YubiKey 5 Nano uživatelský manuál

verze 1.00

Miniaturní bezpečnostní token s USB-A rozhraním, podporou protokolů FIDO2 (bezheslové ověřování), OTP, PIV (Smart Card) a OpenPGP, pomocí kterého maximálně zabezpečíte váš e-mail, sociální sítě, kryptoburzu nebo přístup do počítače, pouhým dotykem prstu zcela eliminujete hrozbu phishingu. Lze trvale ponechat v USB portu počítače.

Popis YubiKey 5 Nano

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 potvrzuje stiskem tlačítka na tokenu

Silný multi-faktor

Uživatel zadává jméno a heslo, poté odemyká token PINem a potvrzuje stiskem jeho tlačítka

Bezheslové ověřování

Uživatel bez zadání přihlašovacích údajů rovnou odemyká token PINem, potvrzuje stiskem jeho tlačítka

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.

Další funkce YubiKey tokenů

- Zabezpečení přihlašování k počítačům, notebookům, tabletům a serverům
- Zabezpečení přihlašování do VPN a vzdálené ploše
- Uchovávání privátních klíčů pro šifrování, dešifrování a podepisování dokumentů
- Fyzický přístup do budovy, kde YubiKey nahradí vstupní kartu
- Snadno nasaditelné řešení pro firmy, které se výrazně sníží náklady na provoz a zjednoduší se procesy spojené s přihlašováním uživatelů jako například obnovení hesla, registrace nových uživatelů nebo rozlišování úrovně přístupů pro jednotlivé zaměstnance

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.

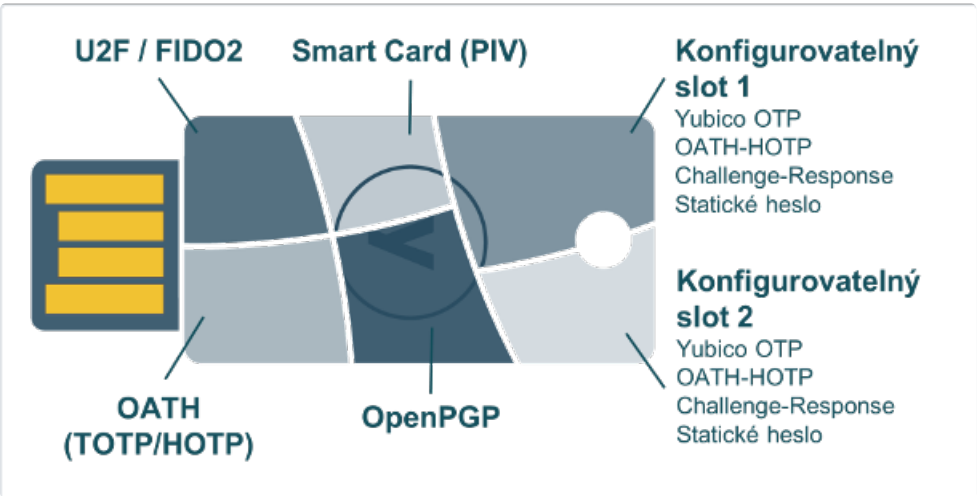
Princip potvrzování

YubiKey 5 Nano disponuje metalickým tlačítkem, které uživatel stiskne a tím potvrdí prováděnou operaci (nemusí být vždy vyžadováno). Token rozlišuje mezi dlouhým a krátkým stisknutím. Tlačítko je čistě mechanické, otisk prstu se nesnímá. Vedle stisku tlačítka uživatel zadává i číselný PIN, pokud je to potřeba (analogie je platební karta při výběru z bankomatu).

Technické parametry

Základní parametry	
Název produktu	YubiKey 5 Nano
Rozhraní	USB 2.0 (USB-A)
Princip potvrzování	Mechanický dotek tlačítka
Funkcionalita	
Autentizační metody	Passwordless, Strong Two Factor, Strong Multi-Factor
Funkce	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F), Smart card (PIV-compatible), Yubico OTP, OATH – HOTP (Event), OATH – TOTP (Time), Open PGP, Secure Static Password
Certifikace	FIDO 2 Certified, FIDO Universal 2nd Factor (U2F) Certified
Kryptografie	RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384
Typ zařízení	FIDO HID Device, CCID Smart Card, HID Keyboard
Technické vlastnosti	
Stupeň krytí	IP68
Odolnost	neobsahuje baterie, neobsahuje pohyblivé částice, vysoká mechanická odolnost, voděodolnost
Barva	černá
Rozměry	12mm x 13mm x 3.1mm
Hmotnost	1g
Pracovní teplota	0°C - 40°C
Skladovací teplota	-20°C - 85°C
Rozměry obalu	55mm x 85mm x 5mm
Hmotnost včetně obalu	4g
Obsah balení	1 token
Další informace	
EAN	5060408461457
Země původu	Made in USA & Sweden
Výrobce	Yubico
Záruka	24 měsíců
Odkazy	
"YubiKey 5" Technický manuál výrobce (anglicky)	

Funkce



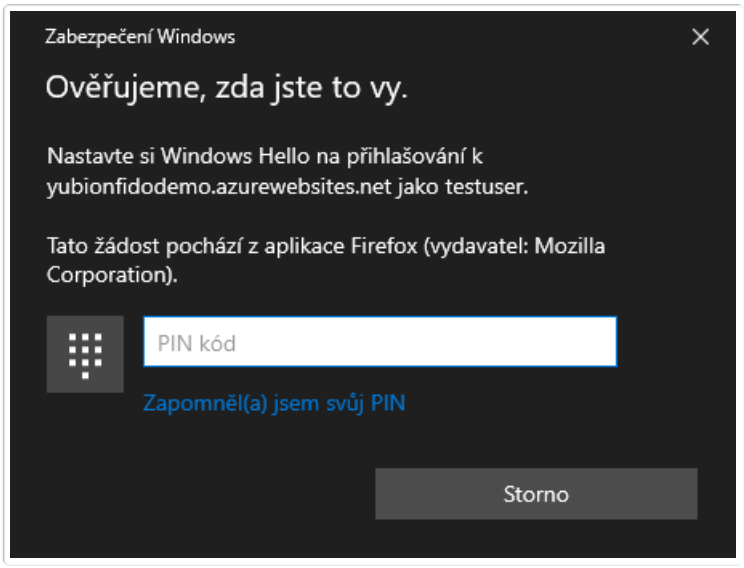
YubiKey 5 Nano disponuje šesti oddělenými funkčními moduly. Každý modul poskytuje jinou funkcionalitu. S počítačem, tabletem nebo telefonem tyto moduly komunikují skrze 3 rozhraní:

- **OTP** rozhraní se v počítači hlásí jako obyčejná USB klávesnice (HID neboli Human Interface Device). Zaslaná data tokenem do počítače jsou pak simulací stisků kláves na virtuální klávesnici. Z tohoto důvodu není potřeba instalovat žádné speciální ovladače, podpora je napříč platformami.
- **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)
- **CCID** rozhraní umí YubiKey proměnit ve čtečku smartkaret a aplikace na tokenu se poté hlásí jako jednotlivé smartkarty. Podpora je na Windows (s minidriverem) a MacOS, na Linuxu (s PC/SC) a Androidu. Na iOS je potřeba Yubico iOS SDK.

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.

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**.



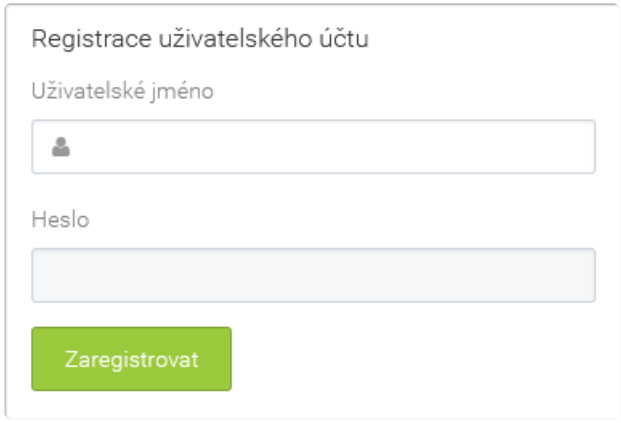
Tradiční 2FA

Klasické přihlašování s heslem, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto

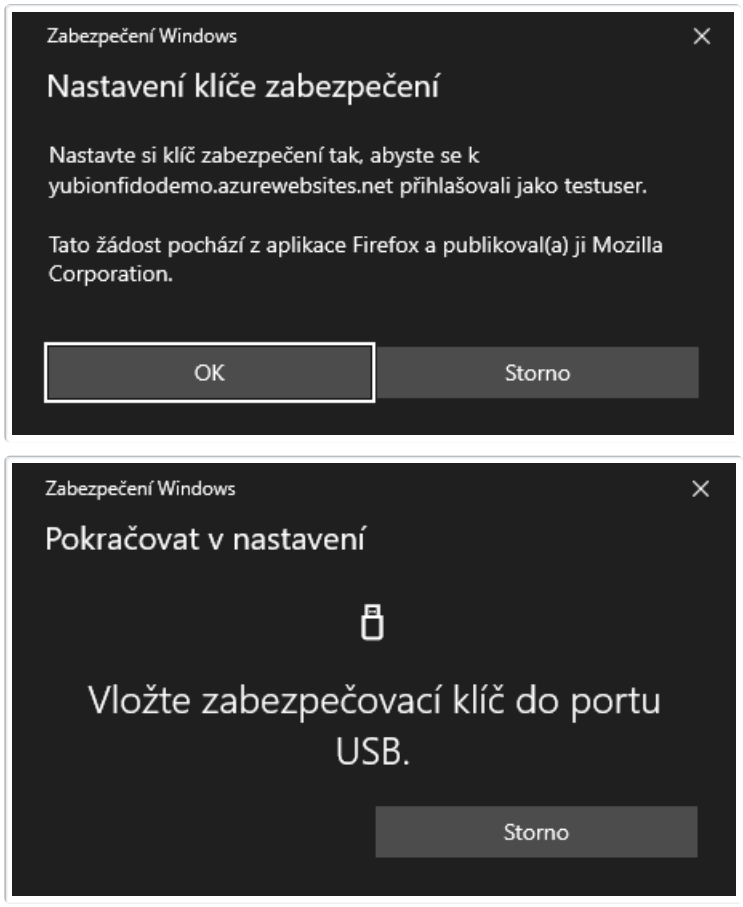
scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě).

Fáze registrace

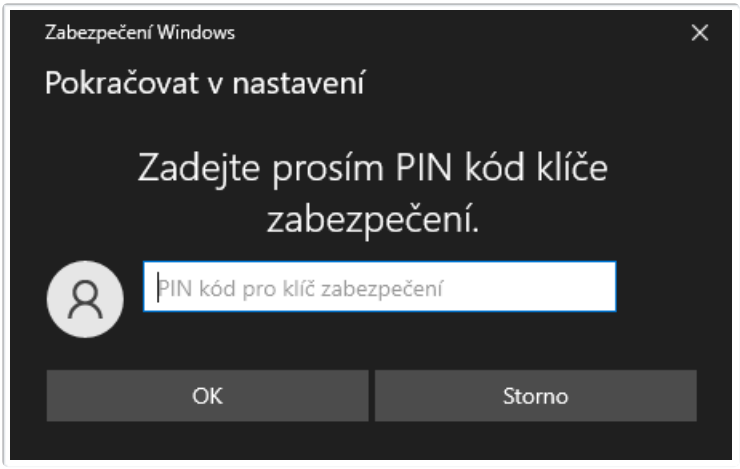
1. Uživatel zvolí uživatelské jméno a heslo



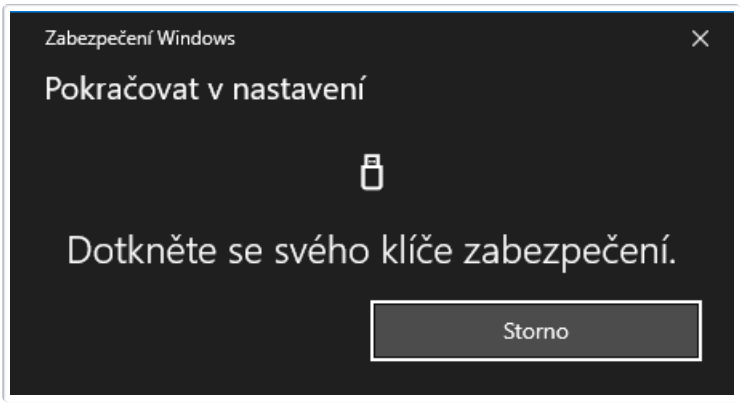
2. Uživatel je vyzván, aby připojil YubiKey



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

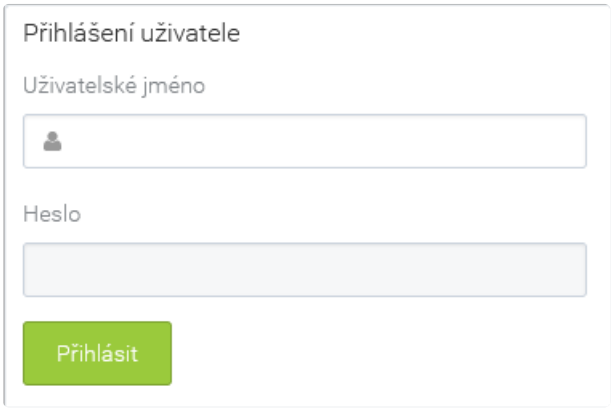


4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey

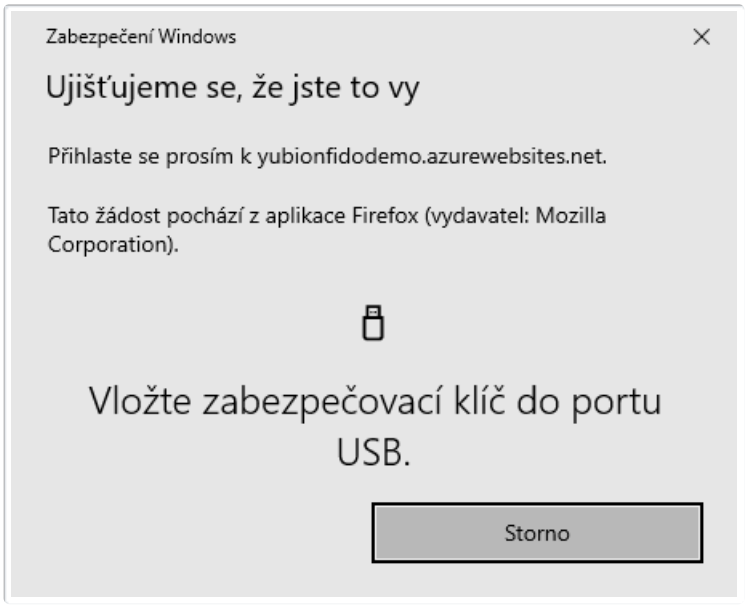


Fáze přihlášení

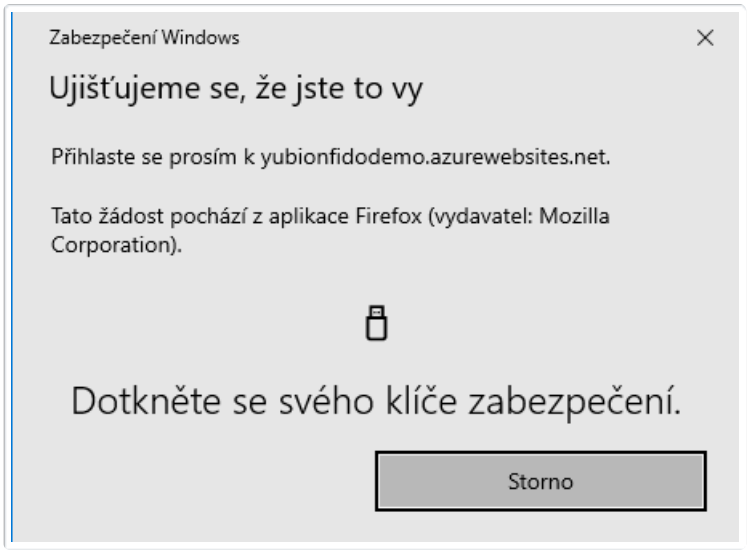
1. Uživatel zadá uživatelské jméno a heslo



2. Uživatel je vyzván, aby připojil YubiKey



3. Uživatel dokončí přihlašování stisknutím tlačítka na YubiKey

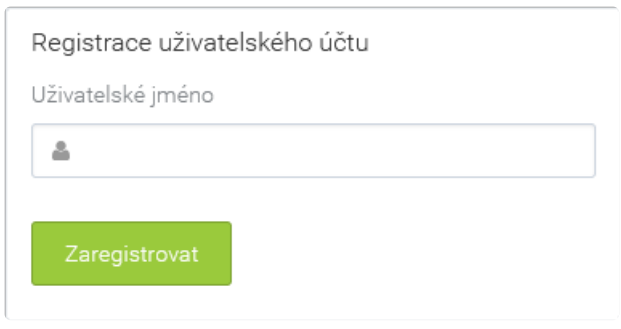


Bezheslové (passwordless) přihlášení s uživatelským jménem

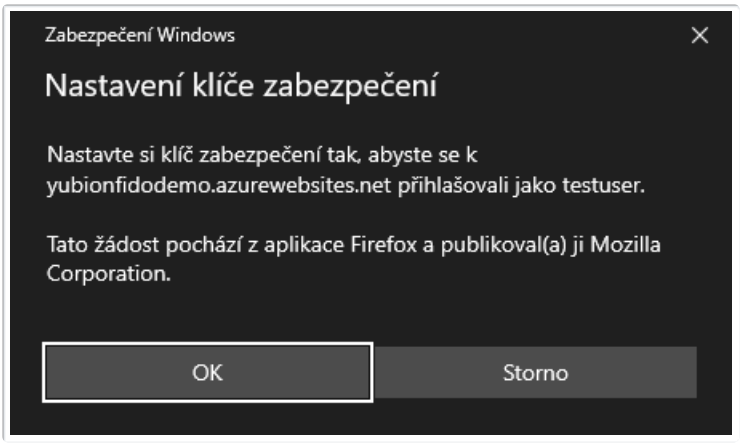
Bezheslové přihlašování s uživatelským jménem, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě)

Fáze registrace

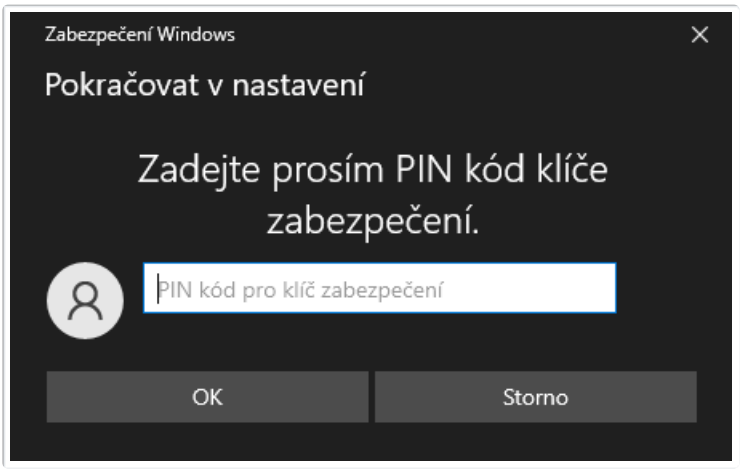
1. Uživatel zvolí uživatelské jméno



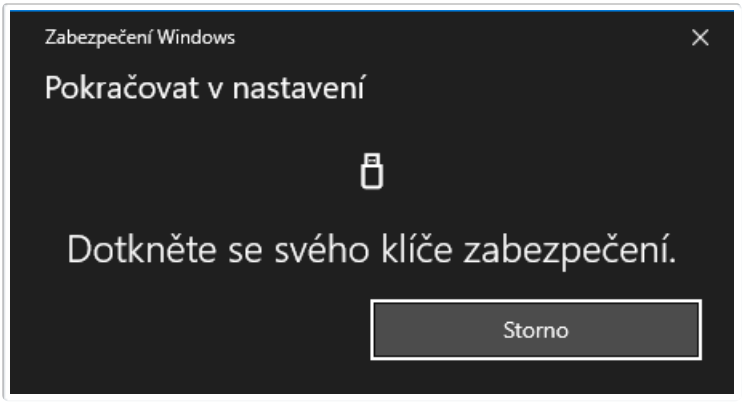
2. Uživatel je vyzván, aby připojil YubiKey



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



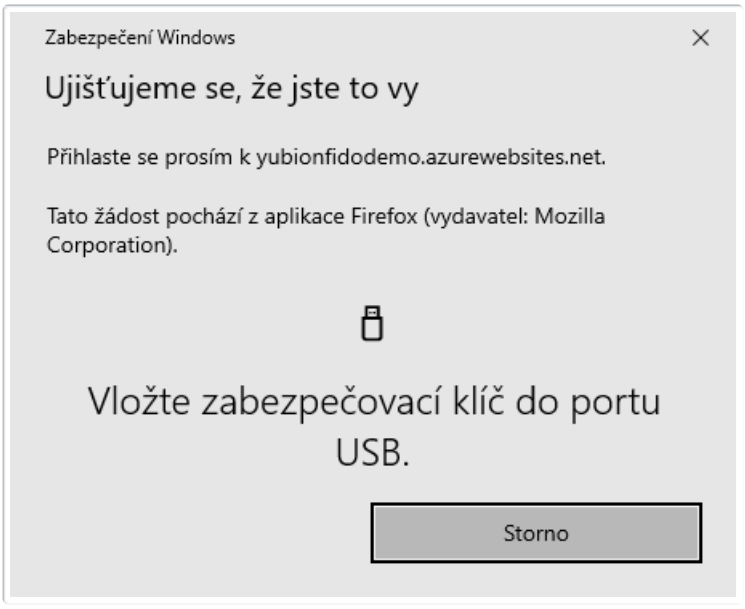
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



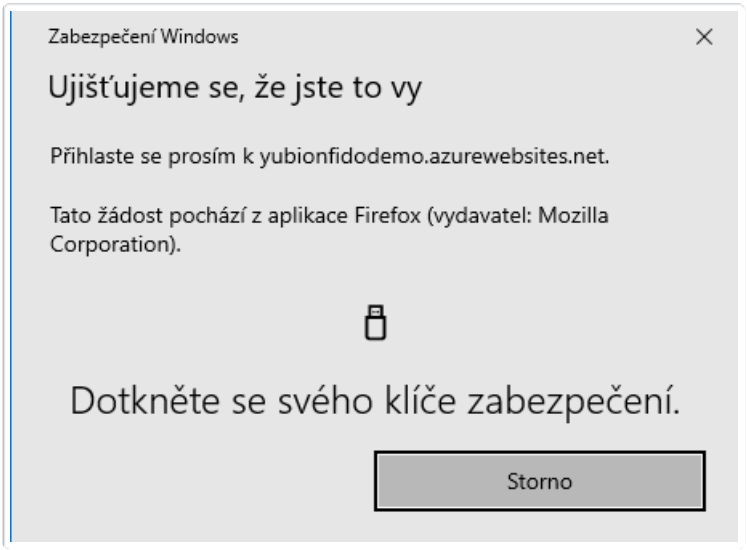
Fáze přihlášení

1. Uživatel zadá uživatelské jméno

2. Uživatel je vyzván, aby připojil YubiKey



3. Uživatel dokončí přihlašování stisknutím tlačítka na YubiKey

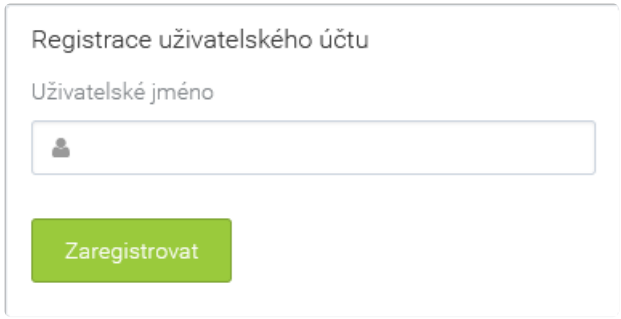


Bezheslové (passwordless) přihlášení bez uživatelského jména

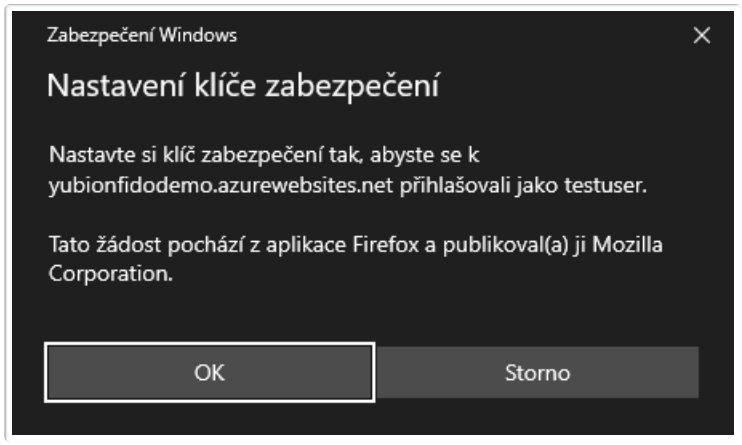
Bezheslové přihlašování bez uživatelského jména, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto scénářem je omezen kapacitou tokenu na 25 (v tokenu se ukládá uživatelské jméno a obecné informace ke službě).

