezeně
PIN	nepoužívá se
Reset	lze provést skrze YubiKey Manager token bude potřeba znovu zaregistrovat u všech služeb neprovádět bez záložního tokenu, nebo dojde ke ztrátě přístupu k registrovaným službám automaticky vyresetuje i všechny FIDO2 zaregistrované služby
Nejznámější globální služby podporující U2F	Zobrazit aplikace
Postup registrace záložního tokenu	doporučeno ihned při registraci primárního tokenu, ale lze kdykoliv později bez omezení

Záložní token

Při koupi hlavního (primárního) YubiKey tokenu je dobré rovnou zakoupit minimálně jeden záložní token. Pokud uživatel primární token ztratí, neodřízne si přístup do svých služeb a následky pak nejsou fatální. Zcela ideální řešení jsou 2 záložní tokeny.

Následující tabulka pomůže majiteli YubiKey C Bio FIDO Edition tokenu zvolit vhodného kandidáta na záložní token s přihlédnutím k pořizovací ceně.

Primární token	Způsob použití	Vhodný záložní token
 YubiKey C Bio FIDO Edition	Lze využít libovolný konektor	 YubiKey 5 NFC
 YubiKey C Bio FIDO Edition	Musí být zachován konektor	 YubiKey 5C NFC

Bezpečnostní zásady

Primární YubiKey C Bio FIDO Edition token má uživatel neustále u sebe (např. připnutý na svazku klíčů), záložní token má uschovaný na bezpečném místě (např. v trezoru). V případě, že má uživatel více záložních tokenů, je dobré je umístit do geograficky odlišných lokalit. Pokud dojde ke ztrátě primárního tokenu, okamžitě si objedná nový token. Mezitím velmi obezřetně používá záložní token (toto je kritický, časově omezený okamžik pokud má uživatel pouze 1 záložní token). Jakmile obdrží nový token, opět si ho zaregistruje ve všech službách a vrací se do normálního režimu tj. primární token neustále u sebe, záložní token uložen na bezpečném místě.

Registrace tokenu

V závislosti na protokolu může být záložní token jako identická kopie primárního tokenu (např. pro generování OTP kódů), nebo jako zcela odlišný sekundární token spárovaný se službou. Ta pak ví, že konkrétní uživatel se může přihlašovat jedním z nich.

Obecně platí, že pokud se registrujeme do nové služby, spárujeme nebo nastavíme všechny tokeny najednou. Toto může být nepříjemné v případě, že záložní tokeny již máme uloženy v jiné lokalitě na bezpečném místě. Je to ale daň za bezpečnost.

Do aplikací, které podporují FIDO2 a U2F protokol, lze přidávat nové tokeny i kdykoliv později, je potřeba se standardně přihlásit do dané služby a obvykle v administraci uživatelského profilu bude možnost přidat nový token.

Bez záložního tokenu

Pokud si uživatel zaregistruje pouze jeden token (např. protože chce ušetřit) a ztratí ho, přijde pravděpodobně o přístup do služby. Pokud se jedná o burzu, kde má uloženy bitcoiny, může se toto šetření docela prodražit.

Pokud si uživatel zaregistruje pouze jeden token a nastaví si alternativní metodu přihlašování v případě ztráty tokenu, ušetří sice za záložní token, ale degraduje úroveň bezpečnosti celého systému na úroveň záložní metody. Např. pokud bude záložní metoda zadání tzv. **recovery kódu**, vystavuje se uživatel nebezpečí phishingu (útočník ho může přesvědčit, že jeho primární YubiKey nefunguje a vyláká z něj recovery kód).

Celková bezpečnost ověření je pouze tak silná, jak silný je její nejslabší článek.

Prvotní nastavení YubiKey C Bio FIDO Edition

Instalace nástrojů

Nainstalujeme si následující aplikace do počítače nebo notebooku:

- YubiKey Manager
- Yubico Authenticator (verze Desktop)

Nastavení k prvnímu použití

- Přidání otisků prstů v Yubico Authenticatoru

Doporučení

Senzor otisku prstů je potřeba vždy mačkat tak, aby se krajní část prstu dotkla stříbrného rámečku a bříško středu senzoru. Pokud máte suché ruce, použijte hydratační krém nebo vodu před použitím, poté prsty utřete a zkuste se dotknout. Pokud je senzor zaprášený nebo mastný, je potřeba ho nejprve vyčistit. Dvojice LED diod pak signalizuje stav tokenu:

- zeleně blikající LED potvrzuje správný stisk a otisk
- 3 rychlé žluté probliknutí znamenají, že se nepodařilo porovnat otisk
- opakované pomalé blikání žlutě signalizuje uzamknutou biometrii (pravděpodobně výsledek předchozích neúspěšných pokusů)

Nástroje pro YubiKey C Bio FIDO Edition

Yubico k tokenům dodává také software, který je potřeba pro některé scénáře. Všechny níže uvedené nástroje jsou zdarma a aktuální verze se dají stáhnout na příslušných stránkách výrobce. Pokud budete tyto programy využívat, vždy je udržujte aktuální.

YubiKey Manager

S YubiKey Managerem nakonfigurujete FIDO2, OTP a PIV funkcionalitu nebo například nastavíte PIN. Funguje na Windows, macOS, a Linuxu. Součástí je také ykman pro příkazovou řádku.

Přejít na domovskou stránku
Yubico Authenticator

Aplikace Yubico Authenticator (ať už mobilní nebo desktopová verze) umožní zobrazovat časově omezené jednorázové kódy (TOTP). Díky tomu lze YubiKey využít jako alternativu k mobilního telefonu a např. Google Authenticatoru.

Přejít na domovskou stránku
Developer Resources

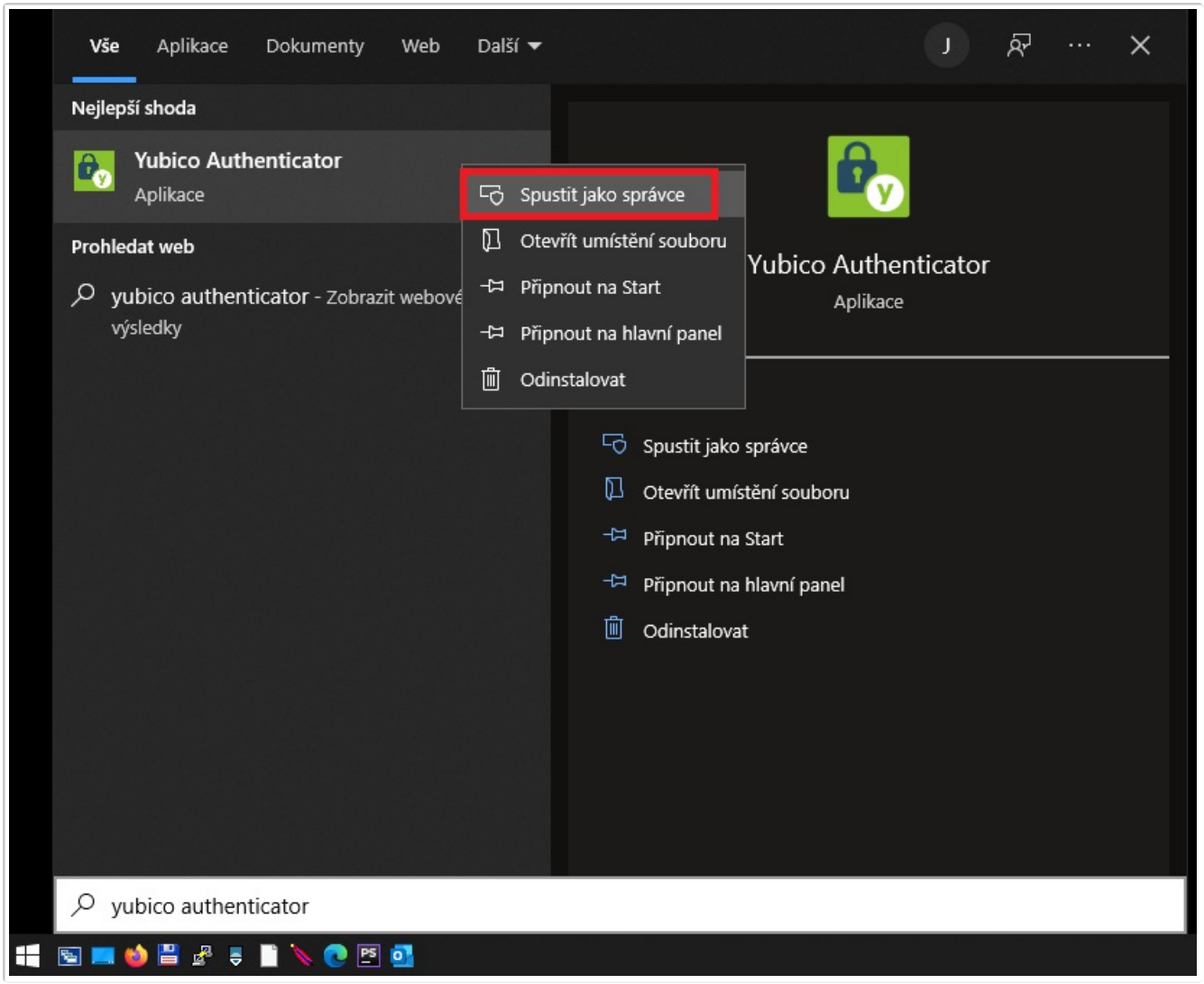
K dispozici jsou nejrůznější knihovny pro vývojáře, které usnadní integraci do vašich aplikací.