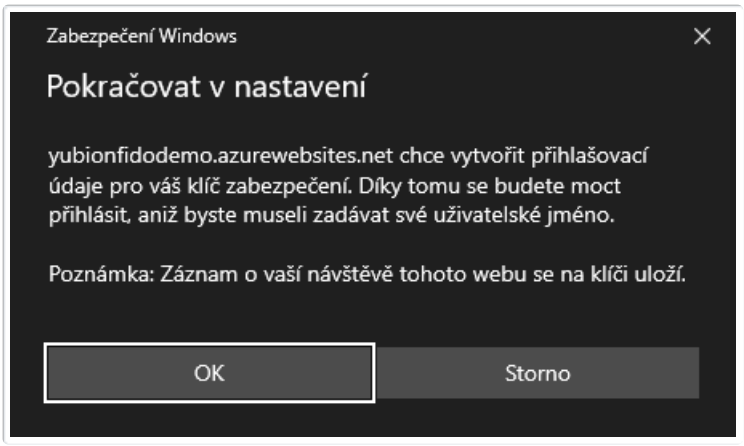
Fáze registrace

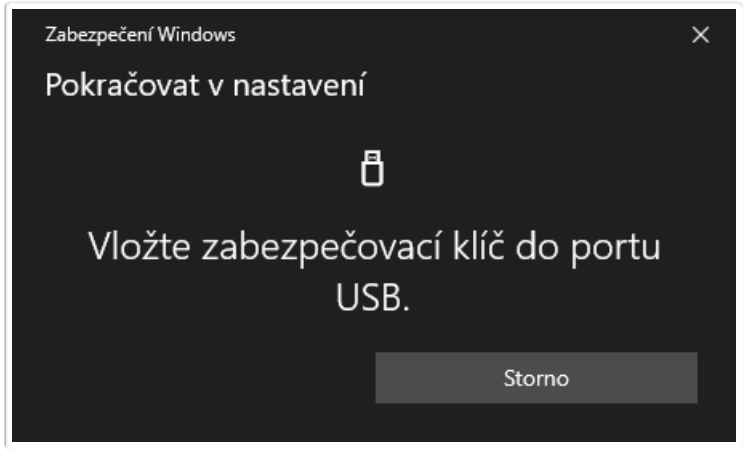
1. Uživatel zvolí uživatelské jméno



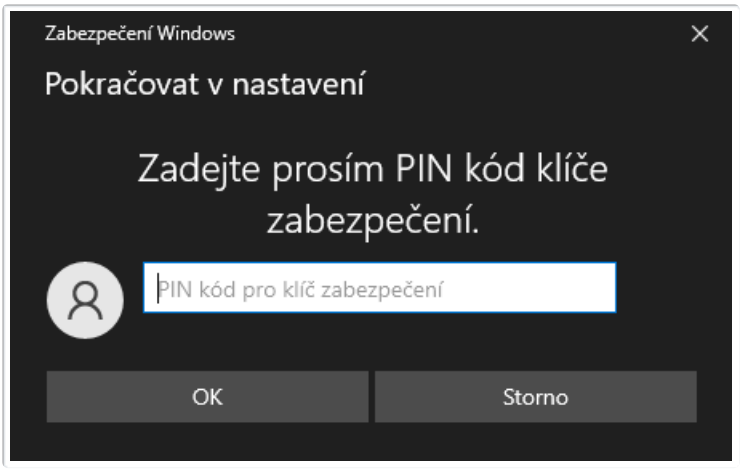
2. Uživatel je vyzván, aby připojil YubiKey



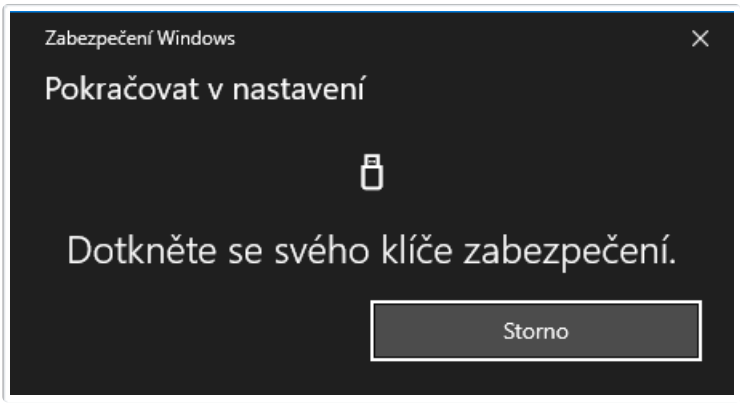




3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání (jinak se tento krok přeskočí)



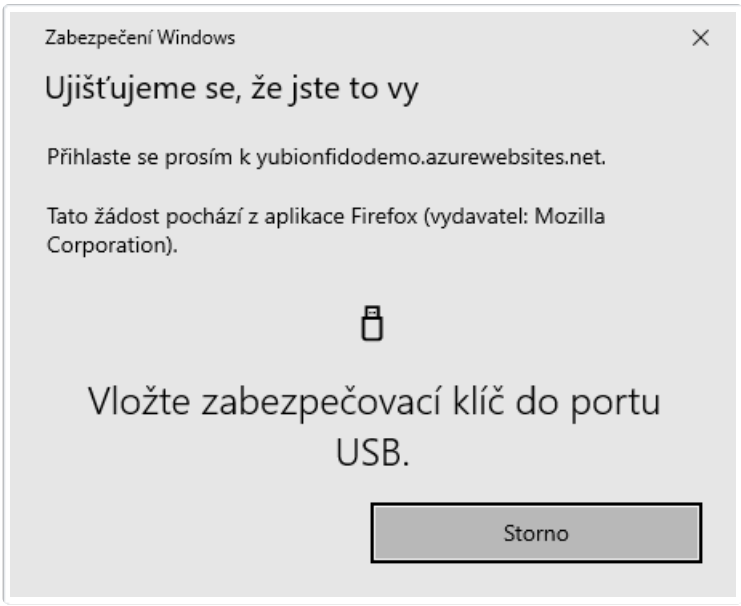
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



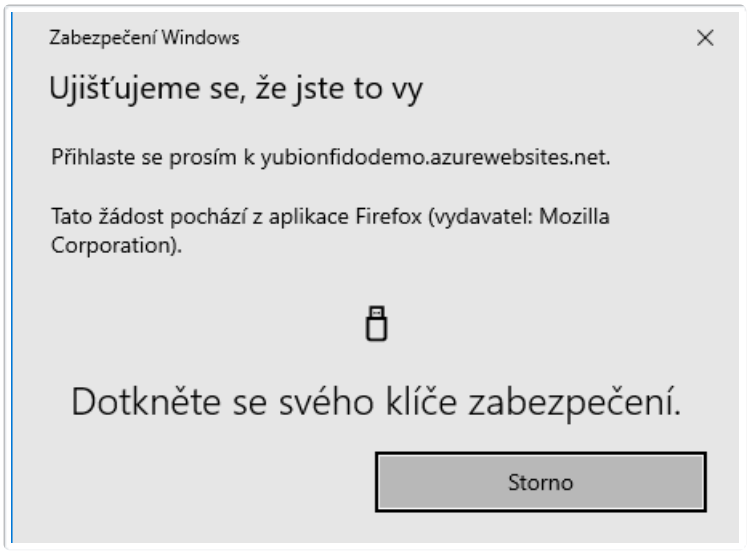
Fáze přihlášení

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

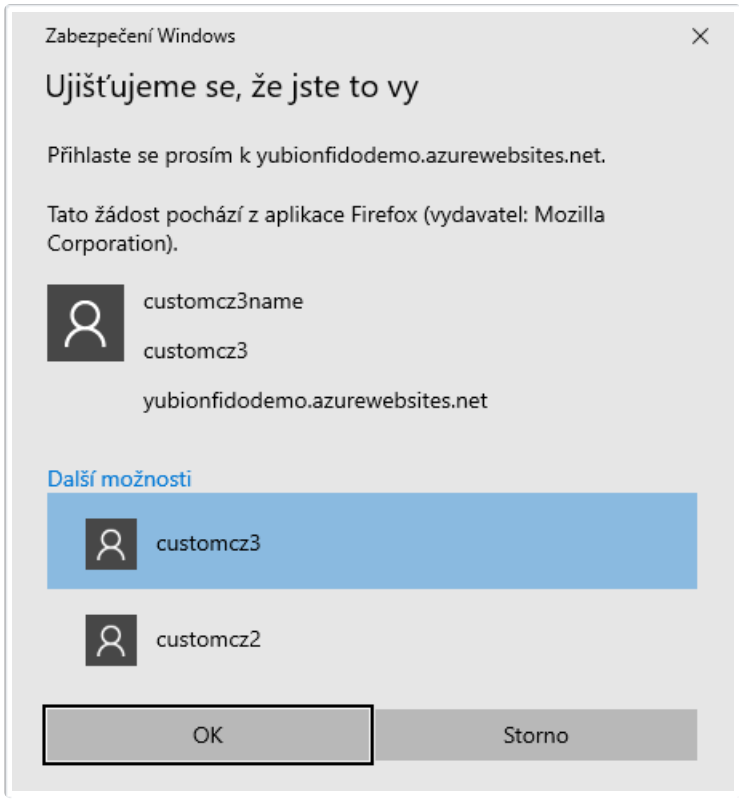
2. Uživatel je vyzván, aby připojil YubiKey



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)

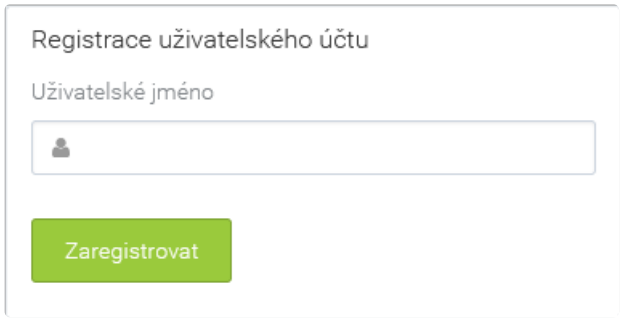


MFA bezheslové (passwordless) přihlášení s uživatelským jménem

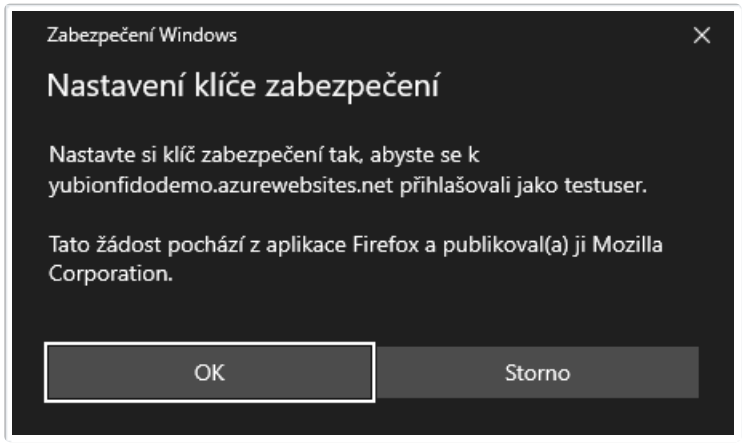
Bezheslové přihlašování s uživatelským jménem, kdy token slouží jako multi-faktor k ověření (zadává se i PIN). Lze vyzkoušet demo. Počet spárovaných služeb využívající token tímto scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě).

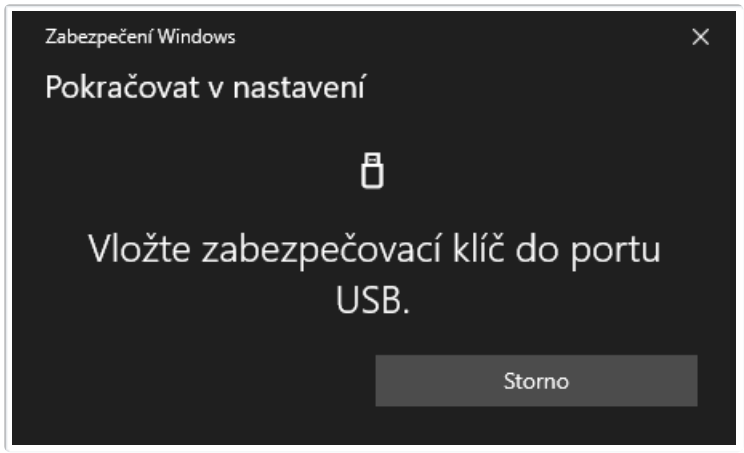
Fáze registrace

1. Uživatel zvolí uživatelské jméno

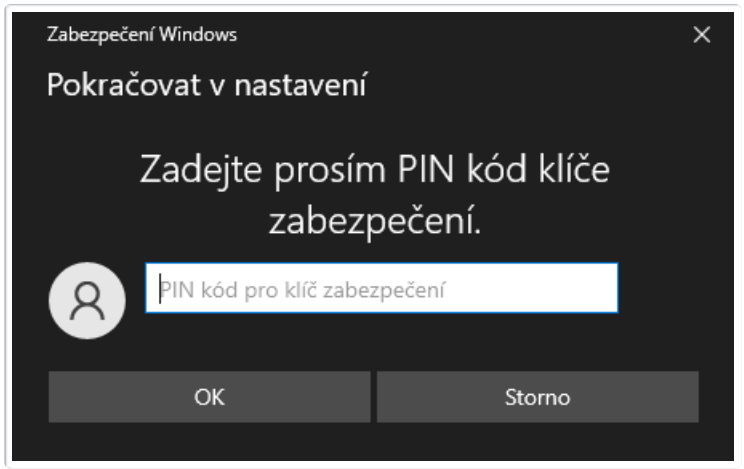


2. Uživatel je vyzván, aby připojil YubiKey

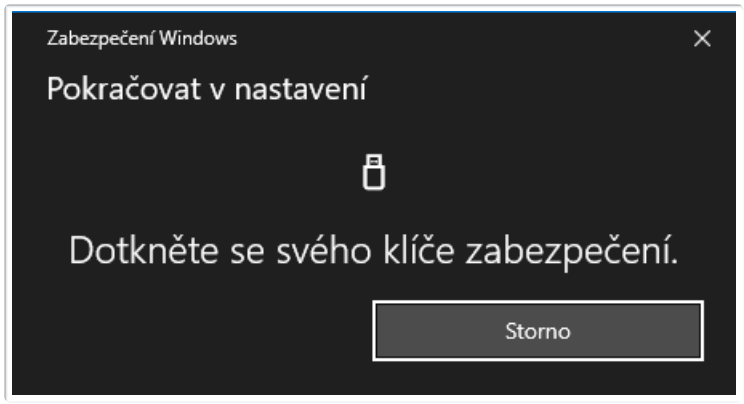




3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání, pokud nikoliv, je vyzván k jeho vytvoření (včetně dodatečného stisku YubiKey tlačítka)



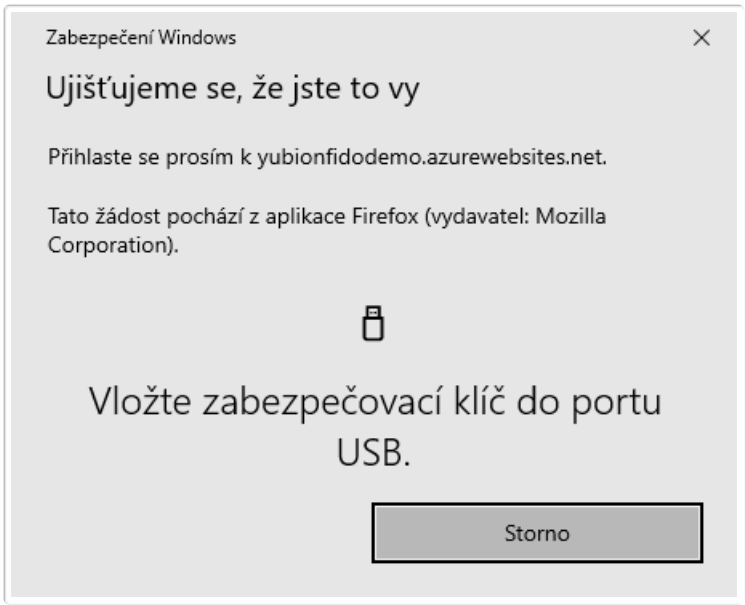
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



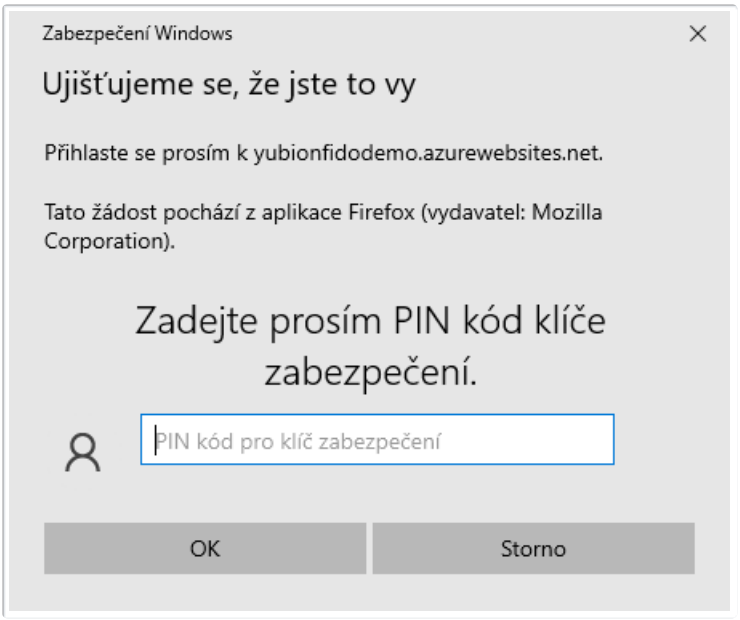
Fáze přihlášení

1. Uživatel zadá uživatelské jméno

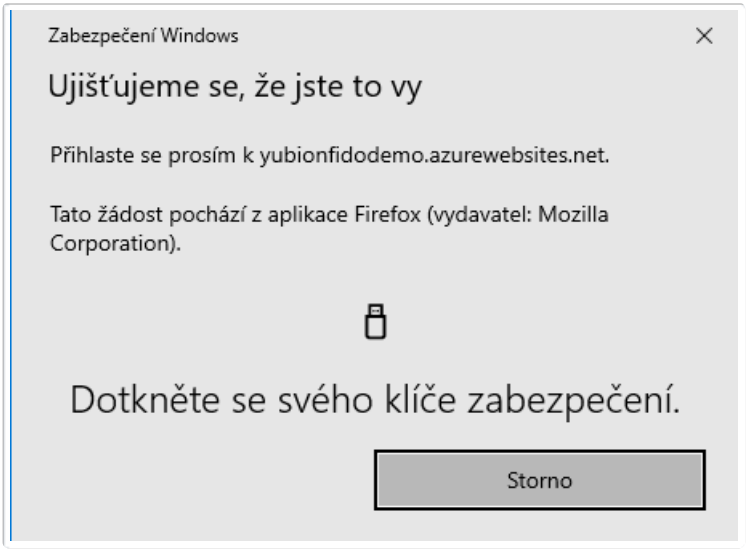
2. Uživatel je vyzván, aby připojil YubiKey



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



4. Uživatel potvrdí přihlašování stisknutím tlačítka na YubiKey

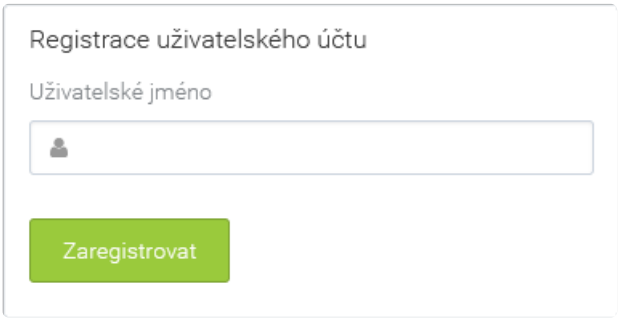


MFA bezheslové (passwordless) přihlášení bez uživatelského jména

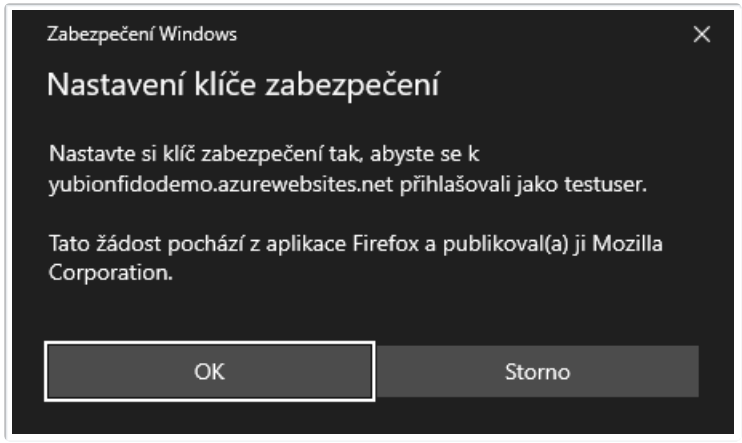
Bezheslové přihlašování bez uživatelského jména, kdy token slouží jako multi-faktor k ověření (zadává se i PIN). Lze vyzkoušet demo (zaškrtnout u registrace *requireResidentKey* a zvolit *userVerification: required* u registrace i autentizace). Počet spárovaných služeb využívající token tímto scénářem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