Přejít na domovskou stránku

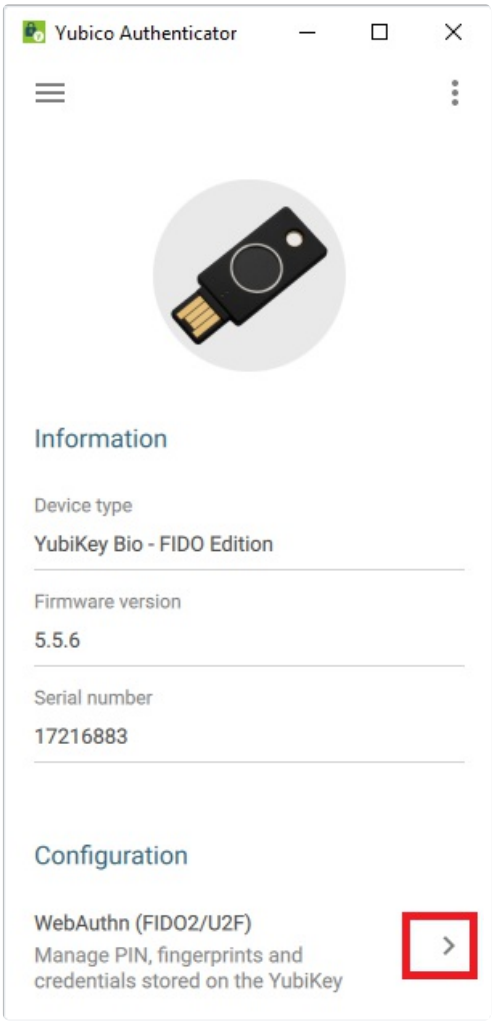
Návody pro YubiKey C Bio FIDO Edition

Přidání otisků prstů v Yubico Authenticatoru

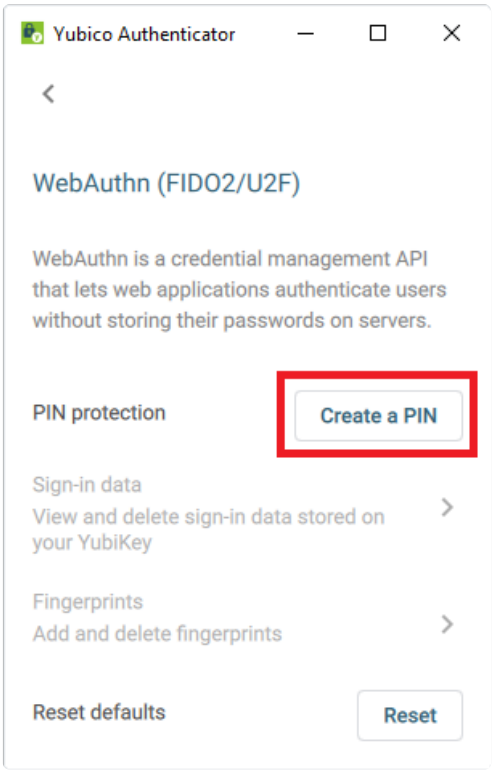
1. Spustíme Yubico Authenticator jako správce pomocí *Spustit jako správce*.



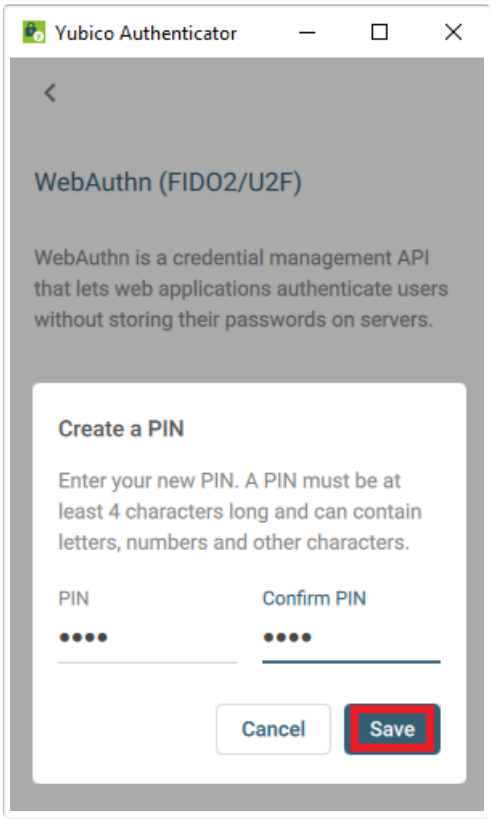
2. Vložíme YubiKey C Bio FIDO Edition do USB portu a klikneme na ikonku šipky u řádku *WebAuthn*.



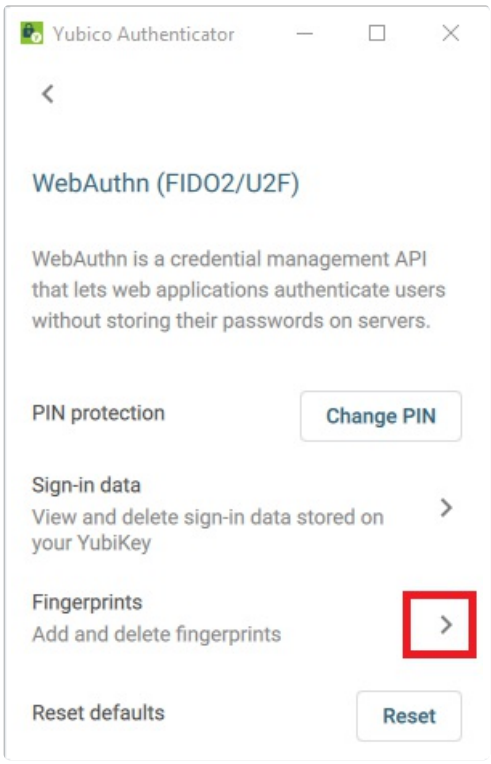
3. Pokud nemáme nastavený FIDO2 PIN, přejdeme k jeho nastavení pomocí *Create a PIN*.



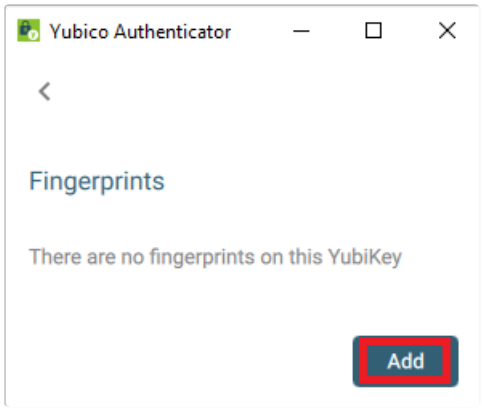
4. Nastavíme PIN do pole *PIN*, potvrdíme ho v poli *Confirm PIN* a uložíme kliknutím na tlačítko *Save*.



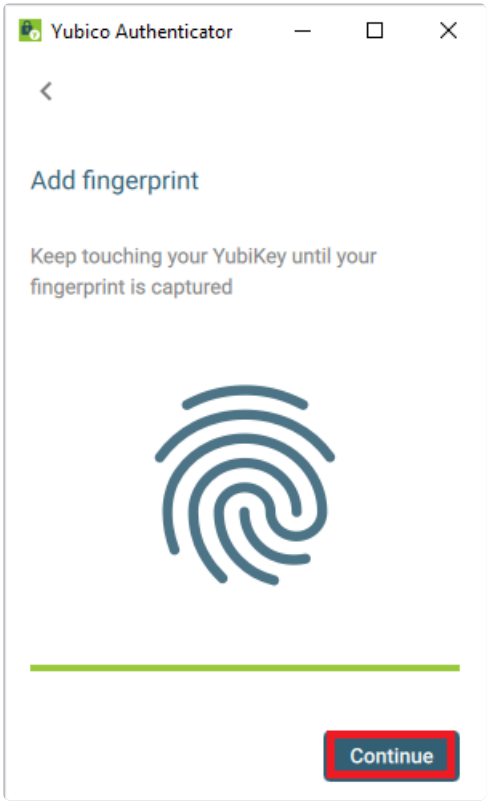
5. Nyní můžeme přejít k administraci otisků.



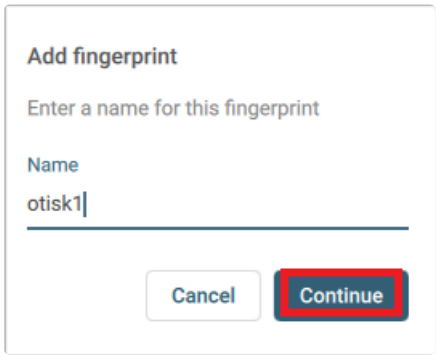
6. Aplikace hlásí, že zatím není uložený ani jeden otisk. Tlačítkem *Add* přejdeme k přidání prvního otisku.