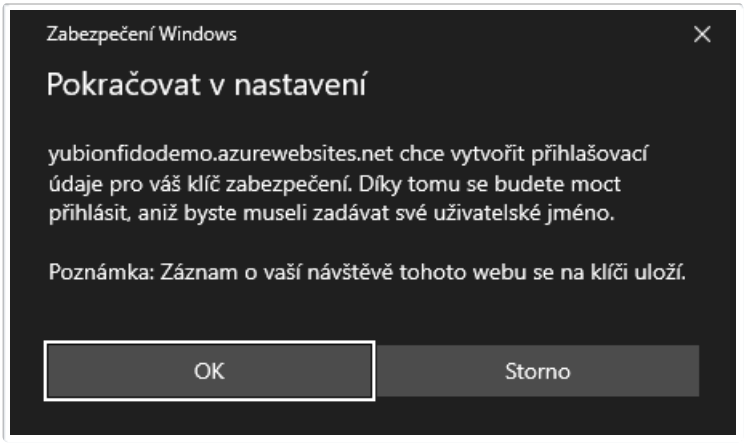
Fáze registrace

1. Uživatel zvolí uživatelské jméno

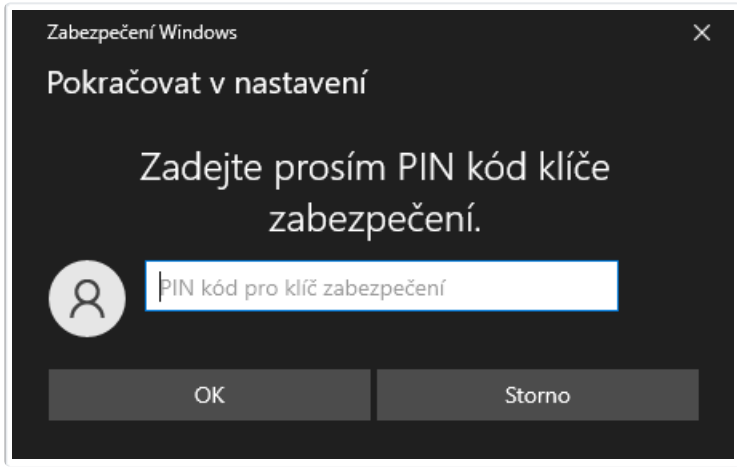


2. Uživatel je vyzván, aby připojil YubiKey

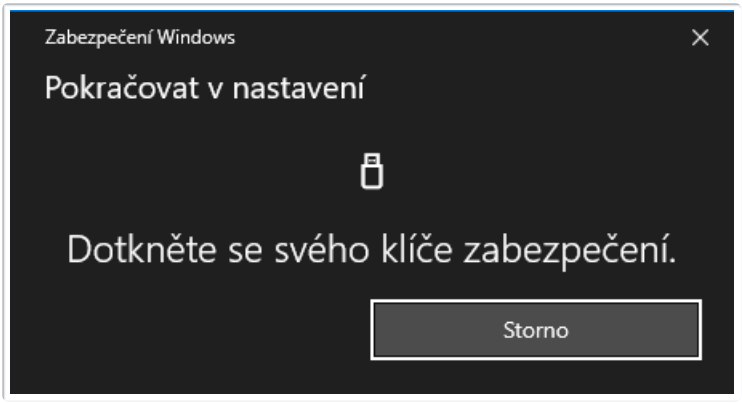




3. Pokud má YubiKey nastavený PIN, je uživatel vyzván k jeho zadání, pokud nikoliv, je vyzván k jeho vytvoření (včetně dodatečného stisku YubiKey tlačítka)



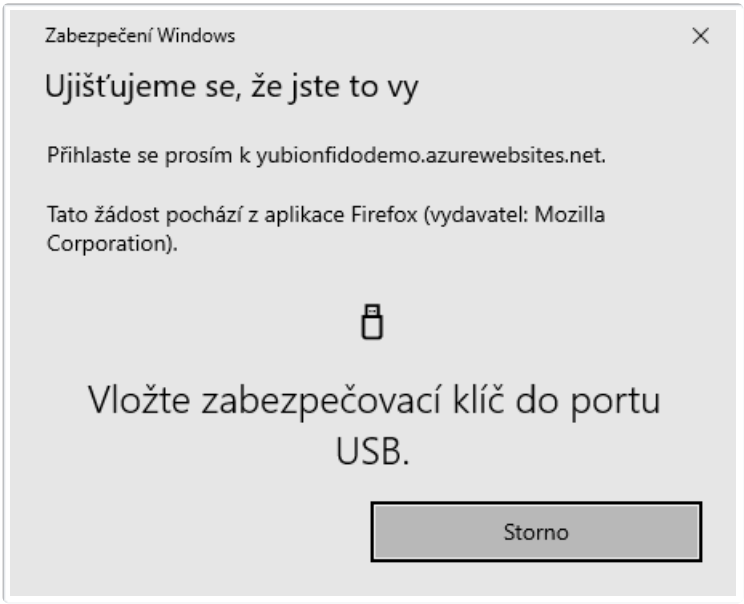
4. Uživatel dokončí registraci stisknutím tlačítka na YubiKey



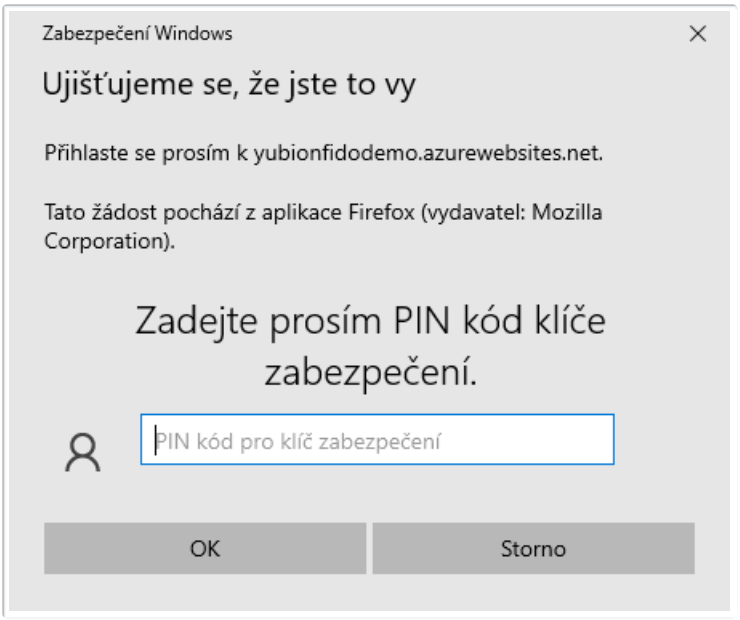
Fáze přihlášení

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

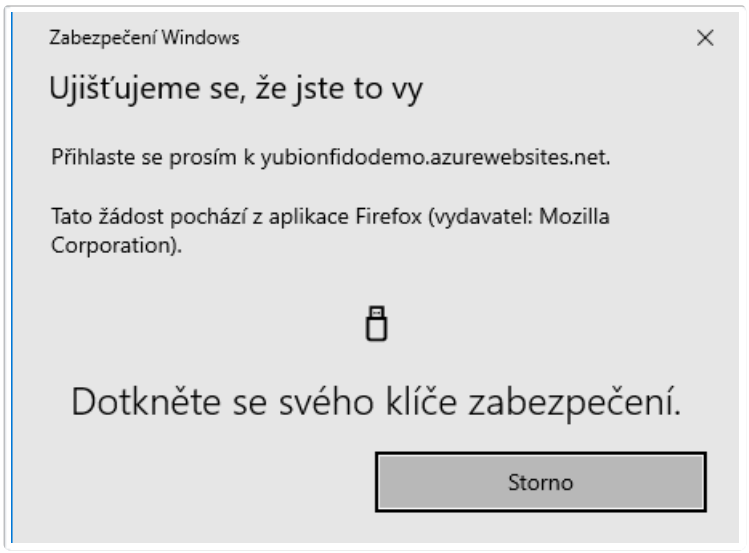
2. Uživatel je vyzván, aby připojil YubiKey



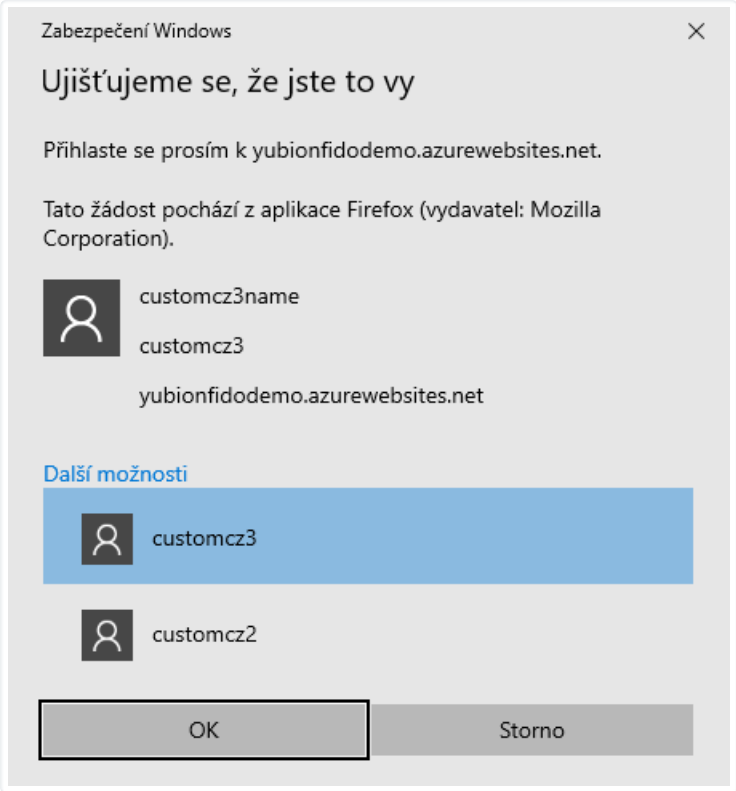
3. Uživatel je vyzván, aby zadal PIN kód k YubiKey



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.

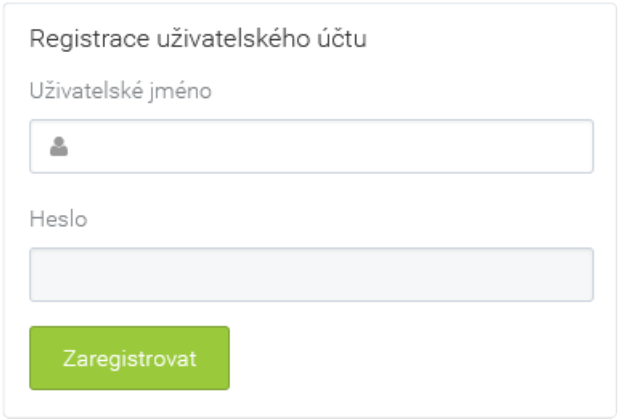
U2F proces se stejně jako u FIDO2 rozděluje na dvě fáze, registrační a přihlašovací. Narozdíl od FIDO2 není tak variabilní a nepoužívá vůbec PIN.

Tradiční 2FA

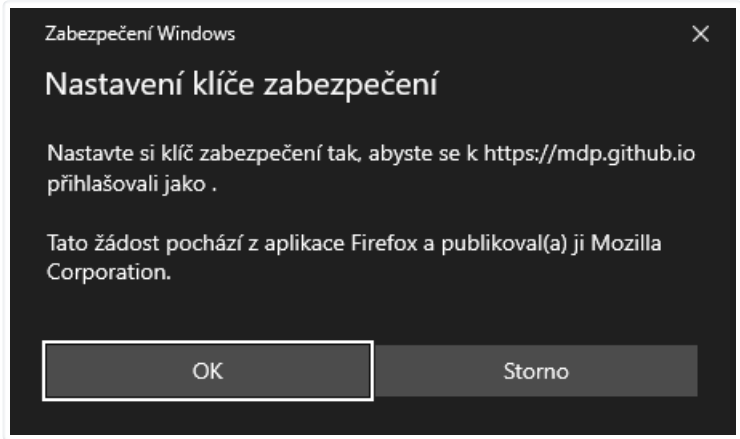
Klasické přihlašování s heslem, kdy token slouží jako druhý faktor k ověření. Lze vyzkoušet na demo nebo na demo. Počet spárovaných služeb využívající token tímto scénářem není nijak omezen kapacitou tokenu (neboť se v tokenu neukládají žádné informace o službě).

Fáze registrace

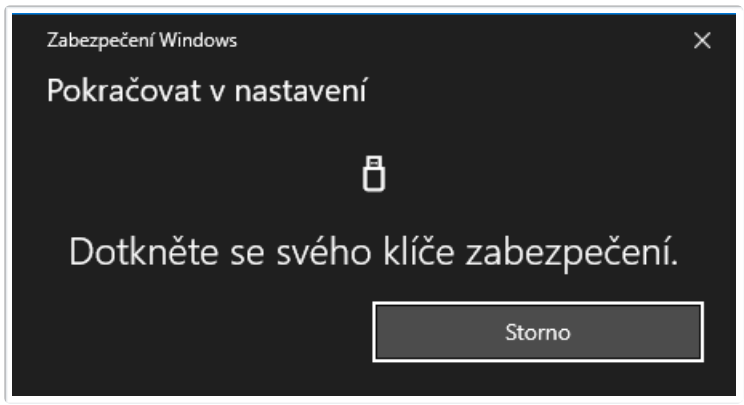
1. Uživatel zvolí uživatelské jméno a heslo



2. Uživatel je vyzván, aby připojil YubiKey

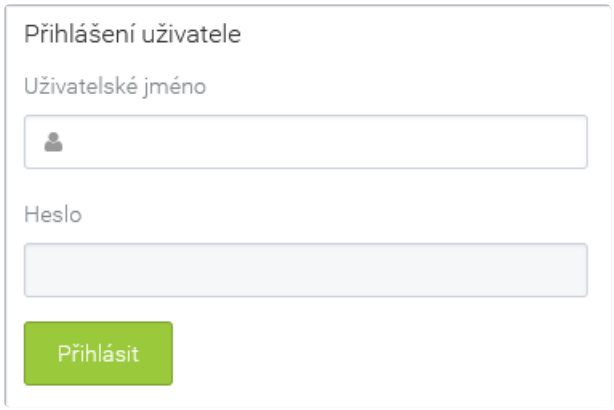


3. Uživatel dokončí registraci stisknutím tlačítka na YubiKey

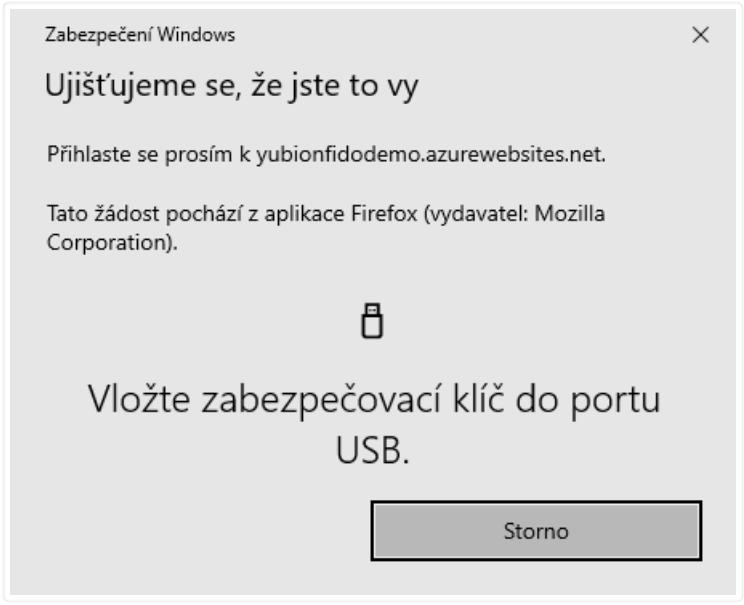


Fáze přihlášení

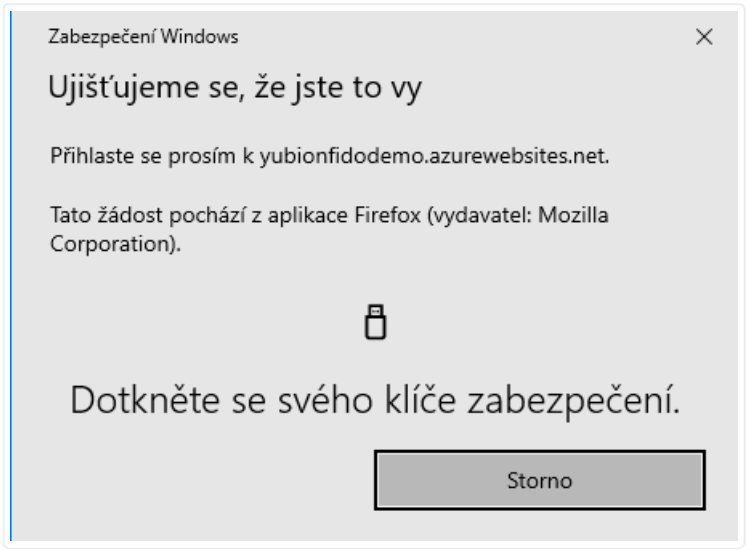
1. Uživatel zadá uživatelské jméno a heslo



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

OTP

OTP modul zahrnuje 2 samostatné konfigurovatelné sloty, na které lze nastavit dle preferencí uživatele tyto funkcionality:

- Yubico OTP
- HMAC-SHA1 Challenge-Response
- Static Password
- OATH-HOTP

Konfiguraci lze provést přes YubiKey Manager nebo skrze YubiKey Personalization Tool . Funkcionalitu jednotlivých slotů pak lze vyvolat různě dlouhým stiskem tlačítka. Sloty lze také ochránit samostatným heslem (při jeho ztrátě lze slot přepsat, nikoliv ale editovat konfiguraci).

- **krátkým stiskem tlačítka** - vyvolá funkcionalitu na slotu 1
- **3 vteřiny dlouhým stiskem tlačítka** - vyvolá funkcionalitu na slotu 2

Yubico OTP

Jedná se o mechanismus ověřování ve formě webové služby s velmi vysokou dostupností od společností Yubico. Provozovatelé služeb tak jednoduše mohou rozšířit své aplikace o druhý faktor (přihlašování, potvrzování důležitých operací) aniž by museli nakupovat specializovaný software nebo pořizovat licence.

Yubico OTP je defaultně přednastaveno na slotu číslo 1.

HMAC-SHA1 Challenge-Response

Tento typ ověřování se nejčastěji používá pro offline autentizaci. Aplikace zašle do YubiKey tokenu výzvu (challenge) a ověří, že token očekávaným způsobem odpověděl. Odeslání odpovědi lze podmínit stiskem tlačítka. Pokud token výzvu neobdrží, není žádný jiný způsob, jak získat odpověď.

Static password

Static password je nejtriviálnější funkcí celého tokenu a jak název napovídá, jedná se o stále stejnou statickou frázi, kterou token generuje. Nejedná se o bezpečnou metodu ověřování, ale v některých prostředích, kde se stále uživatelé potýkají s historickými aplikacemi, může tato funkce usnadnit trápení.

Statické heslo lze využít pro zadávání dlouhých hesel. Token lze pak použít jako generátor statického prefixu hesla (například prvních 10 znaků), kde dalších 8 znaků vždy zadává uživatel. Výsledkem je dlouhé heslo, které si uživatel nemusí celé pamatovat. Zároveň zloděj, který odcizí jeho token, stále nezná celé heslo.

OATH-HOTP

Generátor HOTP kódů, které token emituje stiskem tlačítka (na rozdíl od AUTH modulu, kde HOTP kódy jsou viditelné pouze skrze Yubico Authenticator).

OTP technické informace	
USB Interface	OTP
PIN	nepoužívá se
heslo	defaultní hodnota: není každý slot má vlastní heslo jakmile je jednou nastaveno, lze ho změnit nebo odstranit po jeho zadání v YubiKey Personalization Tool lze ho odstranit přepisem daného slotu
Nejznámější globální služby podporující OTP	• Zobrazit aplikace podporující Challenge-Response • Zobrazit aplikace podporující Yubico OTP • Zobrazit aplikace podporující HOTP
Postup registrace záložního tokenu	doporučeno ihned při registraci primárního tokenu
Poznámky	Apple vývojáři: Challenge-Response na iOS vyžaduje Yubico iOS SDK

OATH

OATH je zkratkou pro Open Authentication a v YubiKey 5 tokenech označuje samostatný modul, který slouží jako úložiště pro celkem 32 jednorázových číselných hesel, neboli OTP (one-time password) kódů. Rozlišujeme dva druhy, OTP kódy generované pomocí TOTP algoritmu (Time-based One-Time Password), kde výsledný kód je platný pouze krátký časový úsek. Po uplynutí času přestává kód platit a je potřeba vygenerovat nový. Naproti tomu OTP kódy generované algoritmem HOTP (HMAC-based One-time Password) jsou platné pouze jednou a každý další kód je odvozen z předchozího (laicky řečeno, výpočet je závislý na nějaké vnitřní inkrementované hodnotě)

Tyto OTP kódy lze zobrazovat přes Yubico Authenticator . Aplikaci lze používat buď v počítači nebo notebooku (desktopová verze) nebo na

telefonu (mobilní verze). Následuje popis desktopové verze. Mobilní verze funguje totožně, akorát aktivace neprobíhá zasunutím YubiKey do USB, ale přiložením tokenu přes NFC rozhraní telefonu.

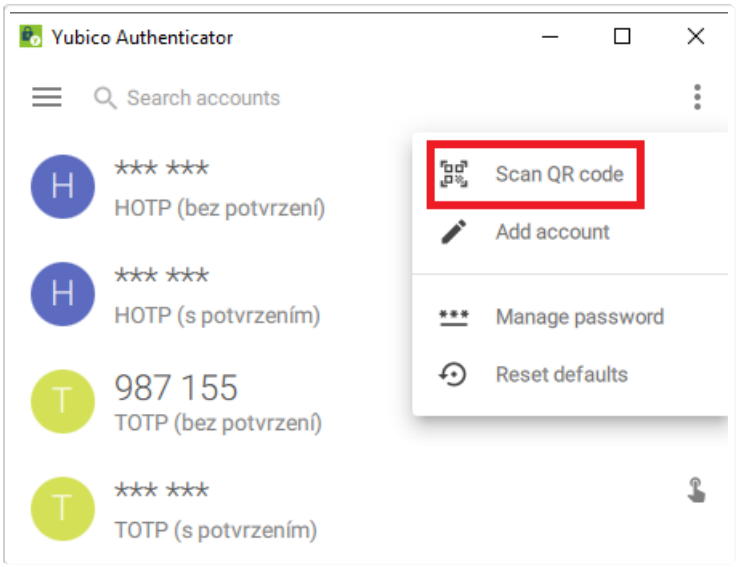
Fáze nastavení

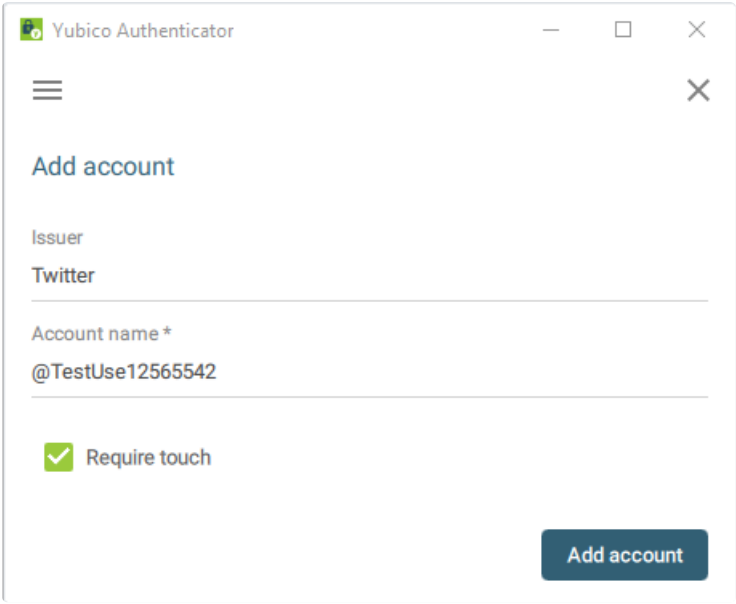
1. Uživatel si ve vybrané službě zvolí dvoufaktorové ověřování pomocí OTP kódů.
   Nejprve je vyzván k nascanování QR kódu. QR kód nese informaci o jménu služby, jménu konkrétního účtu, seedu a nastavení OTP.

   Tento QR kód si nikde neukládejte (úložiště, počítač, mobil), neboť je to jedna z prvních věcí, kterou vyhledává malware.

   Pokud si tento QR kód vytisknete na papír jako zálohu, ověřte si nejprve, že se vaše vytištěné dokumenty neukládají do logu.