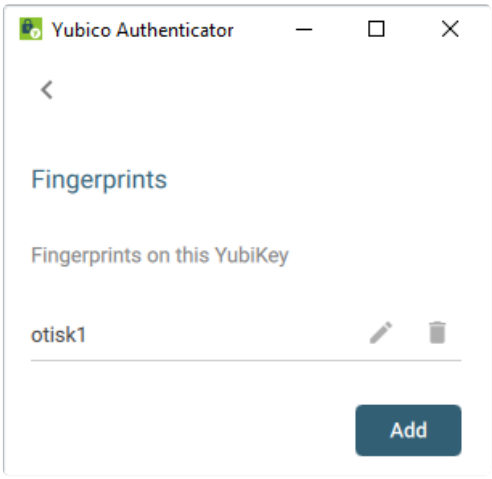
7. Objeví se symbol otisku prstu a LED dioda tokenu bliká rychle zeleně. Vybereme si prst, jehož otisk chceme přidat. Tímto prstem se opakovaně dotýkáme středu senzoru tak, aby se prst zároveň dotýkal i stříbrného rámečku kolem senzoru. Aplikace znázorňuje postup načítání na světle zelené čáře pod symbolem otisku. Jakmile senzor nasnímá dostatek informací, LED dioda přestane blikat, plná čára se zbarví tmavě zeleně. Tlačítkem *Continue* vše potvrdíme.



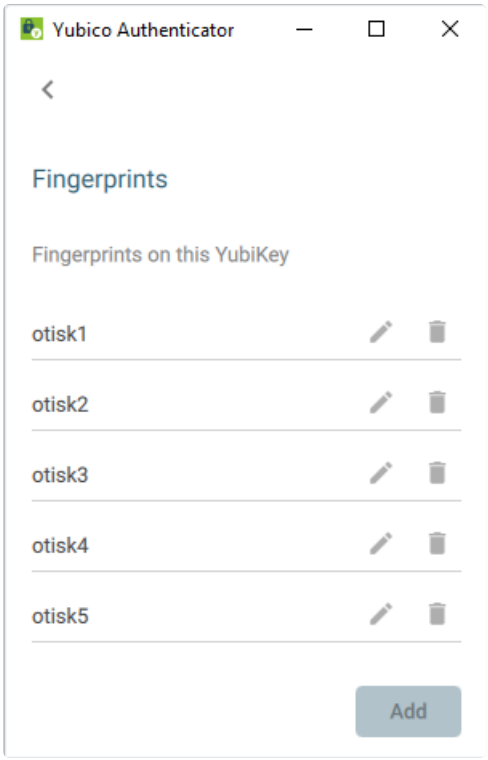
8. Otisk si pojmenujeme (1-15 znaků) a potvrdíme tlačítkem *Continue*.



9. Otisk se zobrazí v přehledové nabídce. Token nemá uložený přímo otisk, ale jednosměrně zašifrovanou informaci o křivkách otisku. To znamená, že neexistuje způsob, jak z této informace zrekonstruovat původní otisk. Pokud token porovnává otisk, vždy nasnímá křivky, zašifruje a poté porovnává výsledek s uloženou hodnotou. Pokud dojde ke shodě, vyhodnotí to jako správný otisk.

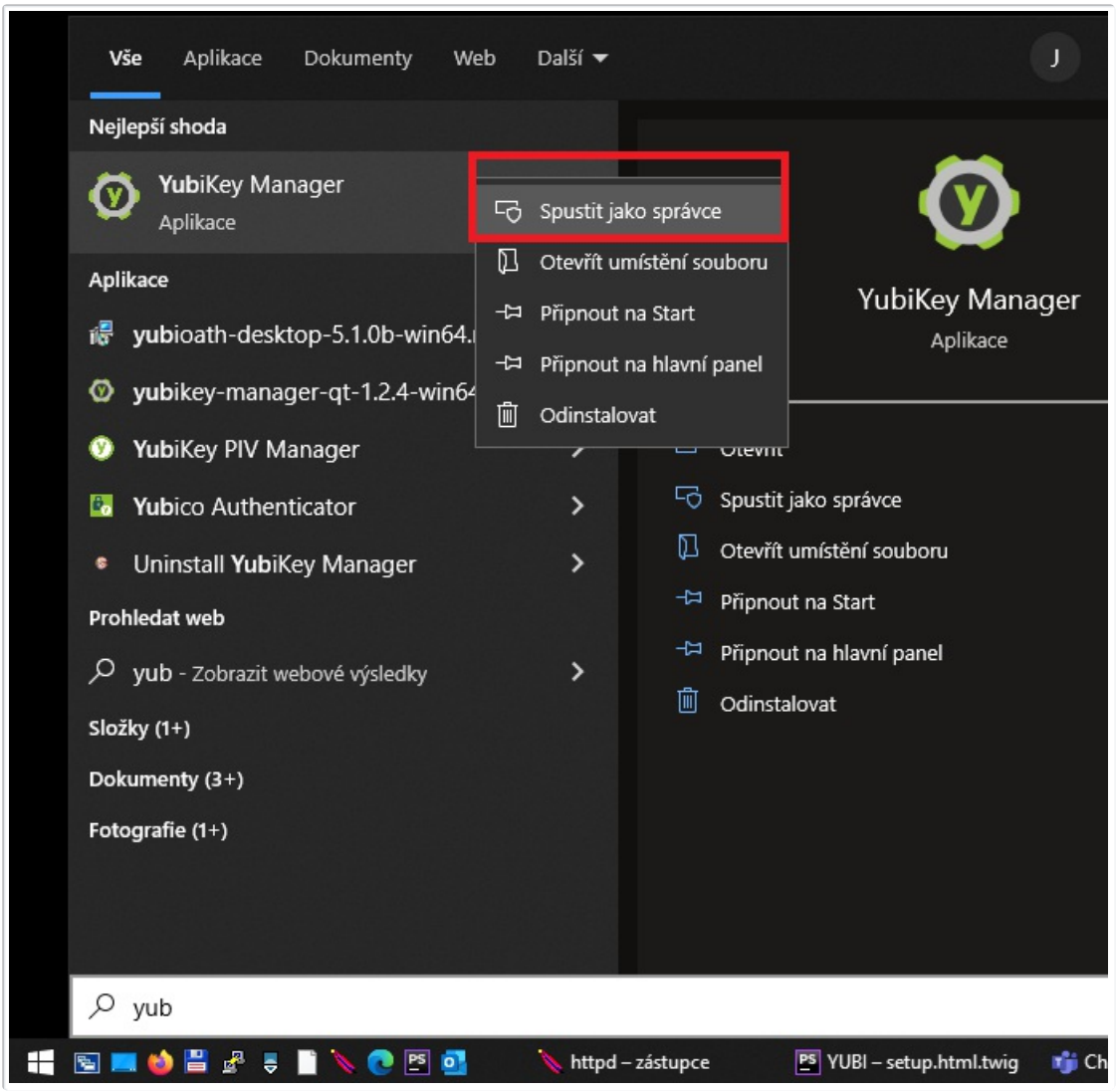


10. Takto lze přidat celkem 5 otisků. Každý otisk lze kdykoliv přejmenovat nebo vymazat pomocí ikonek v řádku daného otisku.