2. Uživatel vloží YubiKey do USB a otevře si Yubico Authenticator, kde zvolí Scan QR code. Aplikace automaticky detekuje QR kód zobrazený na monitoru a zpracuje jej, což předvyplní údaje o Poskytovateli služby (Issuer), název účtu (Account name). Volba Require touch je volitelná a určuje, zda-li má být OTP kód viditelný ihned po otevření Yubico Authenticatoru, nebo zda-li bude ještě potvrdit zobrazení stiskem YubiKey tlačítka



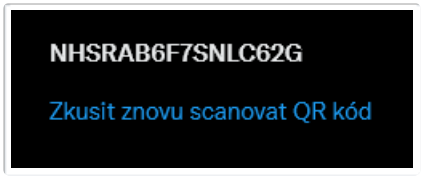


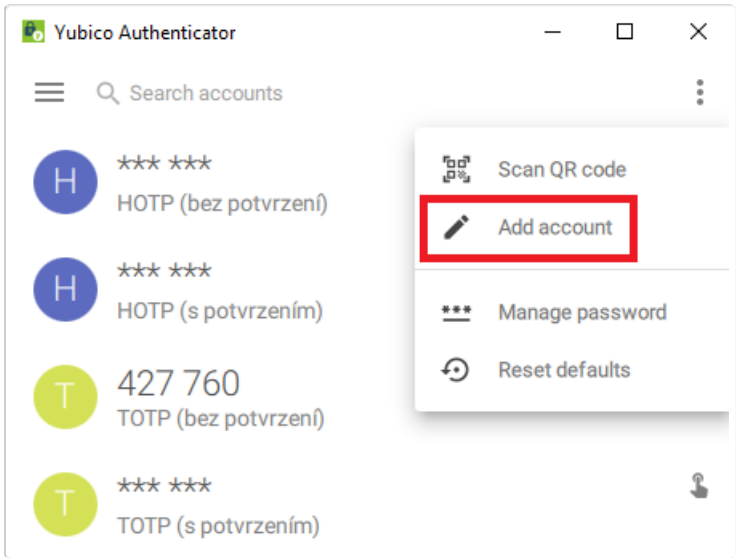
Pokud není QR kód viditelný na monitoru, nebo je překryt právě aplikací Yubico Authenticator, bude aplikace hlásit, že QR kód nenašla. Posuňte okno aplikace mimo QR kód.

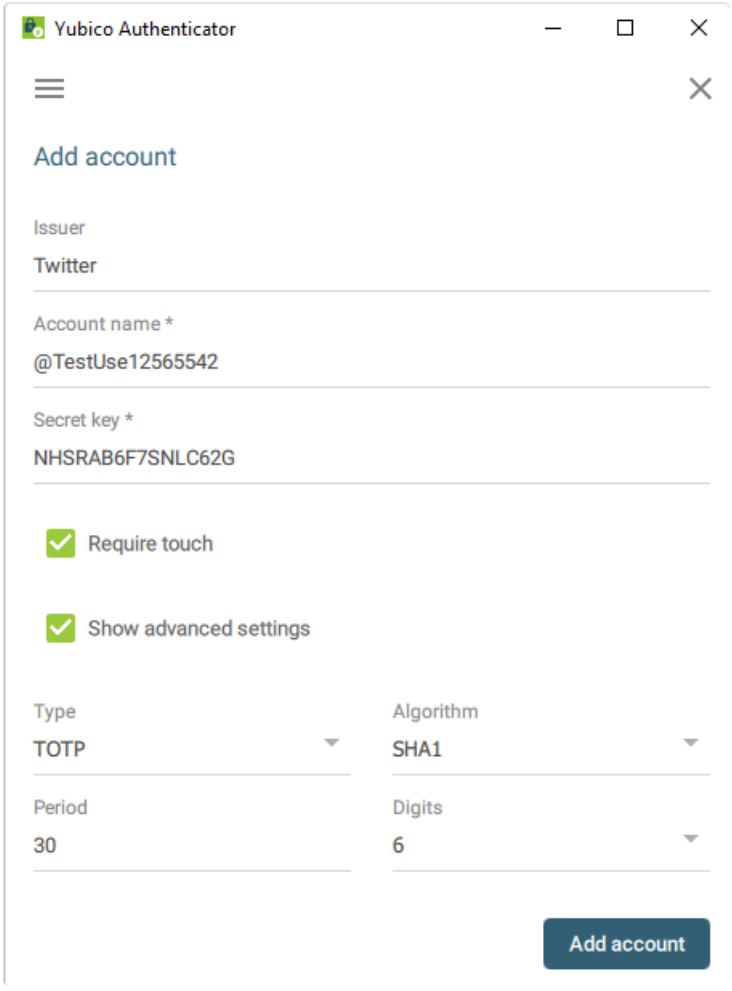
3. Každá služba nabízí i alternativní metodu, pokud nejde QR kód nascanovat, a to opsání seedu (a případně dalších parametrů). V Yubico Authenticatoru je to pak volba Add account. Seed se zadává do pole Secret key. Pomocí Show advanced settings lze měnit parametry generovacího algoritmu. Nejběžněji se používá 6-ti číselný TOTP, který je předvyplněný, pokud služba vyžaduje něco speciálního, uživatele pravděpodobně upozorní.

   Tato možnost se hodí zejména z důvodu vytvoření zálohy. Pokud si uživatel opíše seed (a případně další parametry) a uloží vše na bezpečné místo, bude kdykoliv schopen nastavit jakýkoliv prostředek (YubiKey, Google Authenticator) tak, aby mu začal generovat platné OTP kódy. Stejně tak to ale bude moci učinit útočník, pokud se opsaných údajů zmocní.

   Druhou a bezpečnější strategií je v této fázi nastavit 2 YubiKey tokeny. Záložní token poté uschovat na bezpečné místo. V případě ztráty jednoho tokenu bude ale potřeba celý registrační proces zopakovat, čili přihlásit se do služby zbylým tokenem, zrušit OTP ověřování a nastavit OTP ověřování znovu.



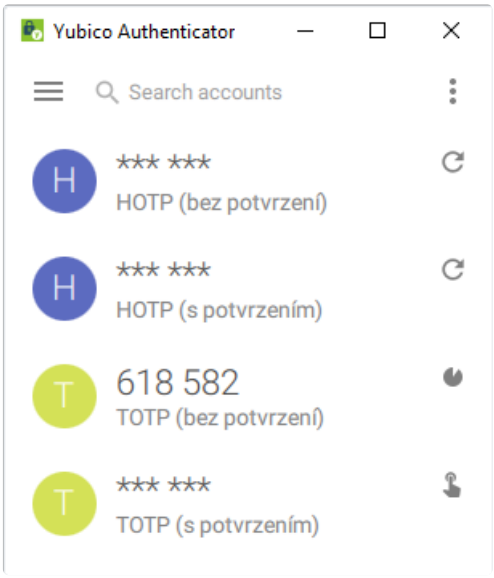




4. Jako potvrzení úspěšného nastavení vás služba požádá o vložení aktuálního OTP kódu. Pokud se jedná o TOTP kódy, které mají omezenou časovou platnost, je potřeba stihnout platný kód přepsat během jeho platnosti.

Služba může mít naimplementovanou jistou toleranci, že i kód, který vypršel, bude po nějakou dobu přijat.

5. Podle typu OTP kódu a nastaveného způsobu zobrazování lze rozlišit 4 situace

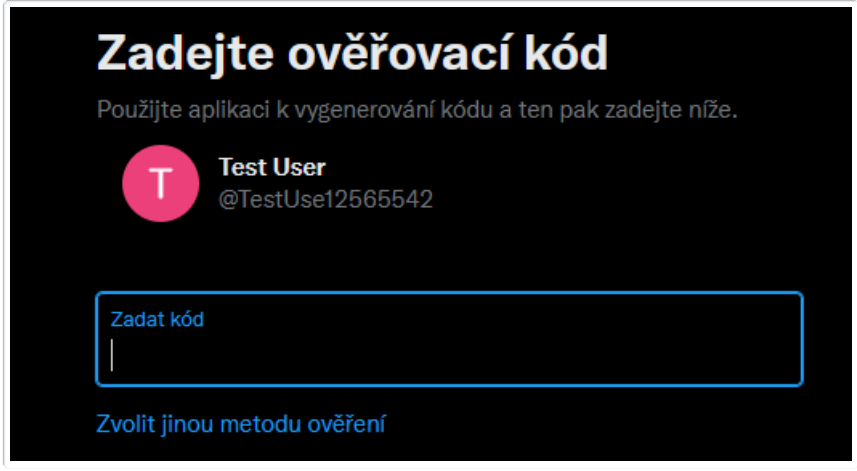


- **TOTP bez potvrzení** se ihned zobrazuje a po vypršení časového intervalu, který definuje životnost aktuálního kódu, se nahradí novým kódem
- **TOTP s potvrzením** se zobrazí jen když uživatel akci potvrdí dodatečným stiskem YubiKey tlačítka, a to pouze do vypršení časového intervalu, který definuje životnost aktuálního kódu
- **HOTP bez potvrzení** se zobrazí poté, co uživatel klikne na daný kód, ten pak zůstane zobrazen dokud uživatel nevygeneruje další
- **HOTP s potvrzením** e zobrazí poté, co uživatel klikne na daný kód a potvrdí akci dodatečným stiskem YubiKey tlačítka, kód pak zůstane zobrazen dokud uživatel nevygeneruje další

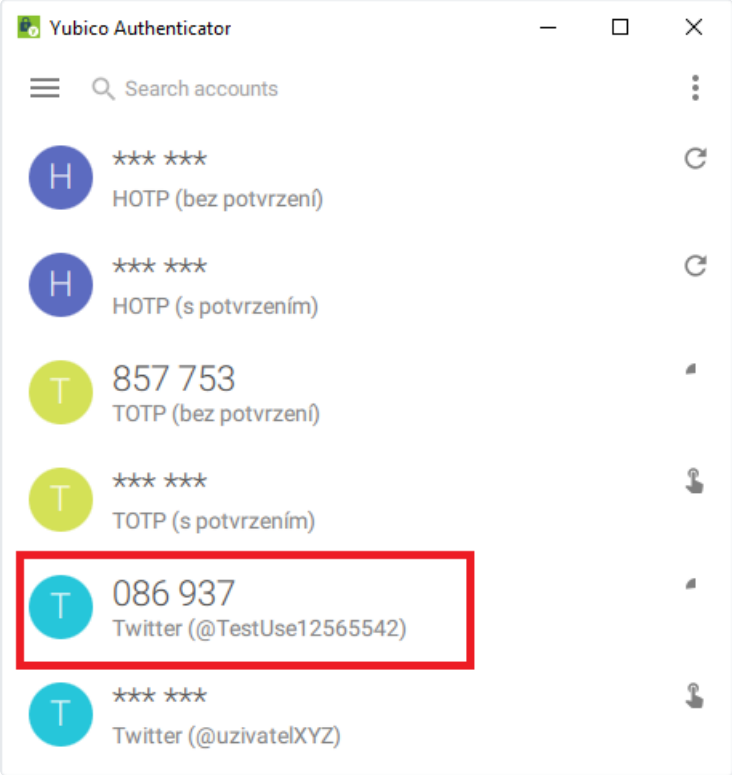
Fáze přihlášení

1. Uživatel zadá uživatelské jméno a heslo

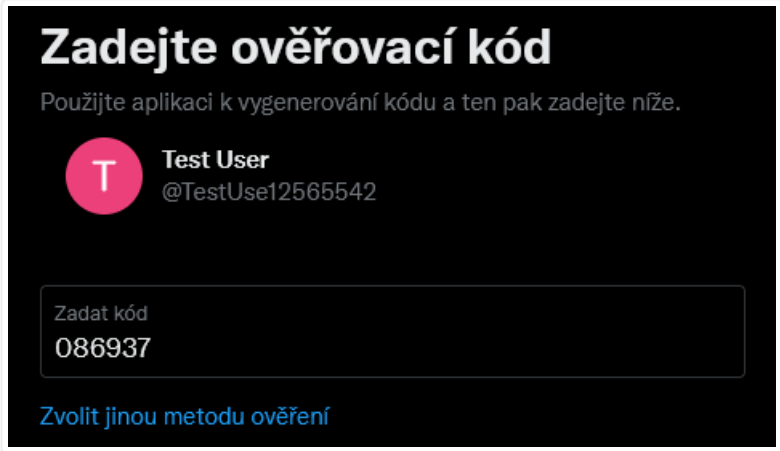
2. Uživatel je vyzván, aby vložil OTP kód



3. Uživatel si otevře Yubico Authenticator a vybere příslušný OTP kód



4. Uživatel vloží OTP kód



OATH technické informace	
USB Interface	CCID
Maximální počet kódů	32
TOTP & HOTP konfigurace	Algoritmy SHA1, SHA256, SHA512 Počet číslic 6, 7, 8
PIN	nepoužívá se
heslo	defaultní hodnota: není jakmile je jednou nastaveno, lze ho změnit nebo odstranit po jeho zadání v aplikaci Yubico Authenticator lze ho odstranit resetem celého OATH modulu

Reset	lze provést přes Yubico Authenticator token bude potřeba znovu zaregistrovat u všech služeb neprovádět bez záložního tokenu, nebo dojde ke ztrátě přístupu k registrovaným službám
Nejznámější globální služby podporující OTP	Zobrazit aplikace podporující TOTP Zobrazit aplikace podporující HOTP
Postup registrace záložního tokenu	doporučeno ihned při registraci primárního tokenu
Poznámky	Apple vývojáři: Na iOS je vyžadován Yubico iOS SDK

PIV (Smart Card)

YubiKey disponuje funkcionalitou čipové karty (smart card) podle amerického vládního standardu PIV (nebo také FIPS 201). Token podporuje algoritmy ECC a RSA ze světa asymetrické kryptografie. Uživatel tak může podepisovat a šifrovat pomocí privátního klíče uloženého v tokenu skrze standardizované rozhraní PKCS#11.

Klíče a certifikáty jsou uloženy v tzv. slotech a mají nastavené defaultní politiky (popis viz tabulka níže), které ale lze změnit.

Aplikace YubiKey Manager nabízí mimojiné tyto funkce pro PIV modul:

- Nastavení PINu, PUKu a Management klíče
- Vygenerování certifikátů tokenem na sloty 9a, 9c, 9d a 9e
- Importování certifikátů do tokenu na sloty 9a, 9c, 9d a 9e
- Vyresetování PIV modulu

The YubiKey 5 podporují rozšířené APDU: Answer To Reset (ATR), Answer To Select (ATS) - na iOS je potřeba Yubico iOS SDK.

Podpora na Windows

Na operačním systému Windows lze PIV funkčnost dále rozšířit pomocí speciálního ovladače YubiKey Smart Card Minidriver. Díky tomuto budou dostupné i tyto funkce:

- Enrollment YubiKey tokenu standardními Windows nástroji
- Auto-enrollment, umožňující uživateli self-provisioning YubiKey tokenu a automatické obnovení
- Podpora více autentizačních certifikátů na jednom YubiKey tokenu
- Změnu PINu z menu po stisknutí Ctrl+Alt+Del
- Odblokování PINu pomocí PUK na Windows přihlašovací stránce

Technické informace	
USB Interface	CCID
PIN	defaultní hodnota: 123456
PUK	defaultní hodnota: 12345678
Management Key (3DES)	defaultní hodnota: 010203040506070801020304050607080102030405060708
RSA algoritmy	RSA 1024 RSA 2048
ECC algoritmy	ECC P-256 ECC P-384
Sloty	
Slot 9a: PIV Authentication	Certifikát a jeho asociovaný privátní klíč v tomto slotu se používají k autentizaci uživatele (přihlašování do systémů). Při první interakci je vyžadován PIN.
Slot 9c: Digital Signature	Certifikát a jeho asociovaný privátní klíč v tomto slotu se používají k digitálnímu podepisování (dokumenty, emaily, soubory). Při jakékoliv interakci je vyžadován PIN.

Slot 9d: Key Management	Certifikát a jeho asociovaný privátní klíč v tomto slotu se používají k šifrování (emaily, soubory). Při první interakci je vyžadován PIN.
Slot 9e: Card Authentication	Certifikát a jeho asociovaný privátní klíč v tomto slotu se používají k fyzickému přístupu do budov (kde jsou použity PIV-kompatibilní zámky). Při interakci není vyžadován PIN.
Sloty 82-95: Retired Key Management	Tyto sloty se používají pro předchozí klíče uložené na slotu Slot 9d: Key Management. Díky tomu bude s tokenem možné dešifrovat emaily a dokumenty šifrované staršími klíči.
Slot f9: Attestation	Tento slot se používá k *atestaci* (attestation) ostatních vygenerovaných klíčů tokenem, které byly vytvořeny s instrukcí f9. Tento slot není vymazán resetováním. Tento slot je přepisovatelný.
Politiky (Policy)	
PIN Policy	Lze určit pro každý slot, jestli má být vyžadováno zadání PINu při požadavku na tento slot. Musí být nastaveno při generování nebo importu klíče - nelze později měnit
Touch Policy	Lze určit pro každý slot, jestli má být vyžadován stisk tlačítka tokenu při požadavku na tento slot. Musí být nastaveno při generování nebo importu klíče - nelze později měnit
Odkazy	
Manuál pro PIV	Yubico stránky (anglicky)
Manuál YubiKey Manageru	stránky (anglicky)
Minidriver ve firemním prostředí	Yubico stránky (anglicky)

OpenPGP

OpenPGP je standard používající asymetrickou kryptografii. YubiKey 5 tokeny fungují jako tzv. OpenPGP karta, což je čipová karta kompatibilní dle ISO/IEC 7816-4, -8, kterou lze používat s PGP aplikacemi (např. GnuPG (GPG)) a uložit na ní GPG klíče pro autentizaci, podepisování a šifrování. Tokenu lze nastavit pravidla potvrzování tlačítkem pro každý klíč zvlášť.
Od verze YubiKey firwaru 5.2.3 je implementovaná podpora OpenPGP karty ve verzi 3.4, která přinesla řadu vylepšení.

Pro využití OpenPGP na iOS je potřeba Yubico iOS SDK.

Technické informace	
USB Interface	CCID
PIN	defaultní hodnota: 123456
Admin PIN	defaultní hodnota: 12345678
RSA algoritmy	RSA 1024 RSA 2048 RSA 3072 (vyžaduje GnuPG verze 2.0 a vyšší) RSA 4096 (vyžaduje GnuPG verze 2.0 a vyšší)
ECC algoritmy	využití pro Signature, Authentication and Decipher secp256r1 secp256k1 secp384r1 secp521r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1 curve25519 x25519 (decipher only) ed25519 (sign / auth only)
Odkazy	

Manuál pro OpenPGP	Yubico stránky (anglicky)
OpenPGP Smart Card 3.4 specifikace	pdf (anglicky)
Podpora 3.4 specifikace	Yubico stránky (anglicky)

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 5 Nano tokenu zvolit vhodného kandidáta na záložní token s přihlédnutím k pořizovací ceně.

Primární token	Vhodný záložní token
 YubiKey 5 Nano	 YubiKey 5 NFC

Bezpečnostní zásady

Primární YubiKey 5 Nano token má uživatel zasunutý v USB portu svého zařízení, které má stále u sebe, 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.

U protokolů založených na OTP není pozdější doregistrování tokenů možné, pokud uživatel nemá uložený tzv. *seed*. A podobné omezení mají certifikáty vygenerované přímo tokenem, které nelze žádným způsobem vyextrahovat. V sekci funkce je u každého protokolu detailně popsáno, kdy provést registraci záložních tokenů a jaké jsou omezení dané technologie.

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 5 Nano

Instalace nástrojů

Nainstalujeme si následující aplikace do počítače nebo notebooku:

- YubiKey Manager
- Yubico Authenticator (verze Desktop)
- YubiKey Personalization Tool

Nastavení k prvnímu použití

- Nastavení FIDO2 PINu v YubiKey Manageru
- Změna továrního PIV PINu v YubiKey Manageru
- Změna továrního PIV PUK kódu v YubiKey Manageru
- Statické heslo na slot 2 v YubiKey Manageru
- Vygenerování Authentication certifikátu v YubiKey Manageru

Nástroje pro YubiKey 5 Nano

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
YubiKey Personalization Tool

YubiKey Personalization Tool umí nastavit programovatelné sloty 1 a 2, zjistit firmware tokenu nebo konfigurovat chování a pokročilé vlastnosti.

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
Yubico Login

Yubico Login aplikaci lze využít pro zabezpečení přístupu do počítače, který využívá lokální účty (nikoliv doménové účty). Uživatel pak musí potvrdit přihlášení svým tokenem.

Přejít na domovskou stránku
Developer Resources

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

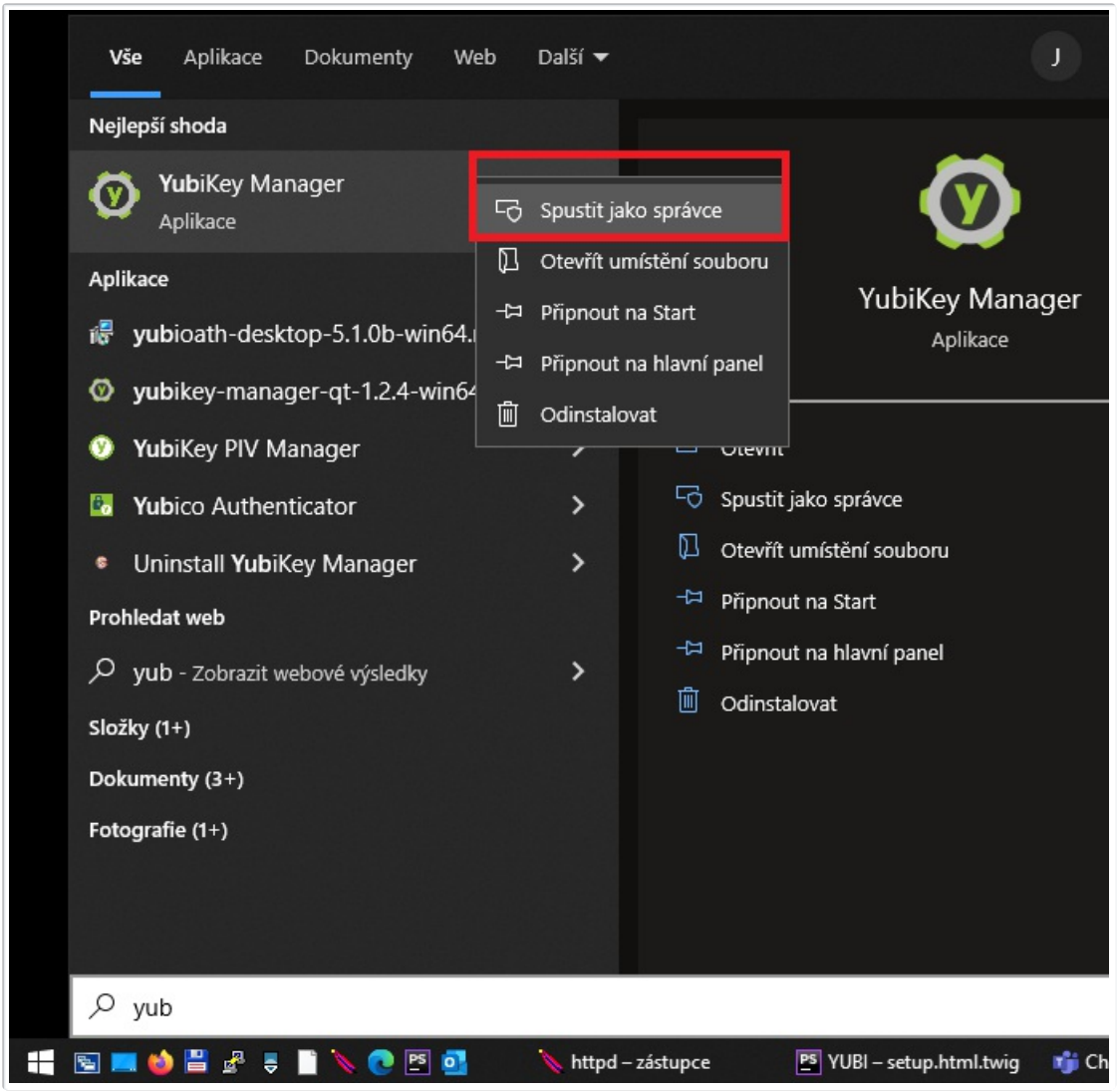
Přejít na domovskou stránku

Návody pro YubiKey 5 Nano

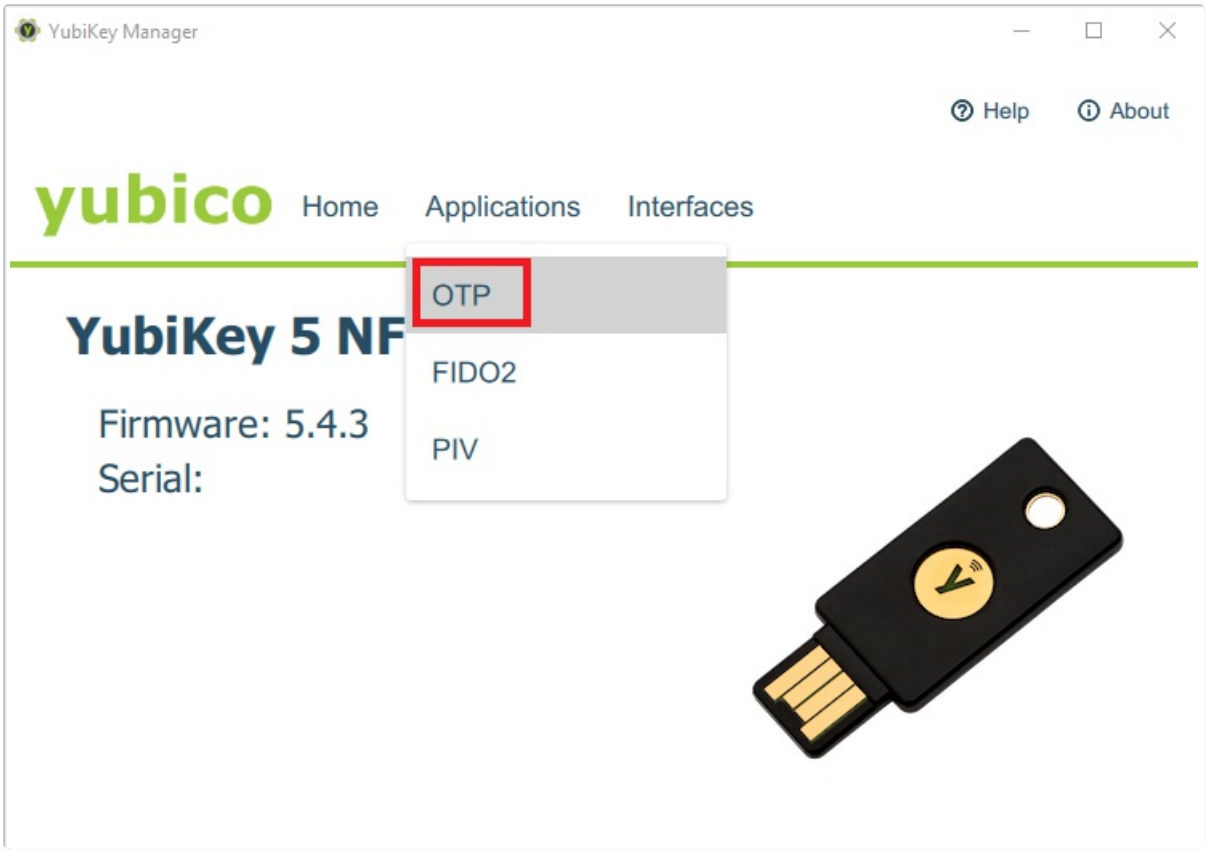
Statické heslo na slot 2 v YubiKey Manageru

Nastavíme dlouhý stisk tokenu tak, aby generoval statické heslo. Může se hodit pro starší aplikace, kde není možnost nastavit jinou metodu přihlašování.

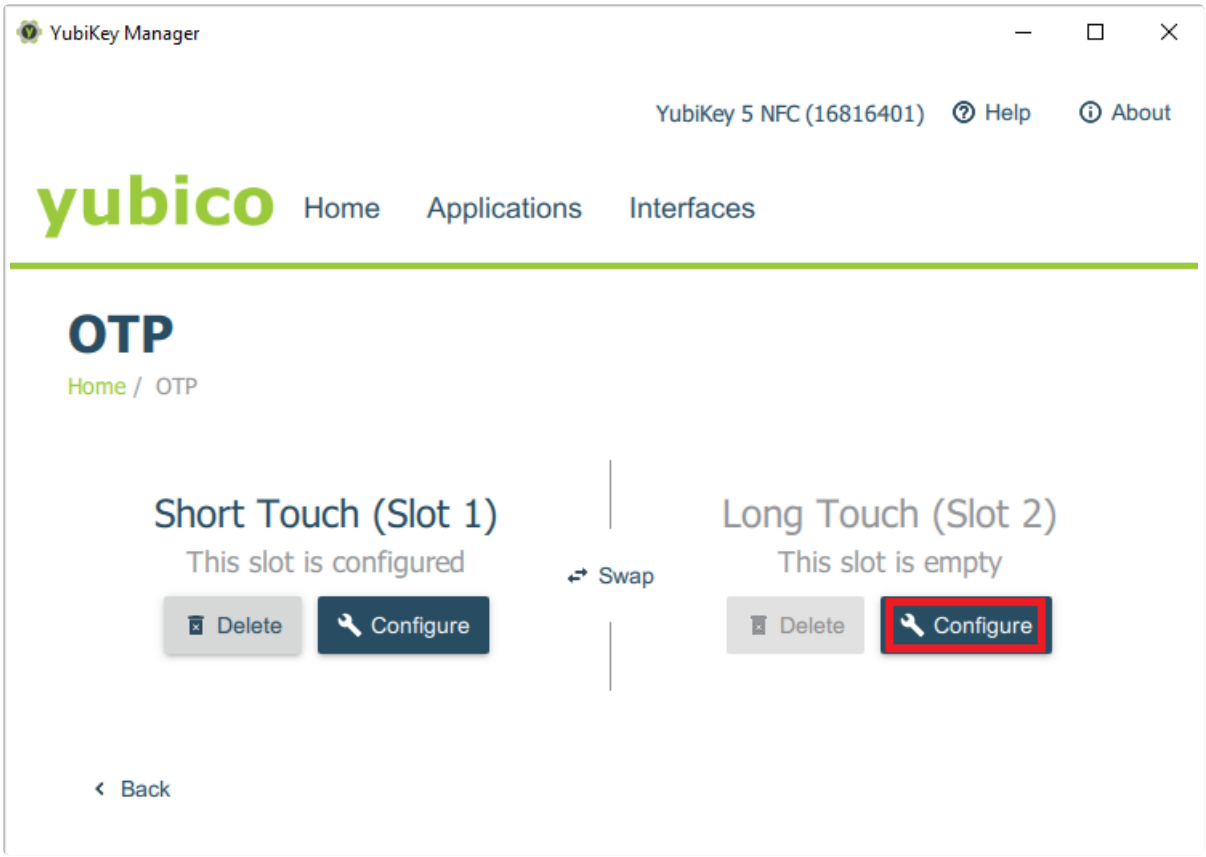
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



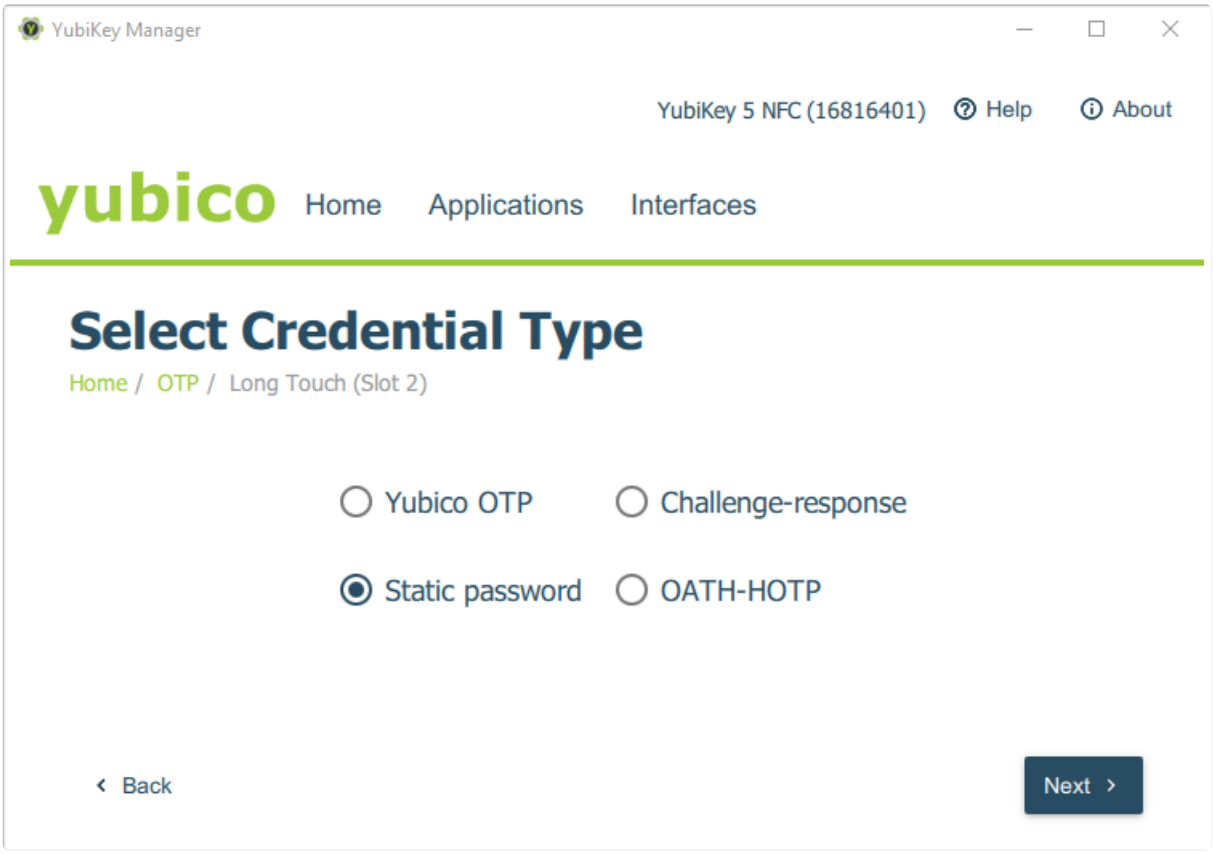
2. Zvolíme volbu *OTP*.



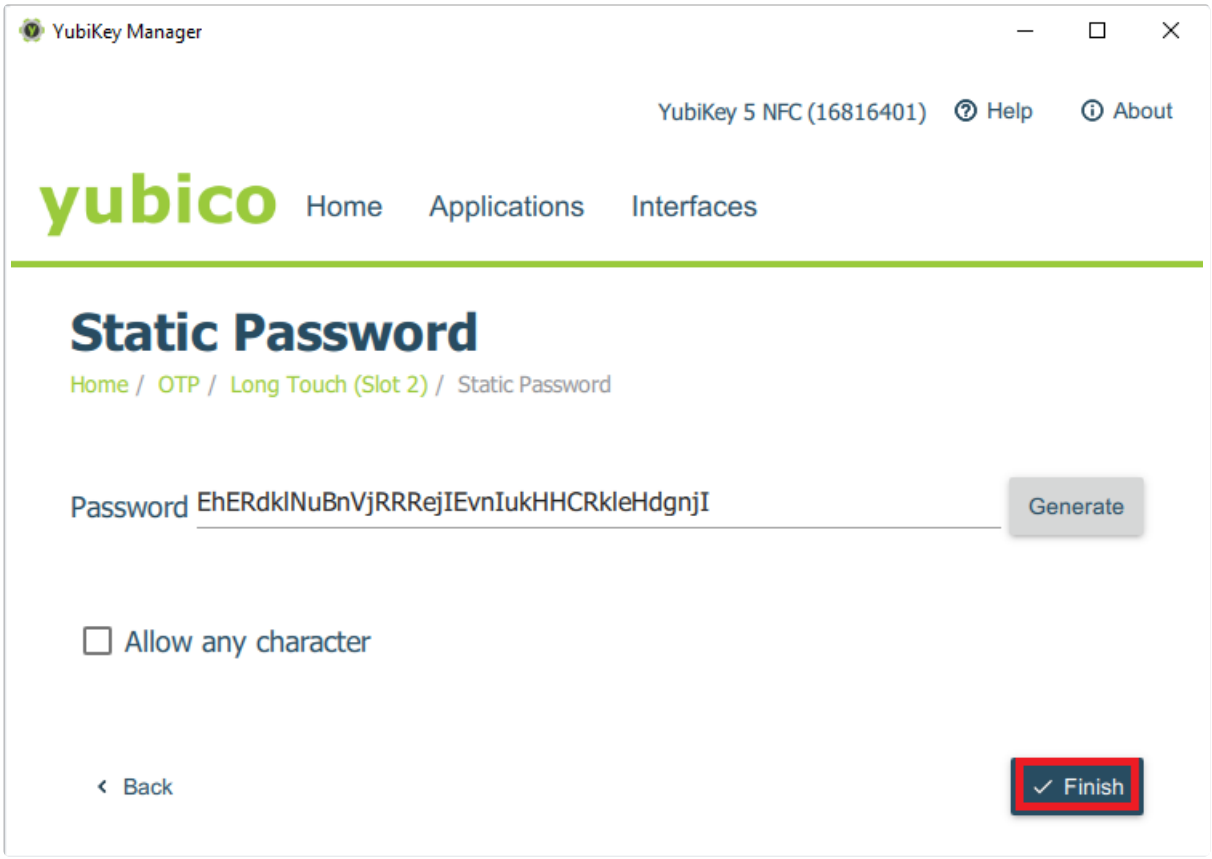
3. Klikneme na *Configure* vpravo pro *Long Touch* (dlouhý stisk).



4. Vybereme volbu *Static password* a stiskneme tlačítko *Next*.

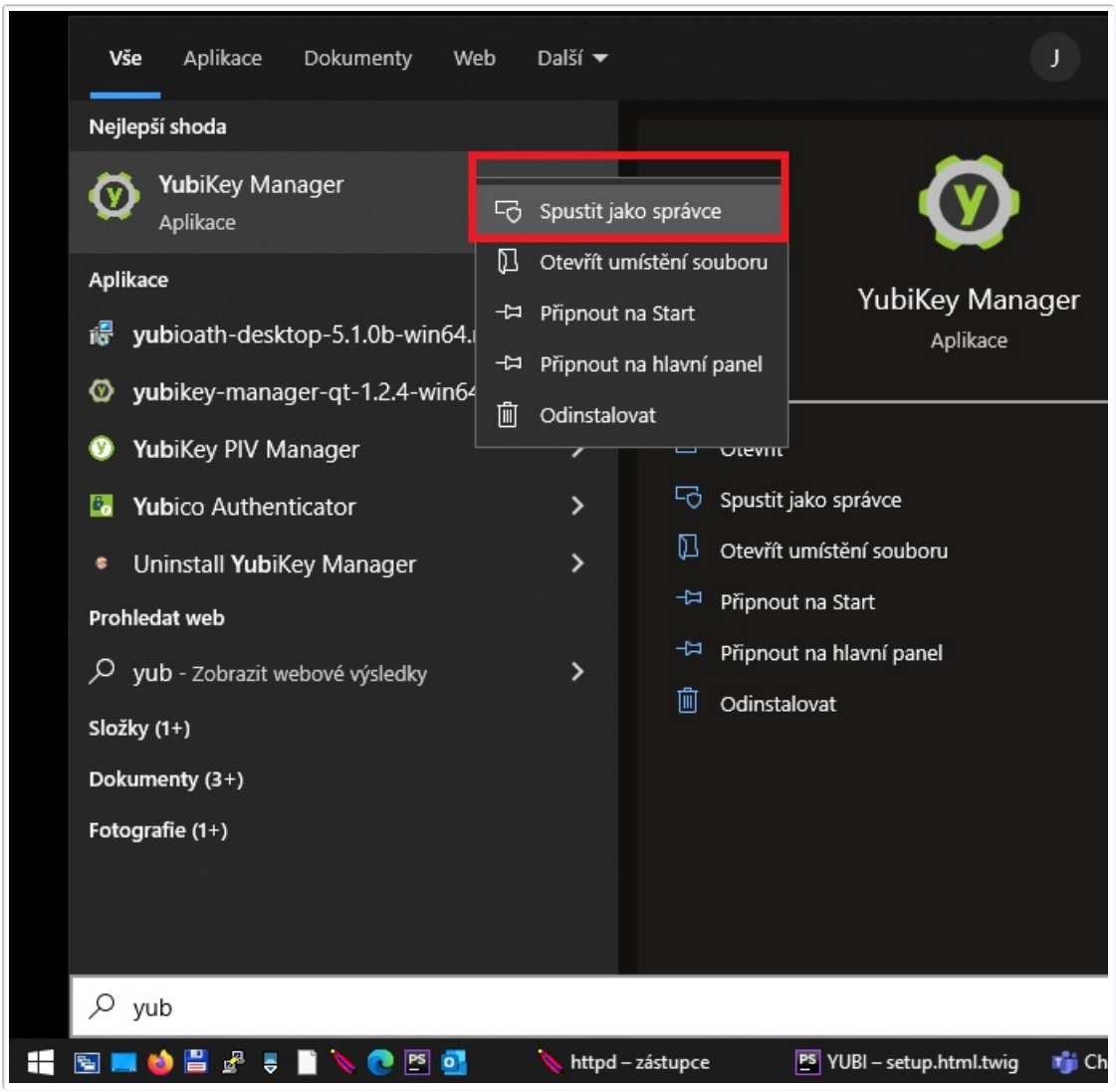


5. Klikneme na tlačítko *Generate*, necháme si heslo vygenerovat a potvrdíme volbu tlačítkem *Finish* (pokud zaškrtneme volbu *Allow any character*, vygenerovaná sekvence znaků bude komplexnější, ale bude fungovat pouze na anglické klávesnici).

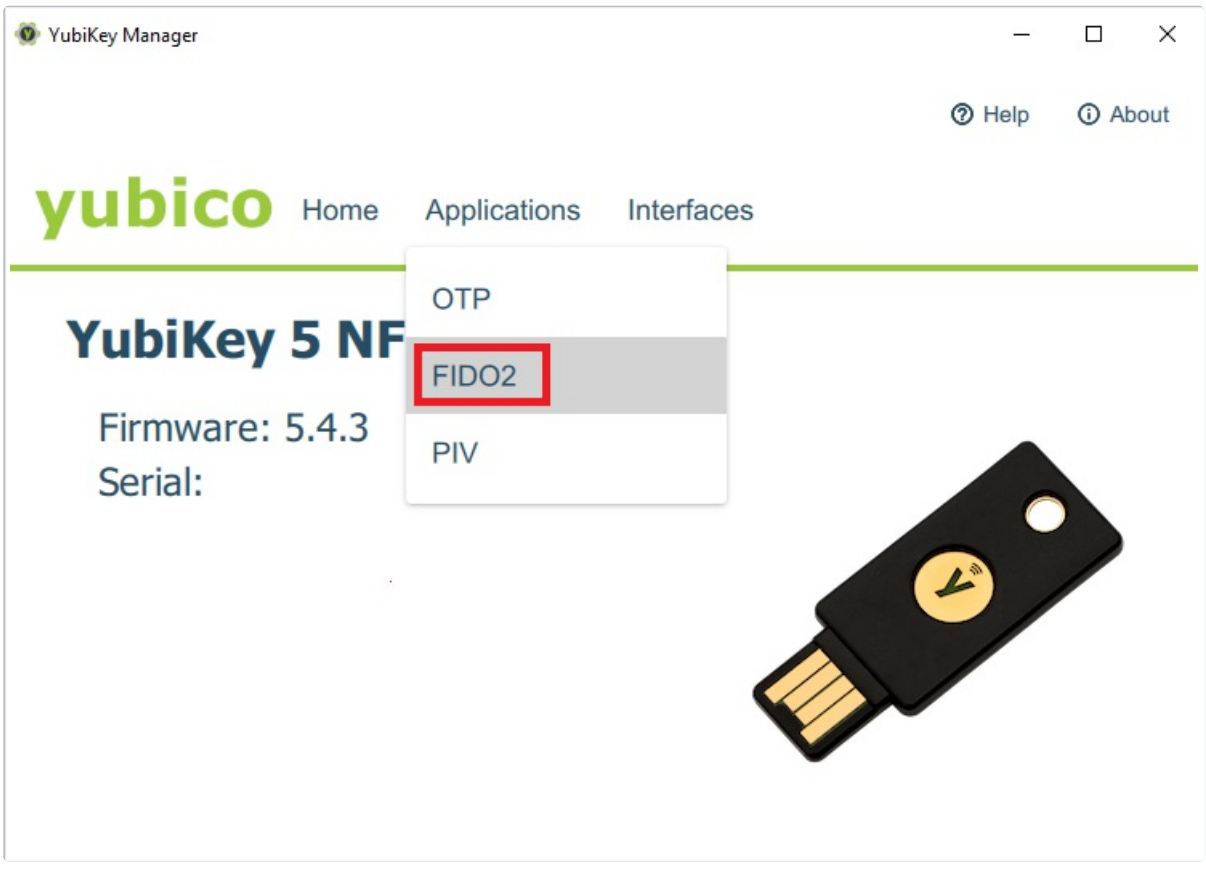


Nastavení FIDO2 PINu v YubiKey Manageru

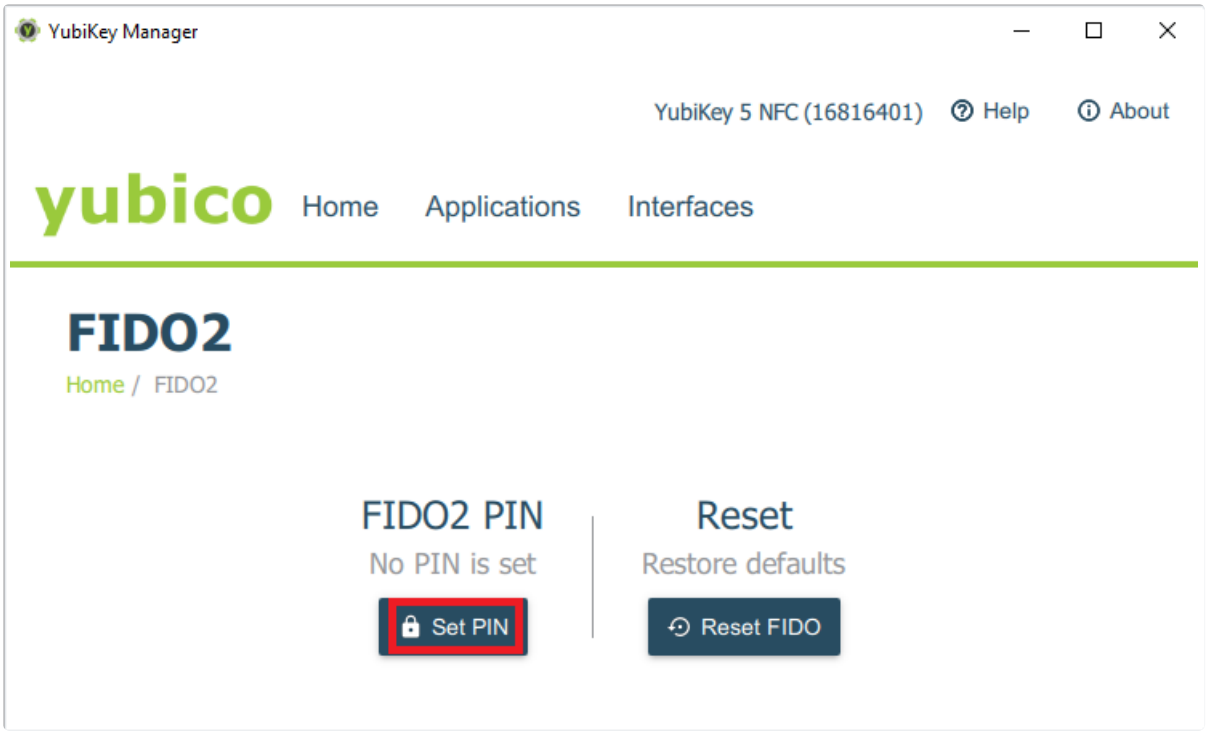
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



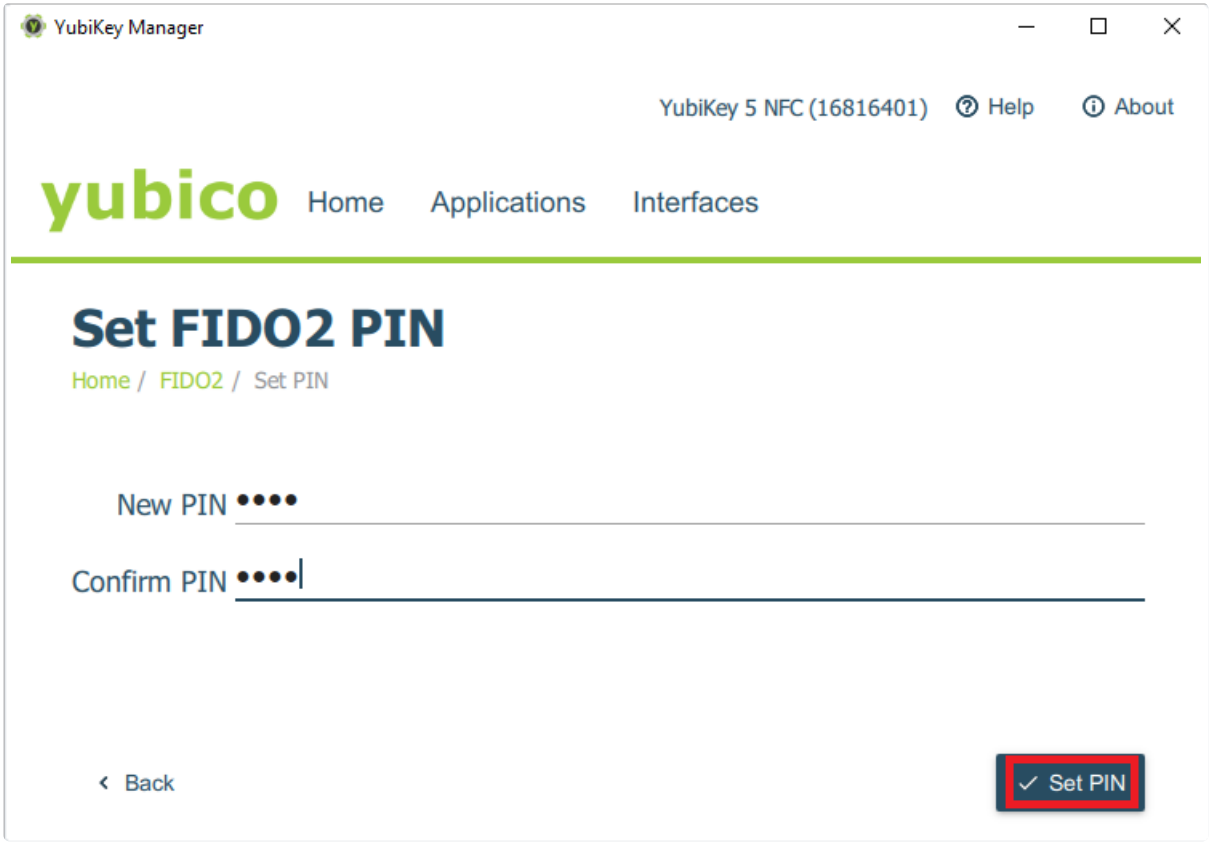
2. Zvolíme volbu *FIDO2*.