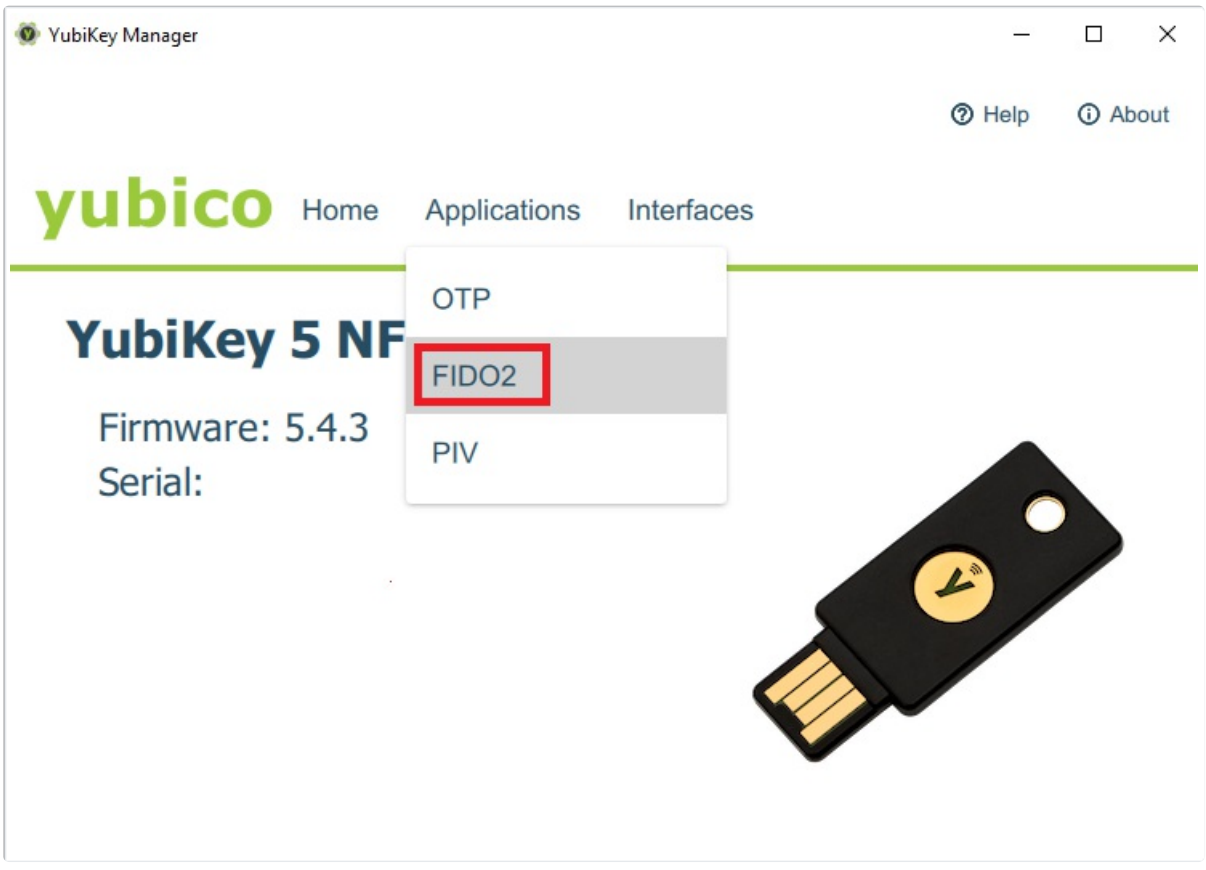


Nastavení FIDO2 PINu v YubiKey Manageru

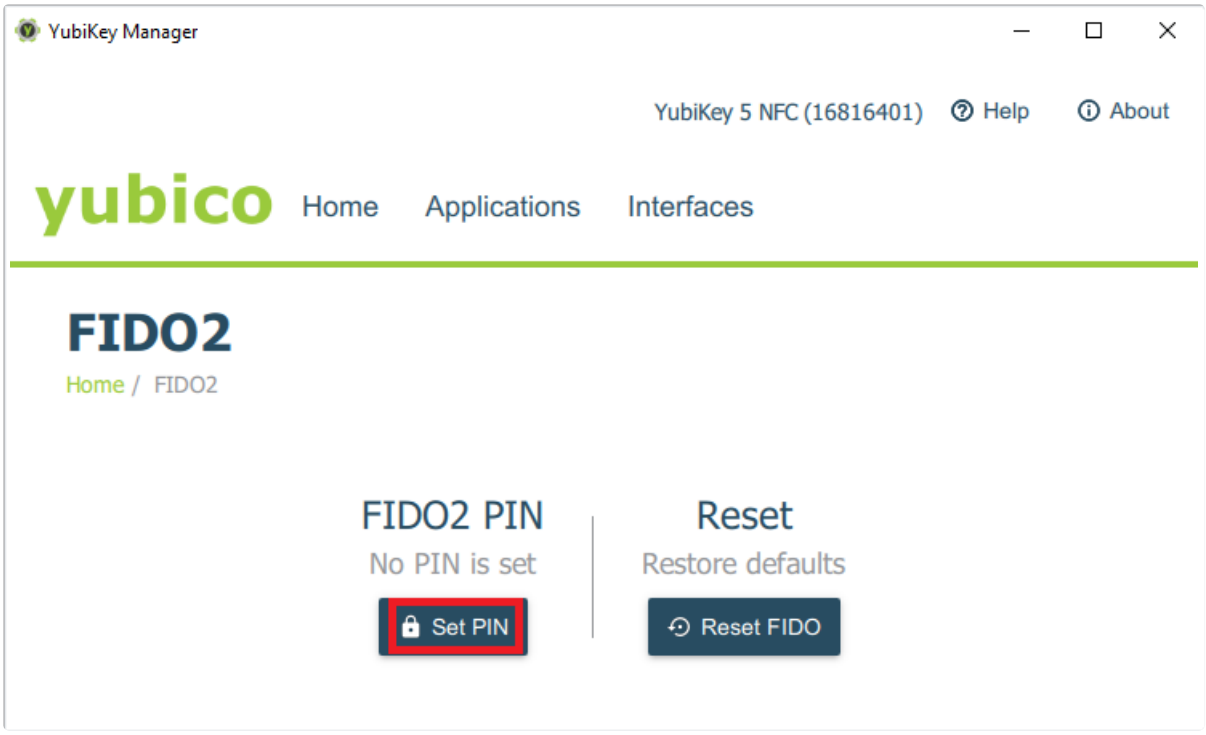
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