3. Klikneme na *Set PIN*.

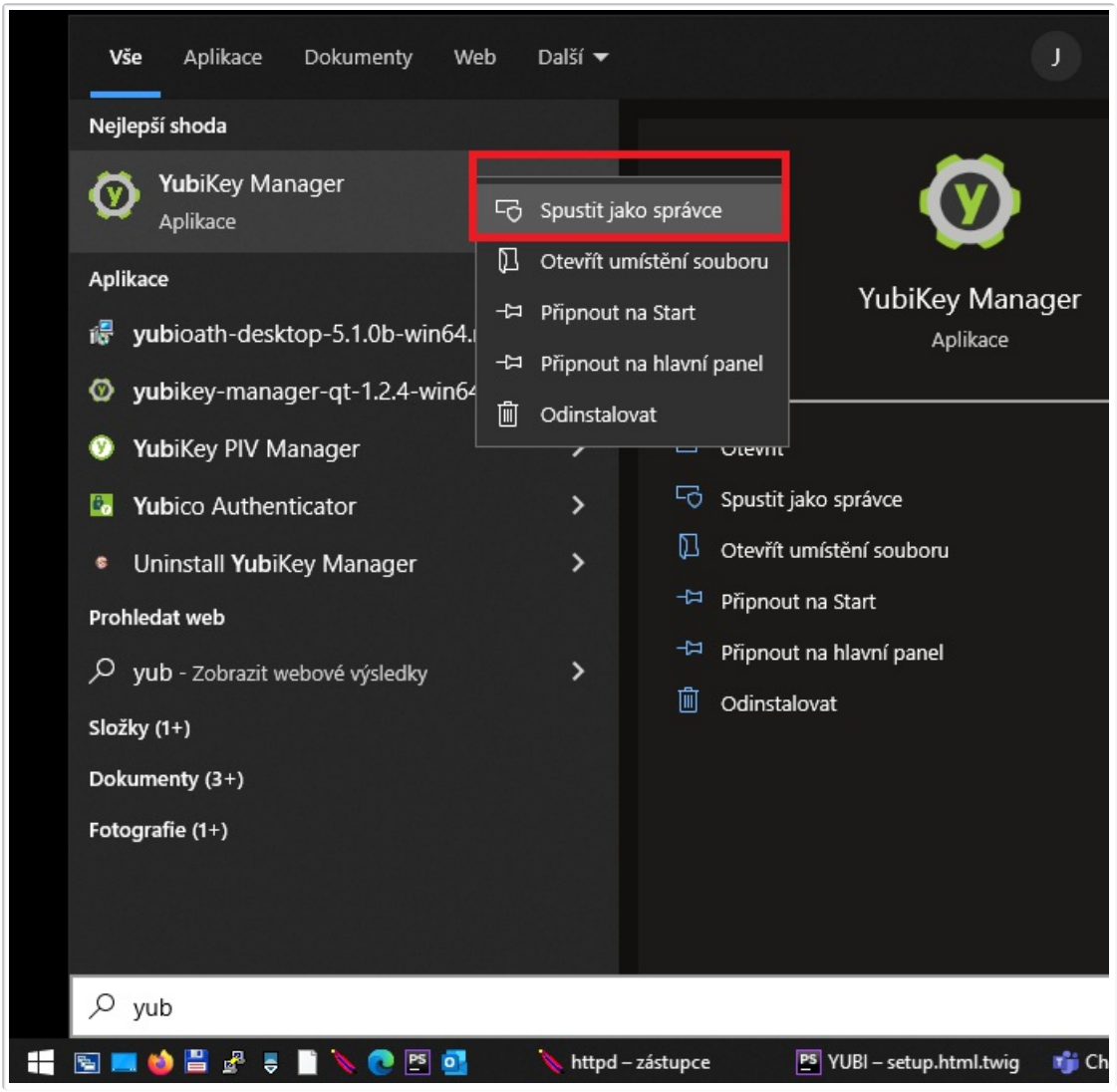


4. Zvolíme si alfanumerický PIN (minimálně 4 znaky) v poli *New PIN*, potvrdíme jej v poli *Confirm PIN* a uložíme pomocí tlačítka *Set PIN*.

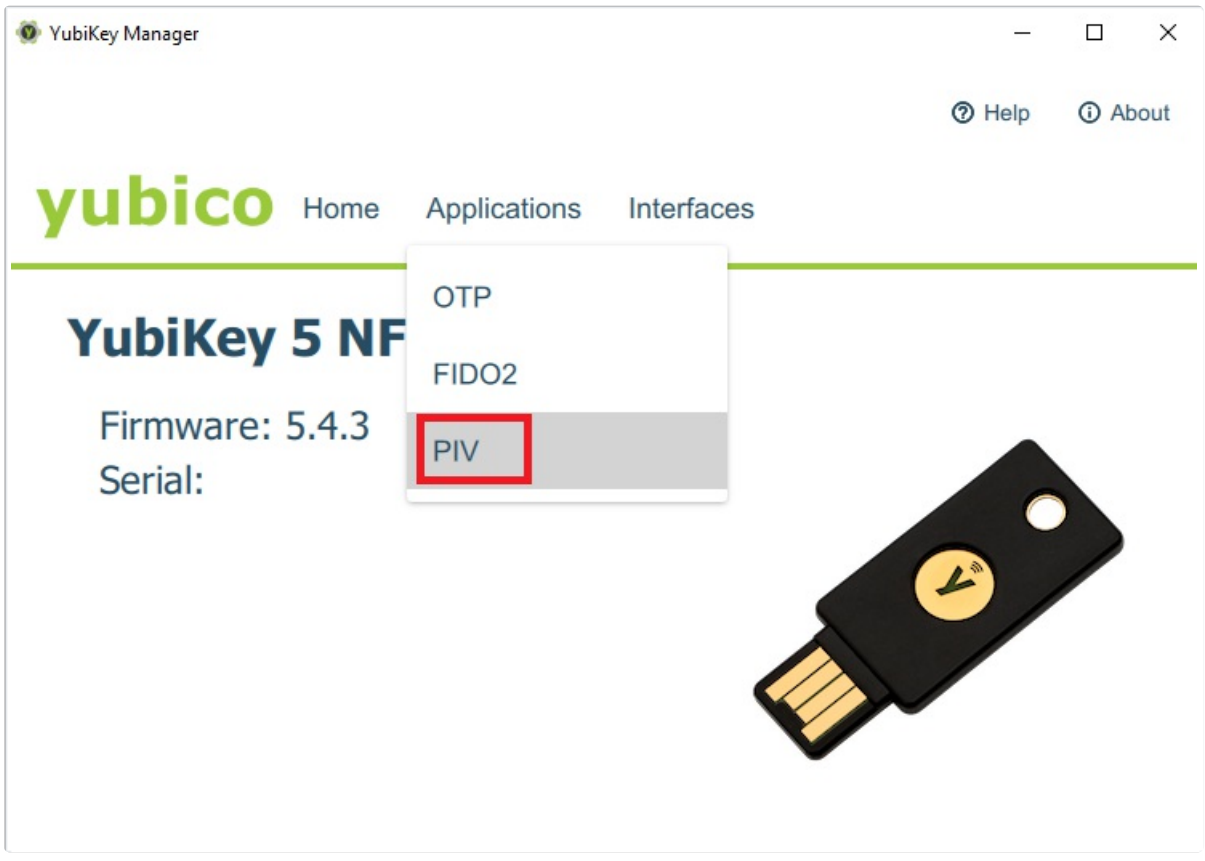


Změna továrního PIV PINu v YubiKey Manageru

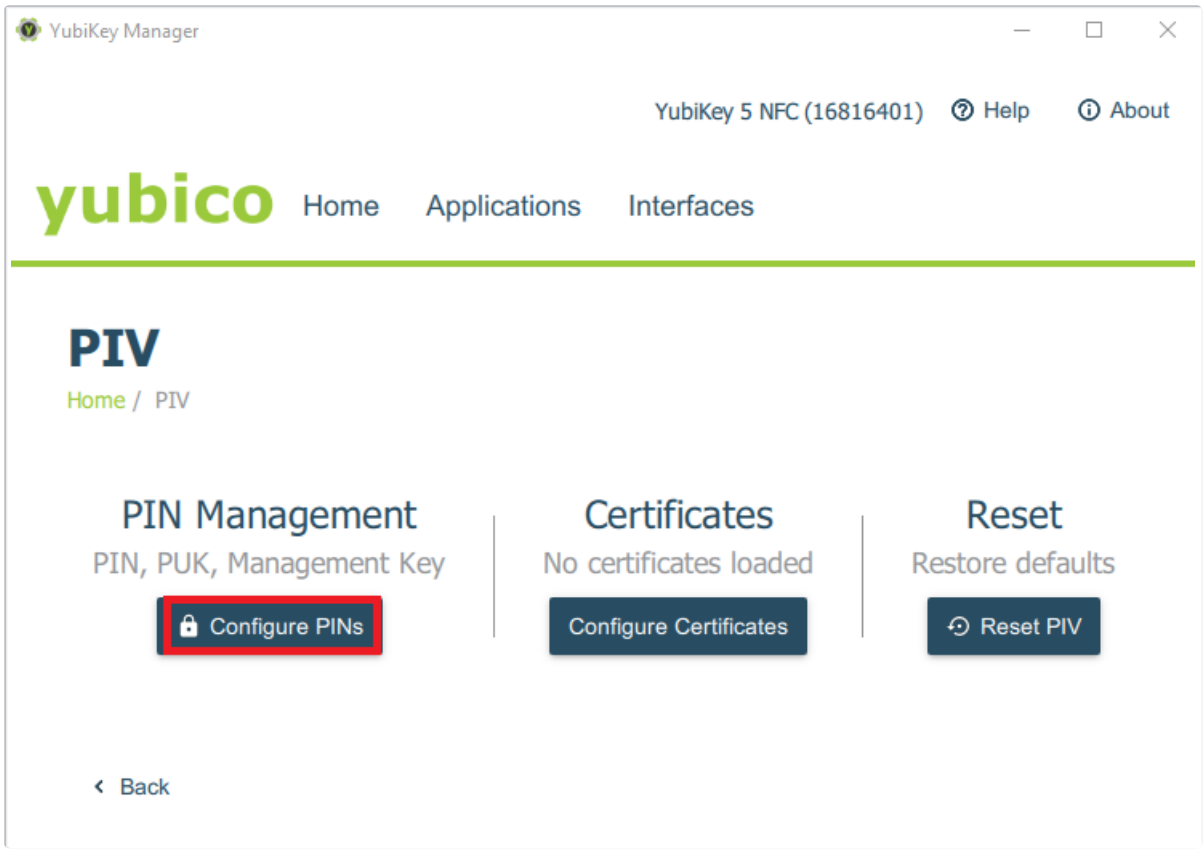
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



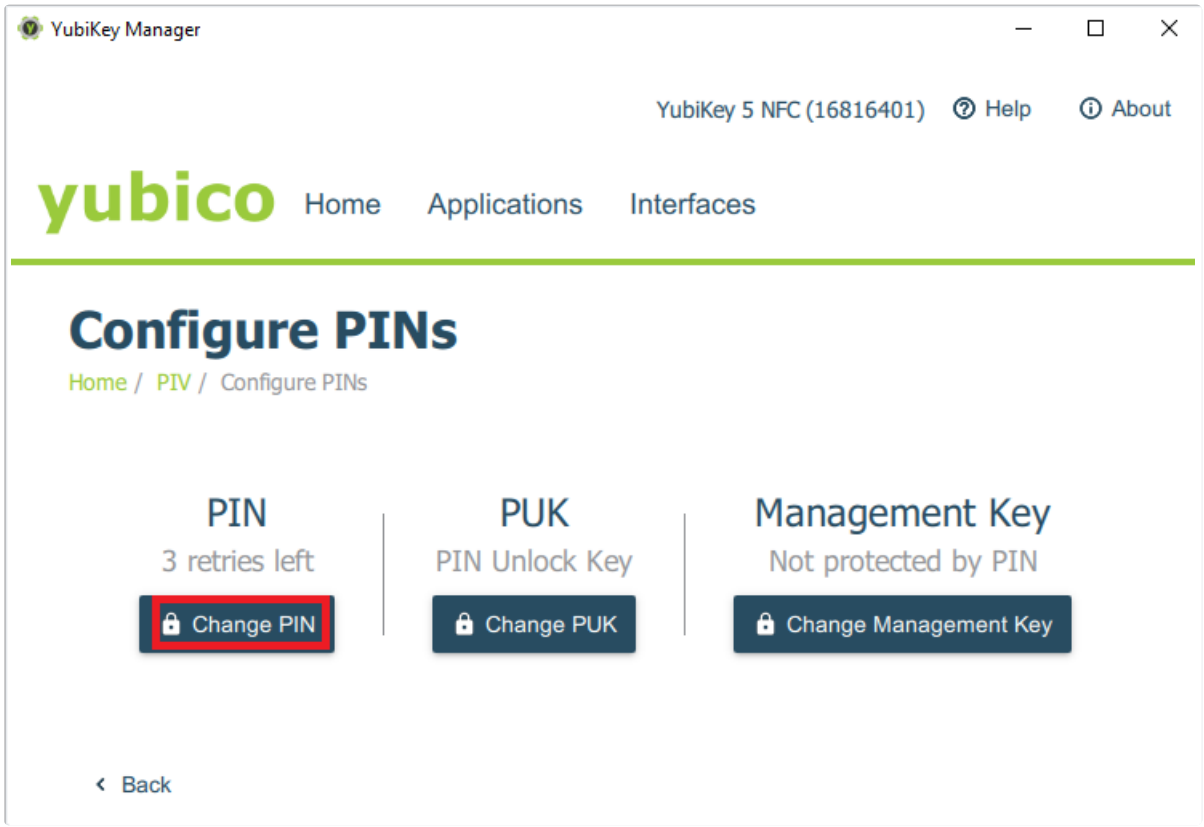
2. Zvolíme volbu *PIV*.



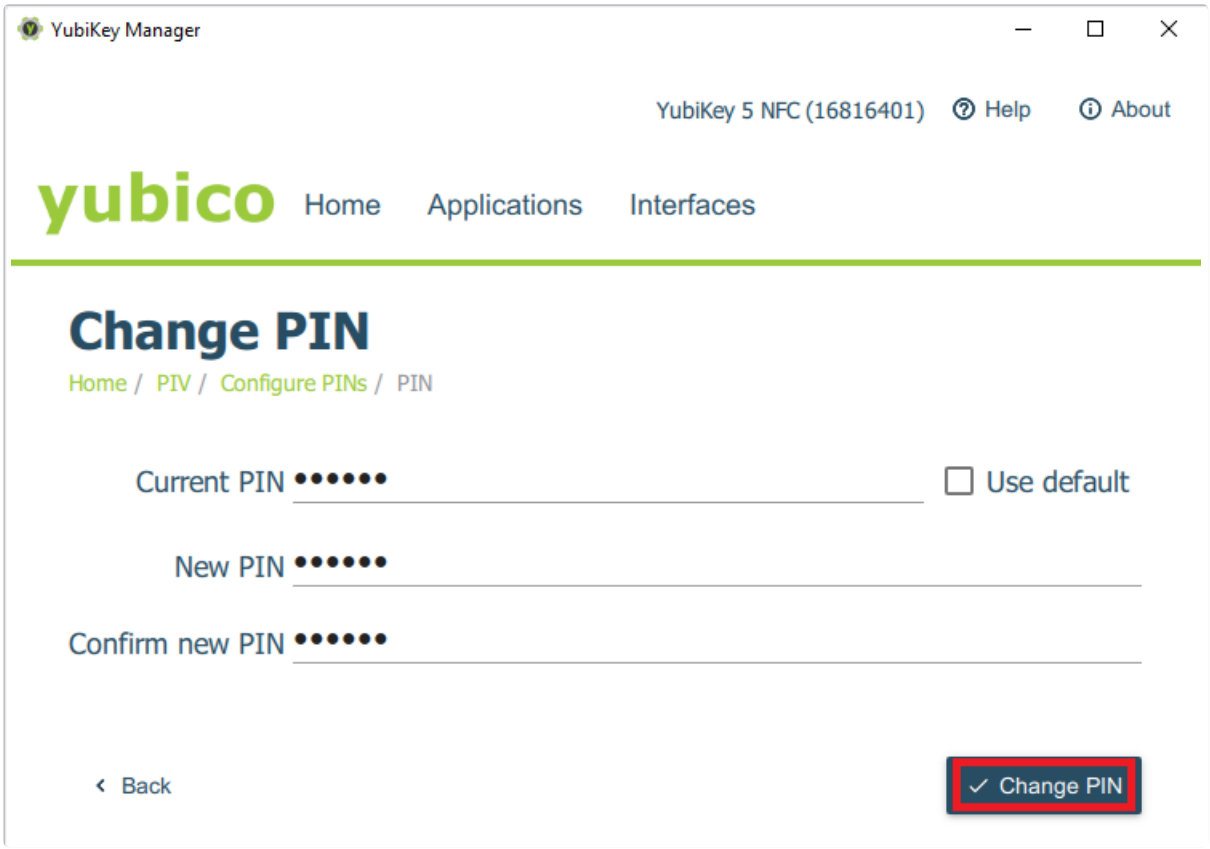
3. Klikneme na *Configure PINs*.



4. Klikneme na *Change PIN*.

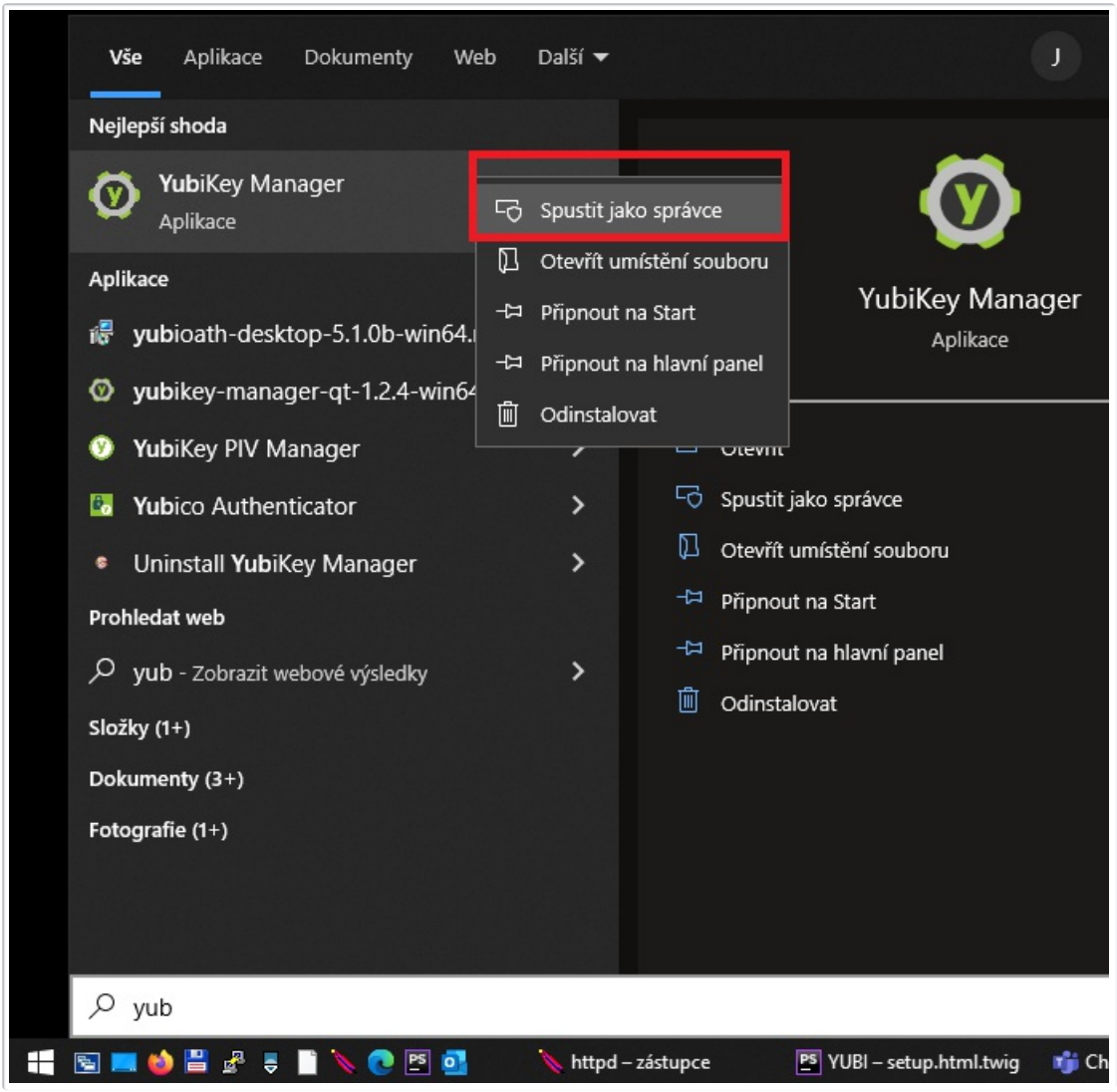


5. Do pole *Current PIN* zadáme defaultní PIN (nebo zaškrtneme volbu *Use default*), nový PIN (6-8 alfanumerických znaků) zadáme do pole *New PIN* a potvrdíme v poli *Confirm new PIN*. Pomocí tlačítka *Change PIN* změnu uložíme.