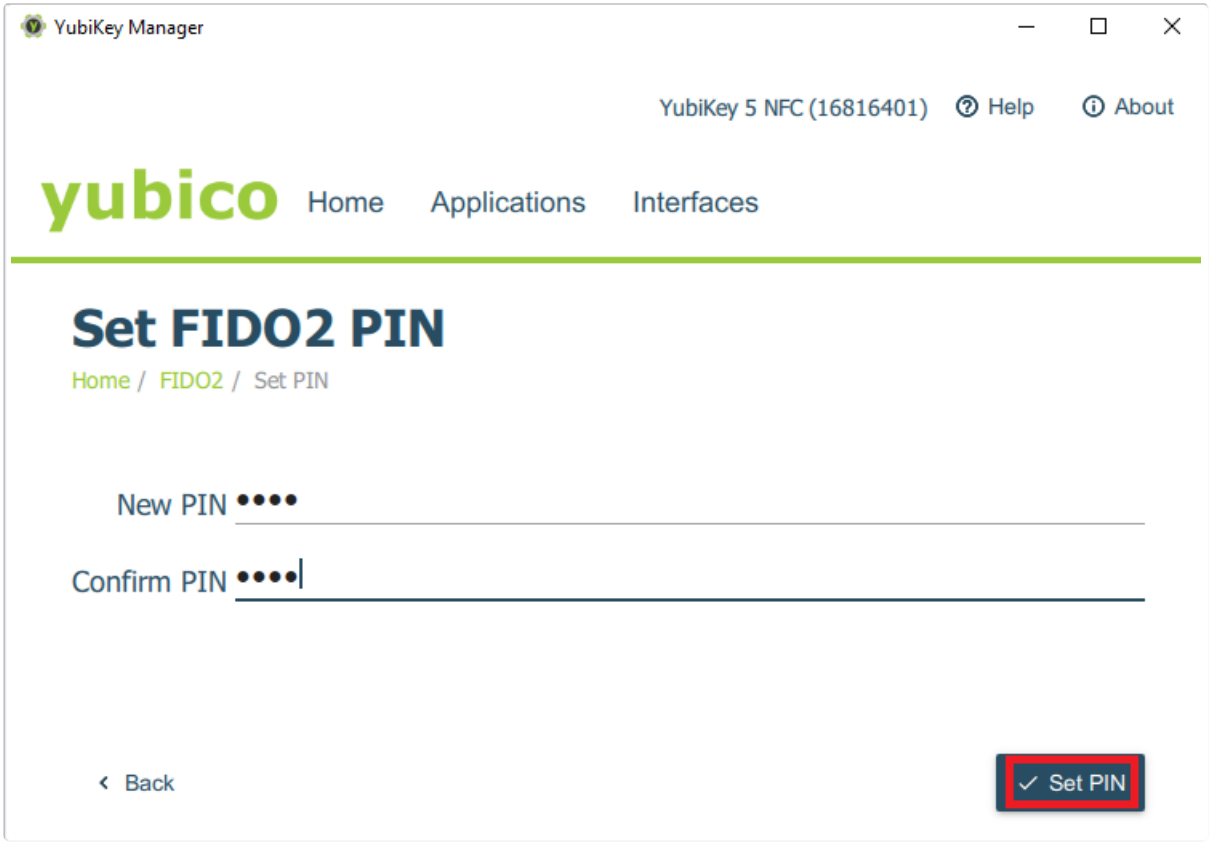
2. Zvolíme volbu *FIDO2*.



3. Klikneme na *Set PIN*.



4. Zvolíme si alfanumerický PIN (minimálně 4 znaky) v poli *New PIN*, potvrdíme jej v poli *Confirm PIN* a uložíme pomocí tlačítka *Set PIN*.



Často kladené dotazy

Lze na token uložit kvalifikovaný certifikát?

Nikoliv.

Lze tokeny YubiKey využít jako správce hesel (tzv. password manager)?

Nikoliv, ale některé správce hesel podporují FIDO2/U2F dvoufaktorové přihlašování a pomocí YubiKey C Bio FIDO Edition lze zabezpečit přihlašování.

Lze na token uložit soubory?

Nikoliv, YubiKey C Bio FIDO Edition není flash disk.

Lze na token uložit nějaké kryptoměny?

Nikoliv, YubiKey C Bio FIDO Edition není kryptopeněženka. Pomocí YubiKey C Bio FIDO Edition lze ale zabezpečit přihlašování do kryptoměnových burz, které podporují FIDO2/U2F dvoufaktorové přihlašování.

YubiKey Manager nerozpoznává můj nový token, proč?

Spouštíte YubiKey Manager aplikaci jako správce? Používáte nejnovější verzi YubiKey Manager? Pro nově vydané tokeny je potřeba i novější verze YubiKey Manageru.

YubiKey C Bio FIDO Edition jsem připojil(a) k zařízení, které mám připojené k PC a disponuje také USB portem. YubiKey C Bio FIDO Edition ale nefunguje jak má.

Připojte YubiKey C Bio FIDO Edition token přímo do USB portu vašeho počítače.

YubiKey se načte v Yubico Authenticatoru/YubiKey Manageru, ale nefunguje správně.

Nemáte najednou spuštený Yubico Authenticator a YubiKey Manageru? Zavřete jednu z aplikací.