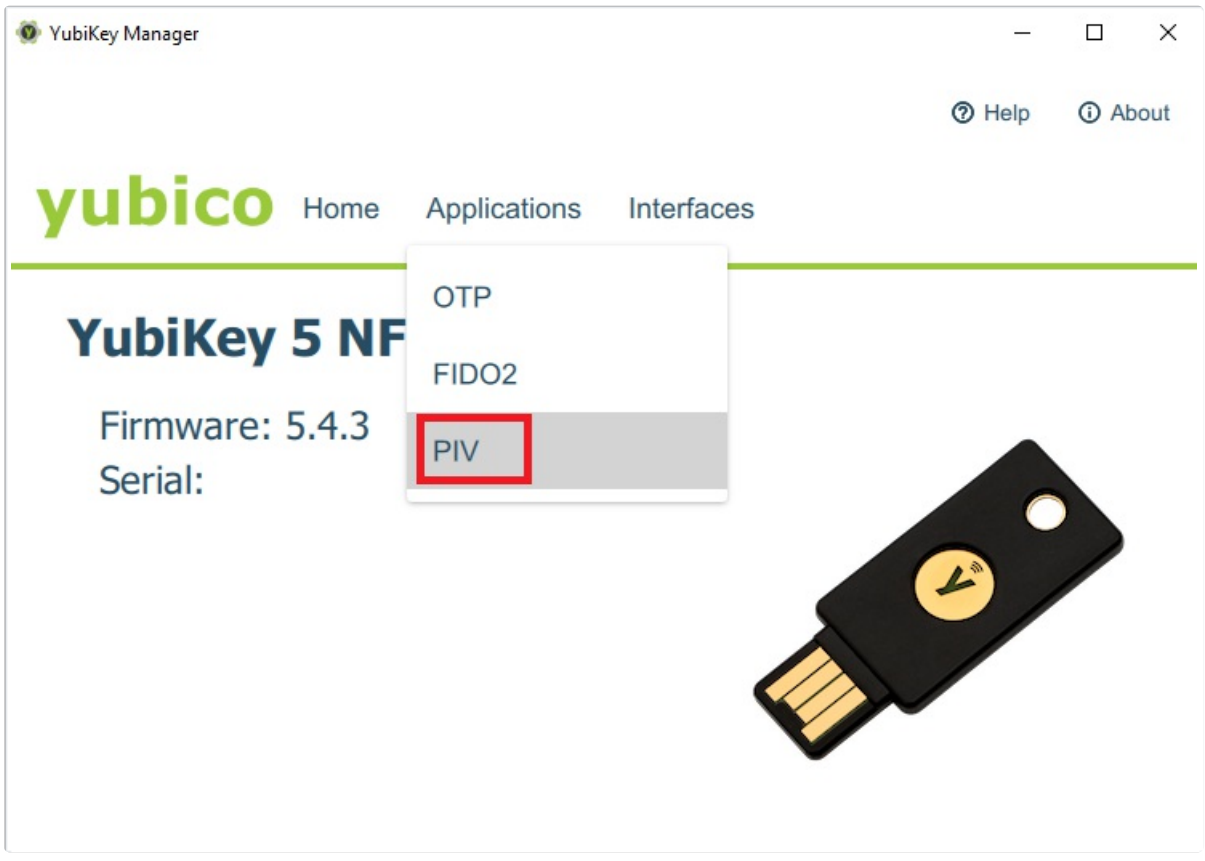


Změna továrního PIV PUK kódu v YubiKey Manageru

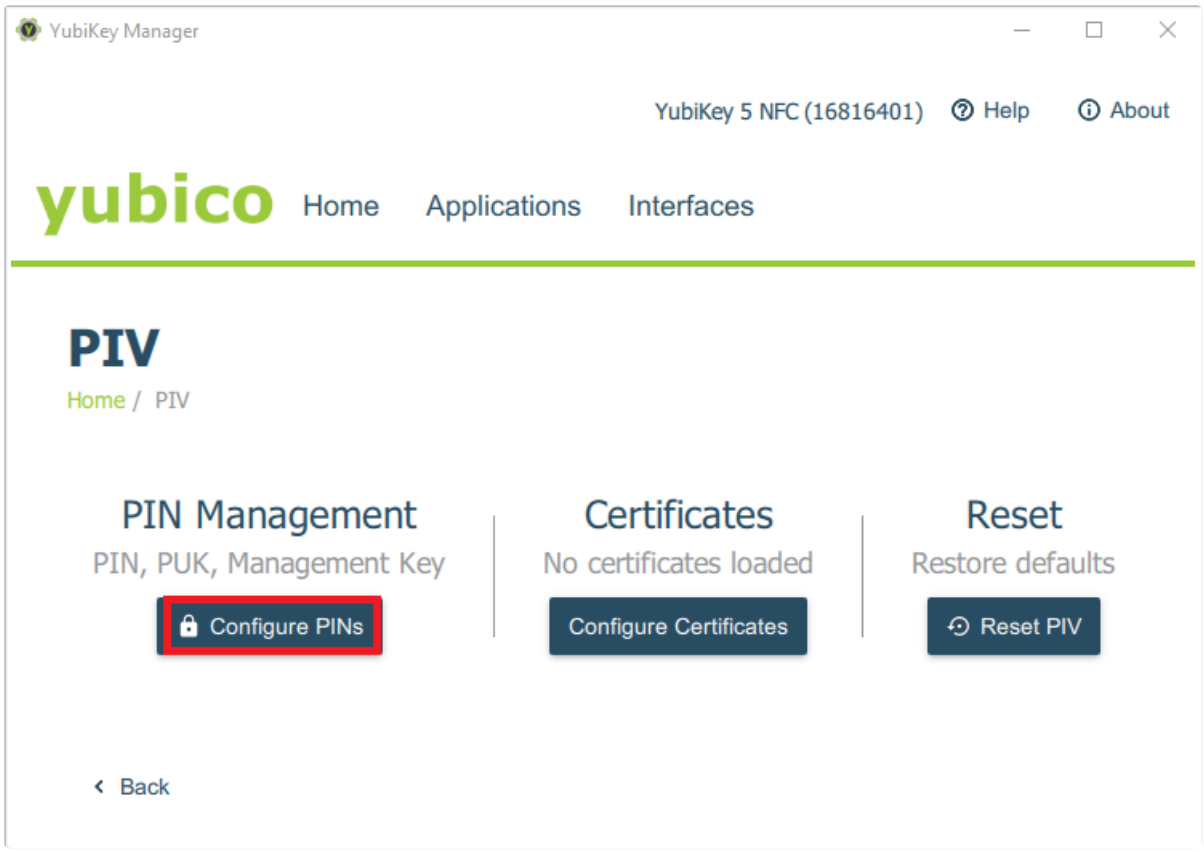
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



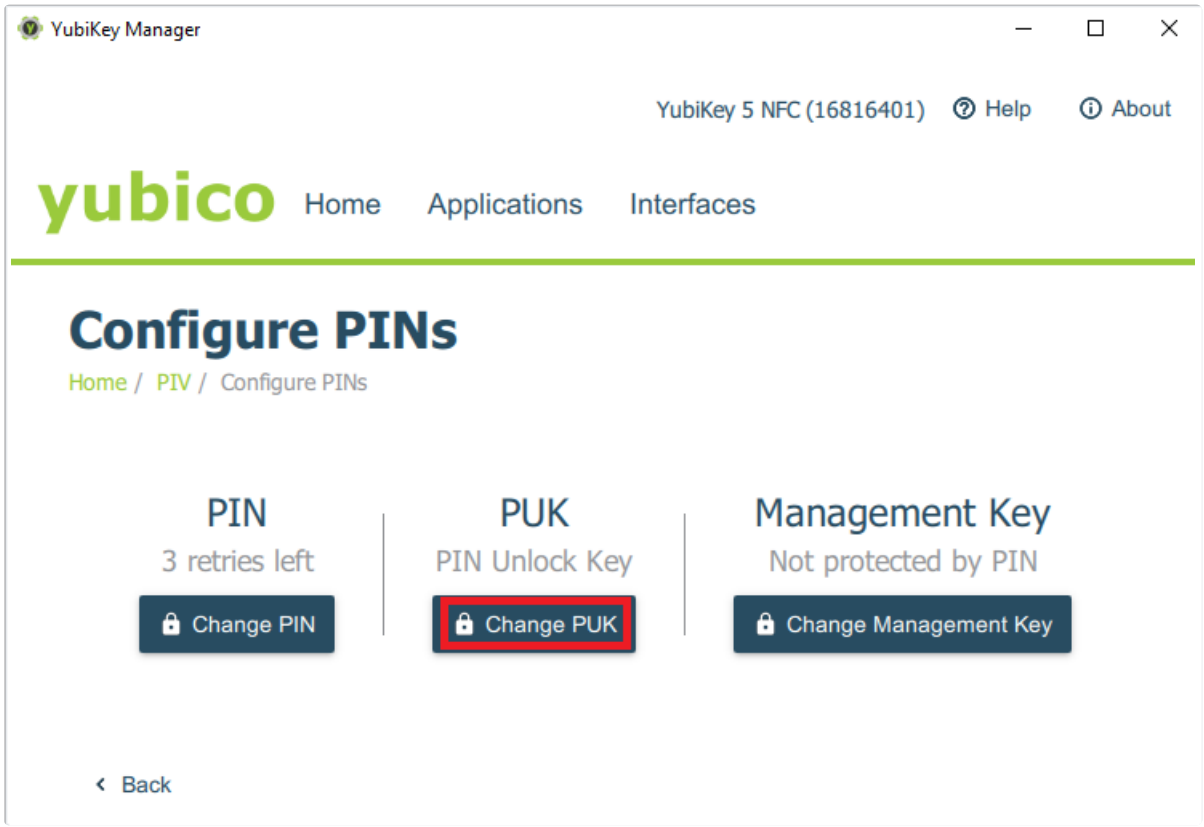
2. Zvolíme volbu *PIV*.



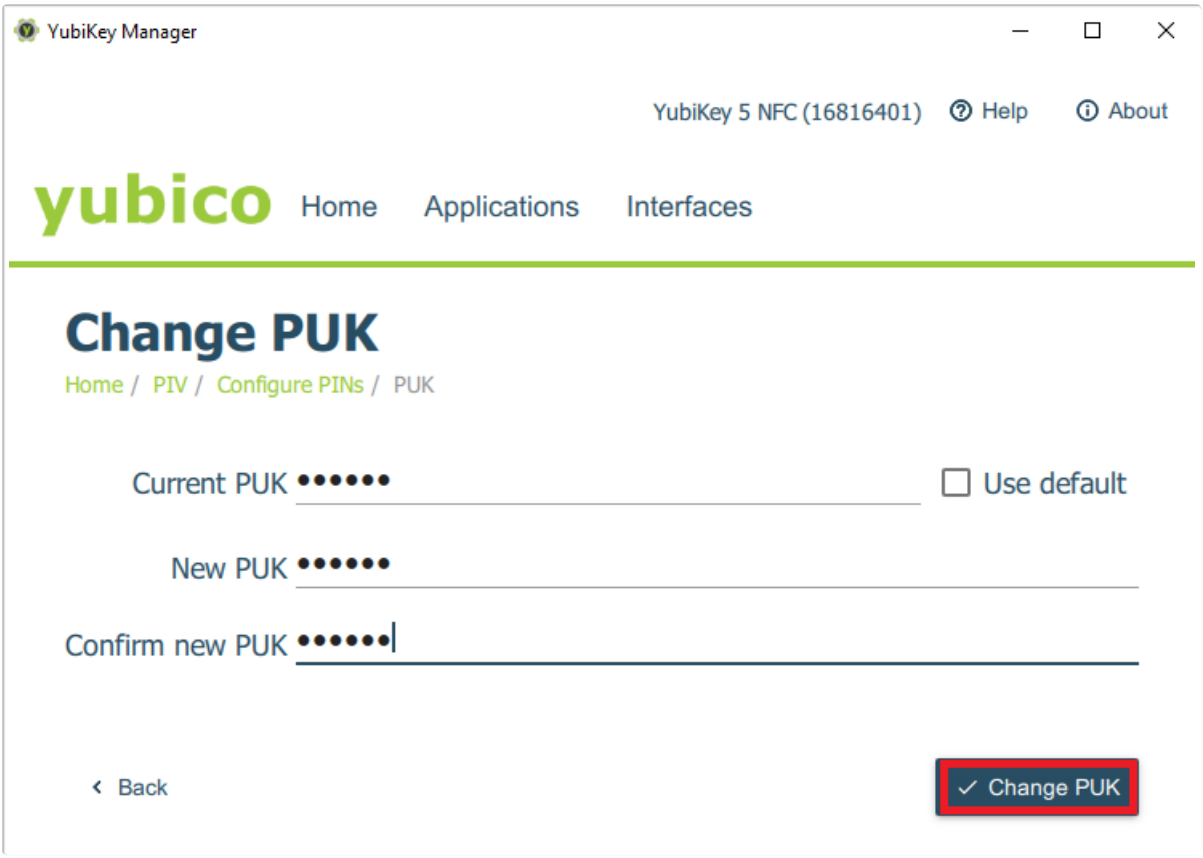
3. Klikneme na *Configure PINs*.



4. Klikneme na *Change PUK*.

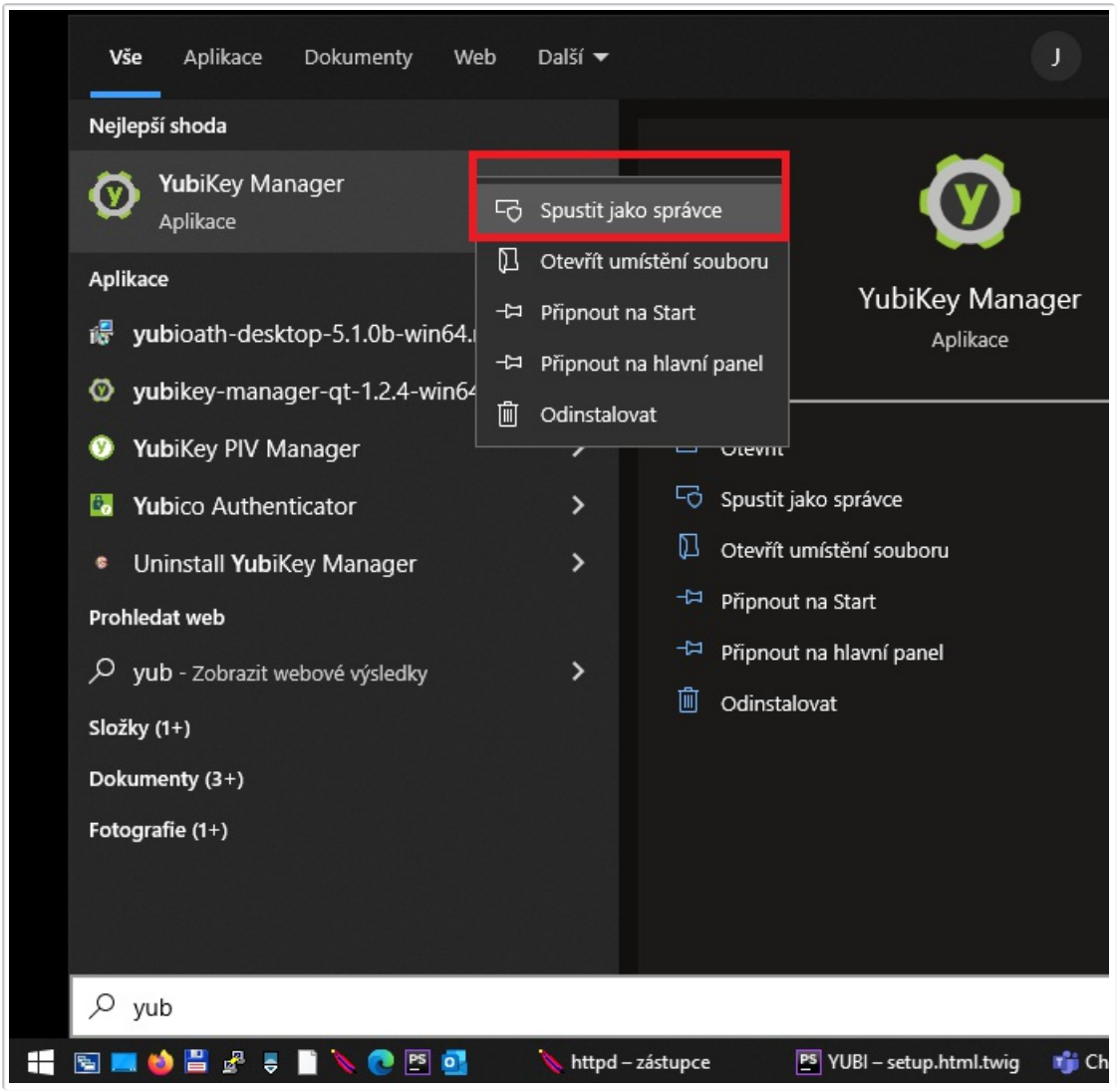


5. Do pole *Current PUK* zadáme defaultní PUK (nebo zaškrtneme volbu *Use default*), nový PUK (6-8 alfanumerických znaků) zadáme do pole *New PUK* a potvrdíme v poli *Confirm new PUK*. Pomocí tlačítka *Change PUK* změnu uložíme.

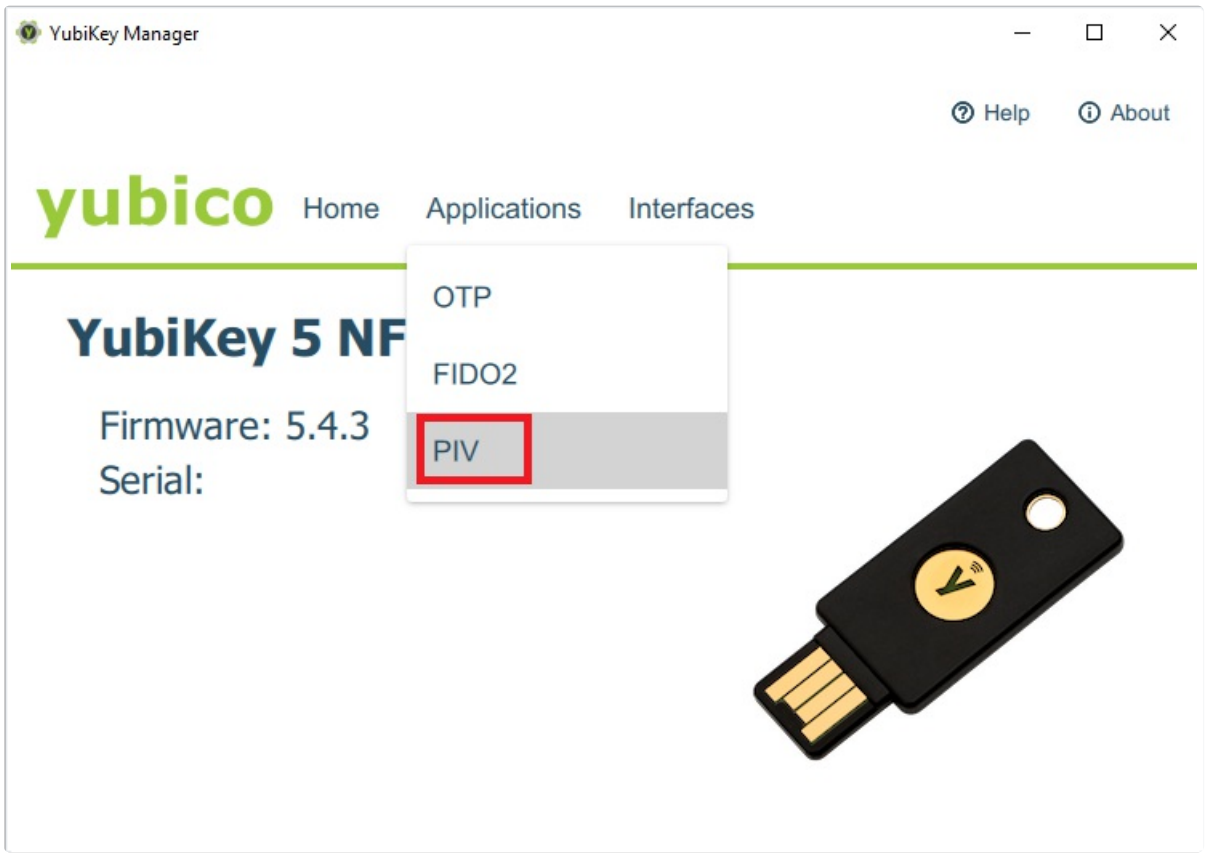


Změna továrního PIV Management Key v YubiKey Manageru

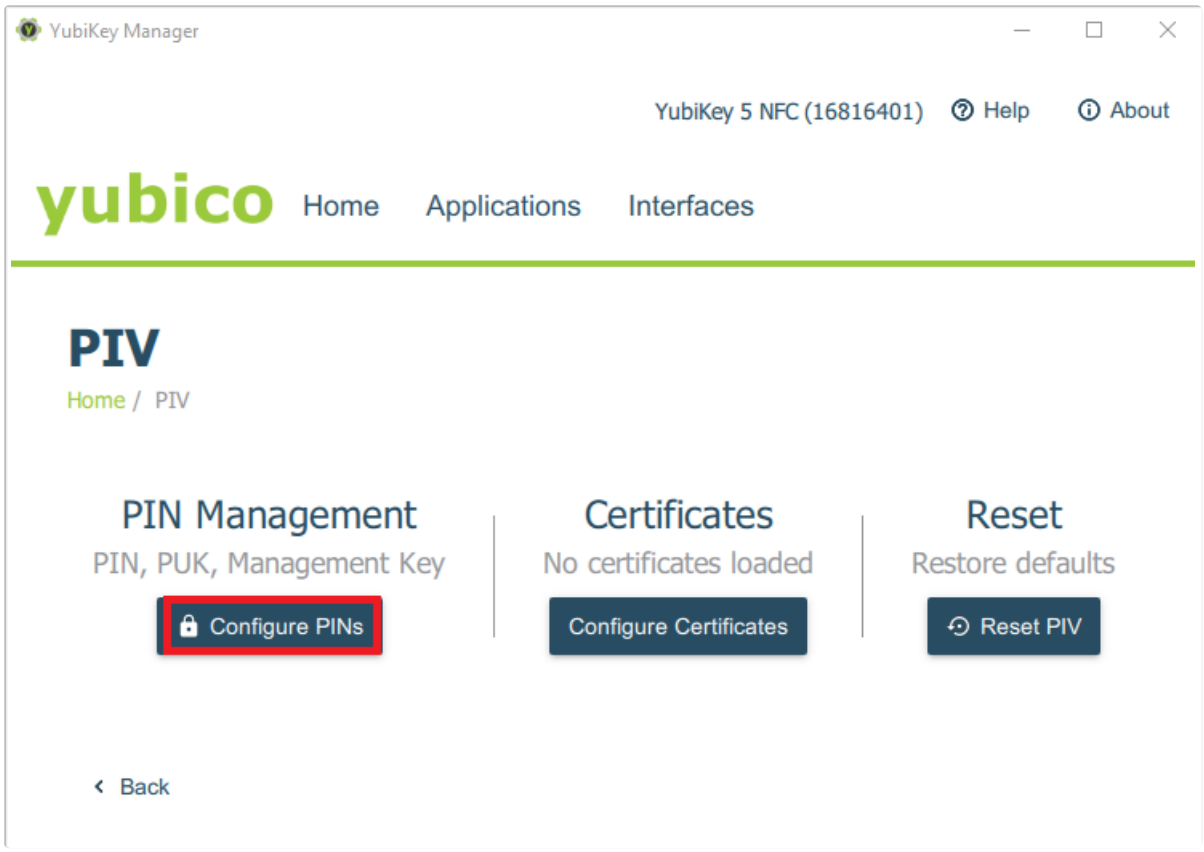
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



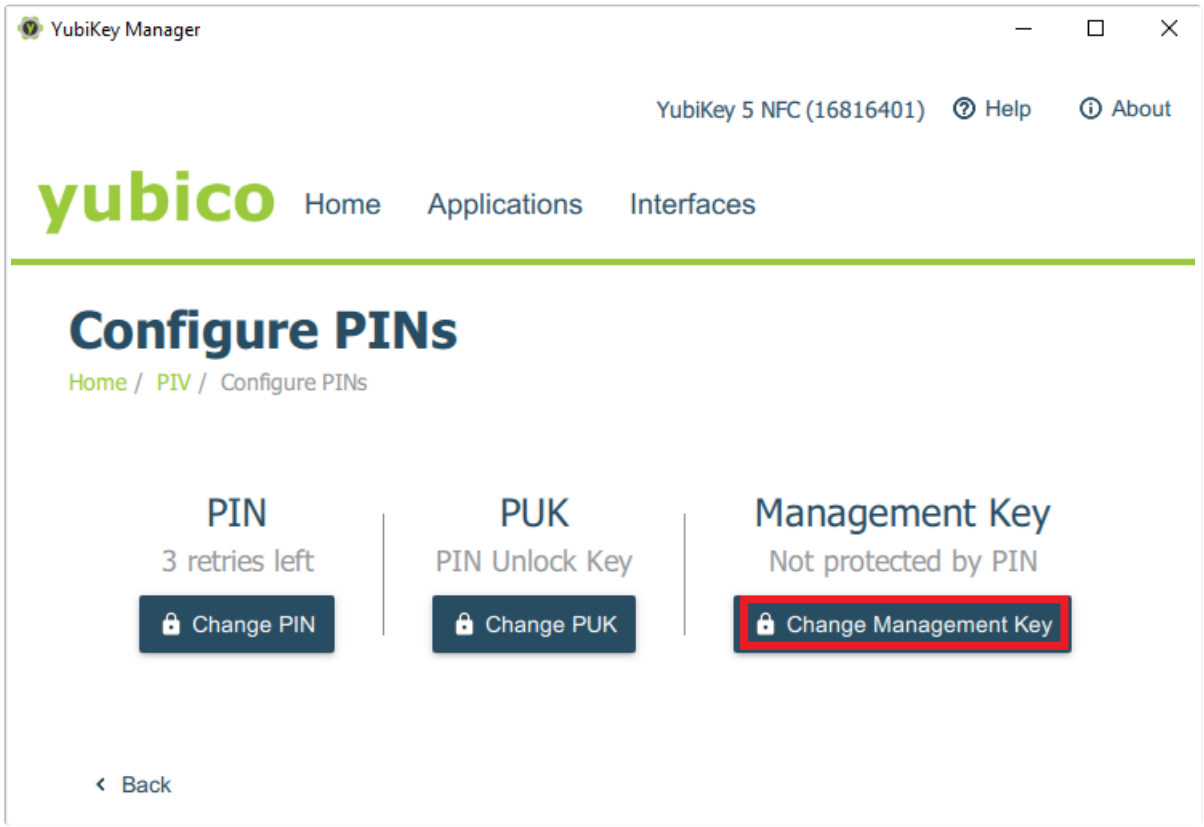
2. Zvolíme volbu *PIV*.



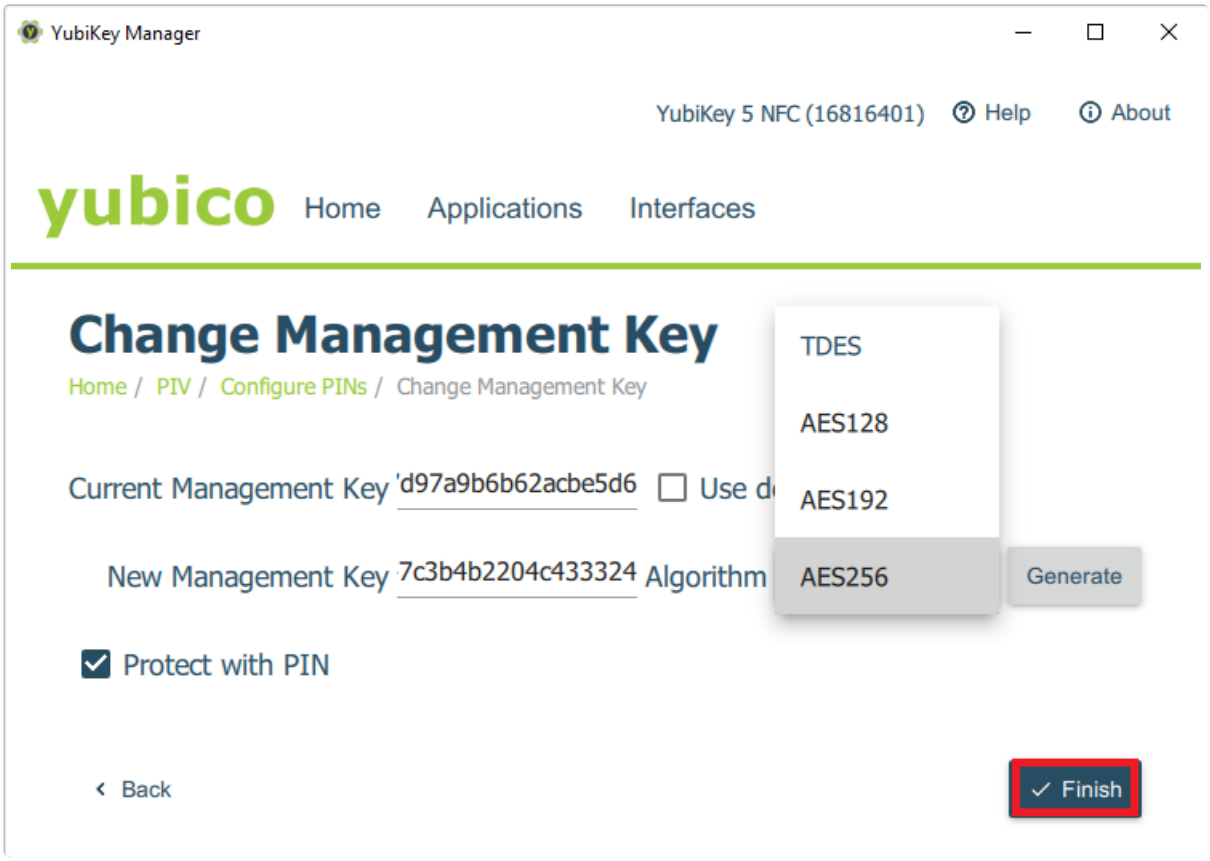
3. Klikneme na *Configure PINs*.



4. Klikneme na *Change Management Key*.

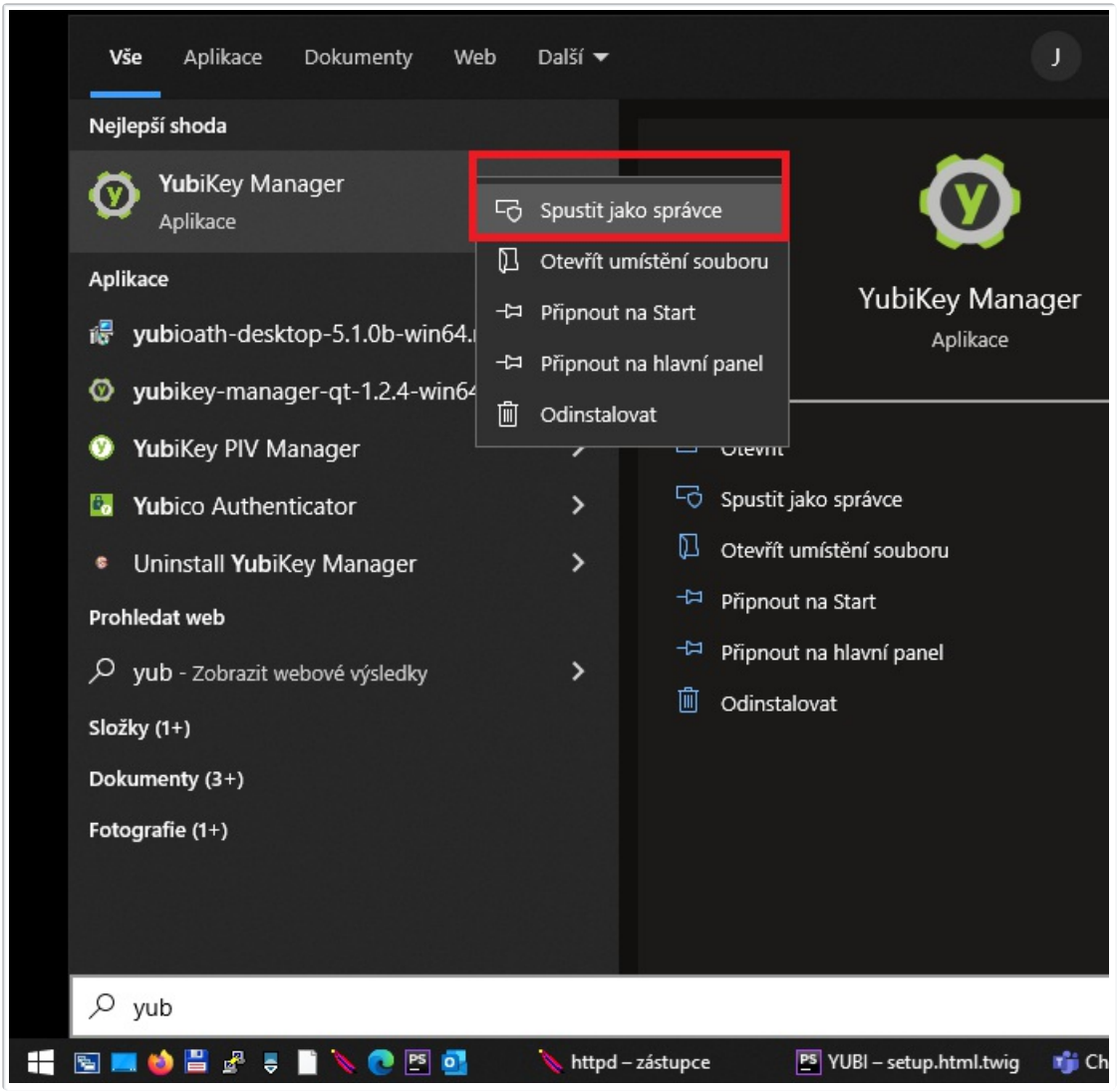


5. Do pole *Current Management Key* zadáme defaultní Management Key (nebo zaškrtneme volbu *Use default*), nový Management Key (48 hexadecimálních znaků) zadáme do pole *New Management Key*, případně pomocí tlačítka *Generate* si necháme klíč vygenerovat - ve volbě *Algorithm* si můžeme vybrat algoritmus, kterým má být klíč vytvořen. Pokud chceme změnu tohoto klíče zabezpečit PIV PINem, zaškrtneme volbu *Protect with PIN*. Pomocí tlačítka *Finish* změnu uložíme.

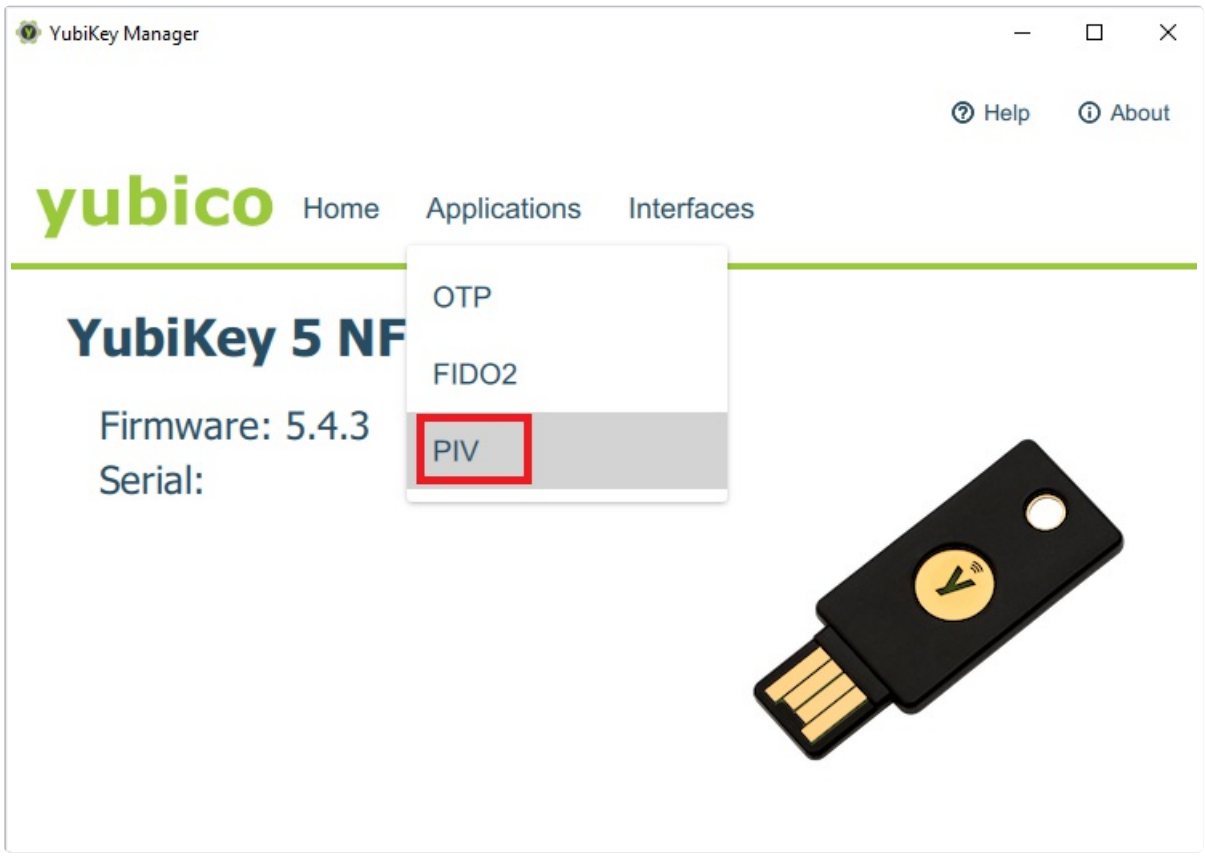


Vygenerování Authentication certifikátu v YubiKey Manageru

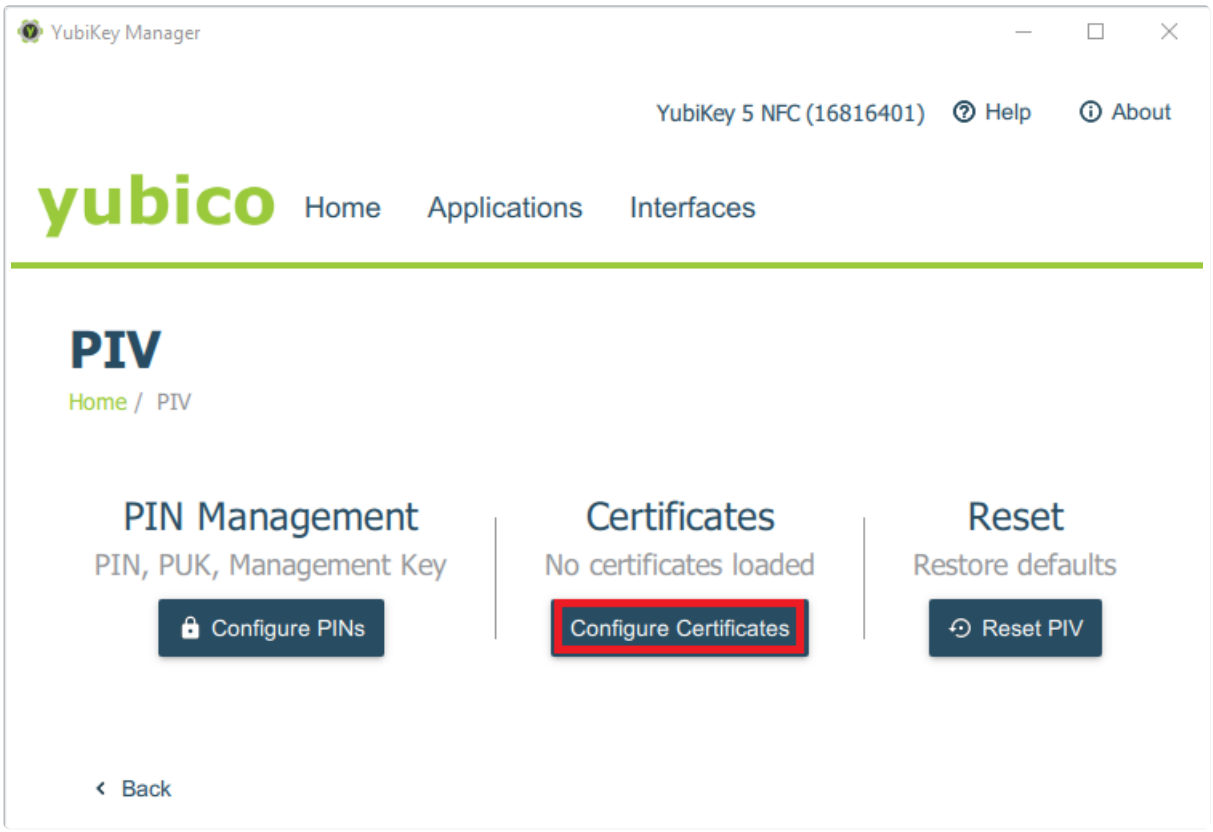
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



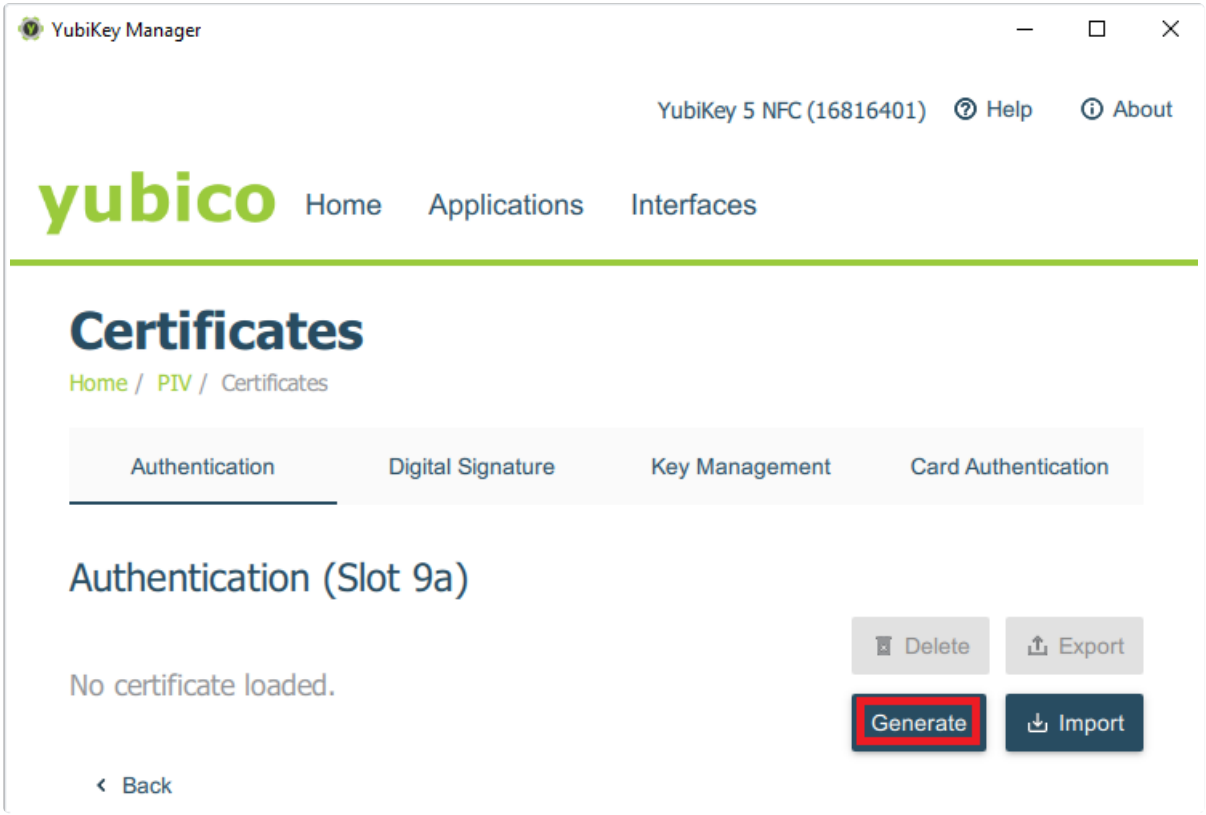
2. Zvolíme volbu *PIV*.



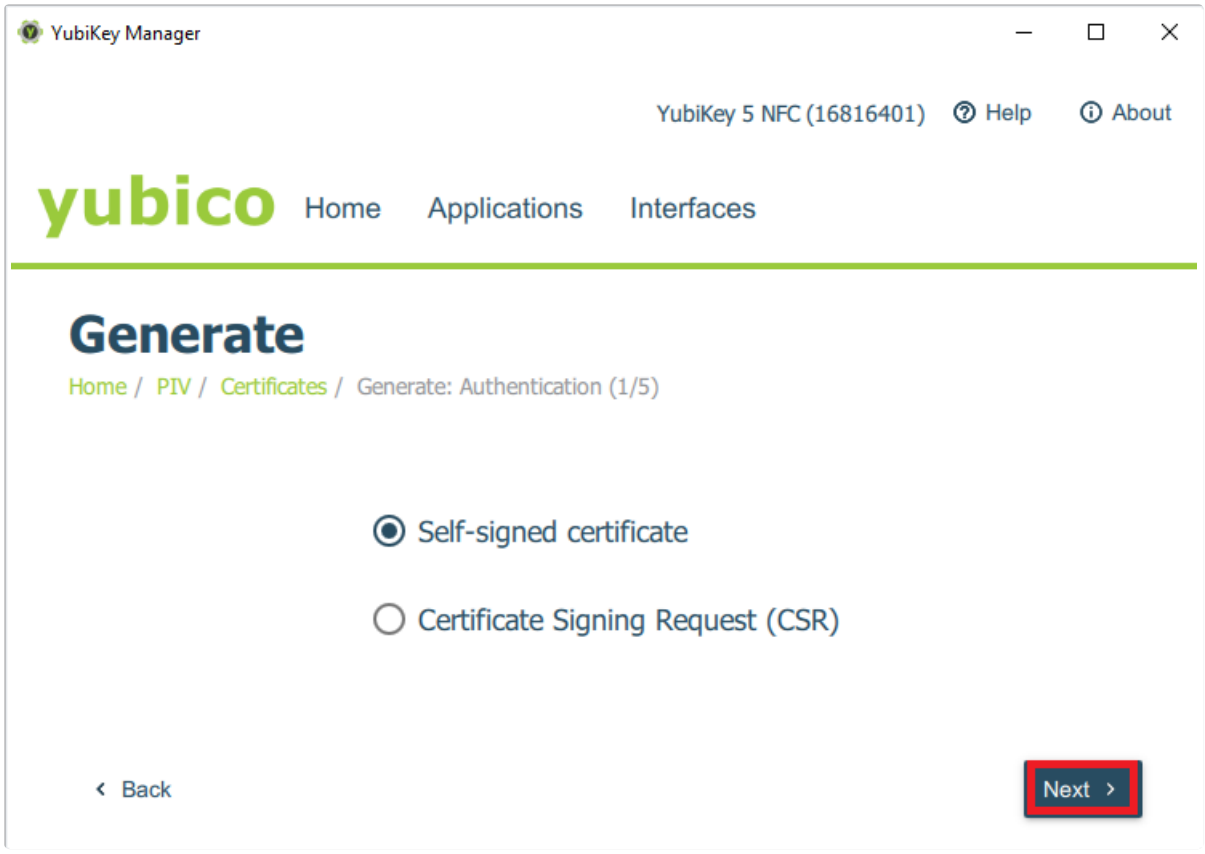
3. Klikneme na *Configure Certificates*.



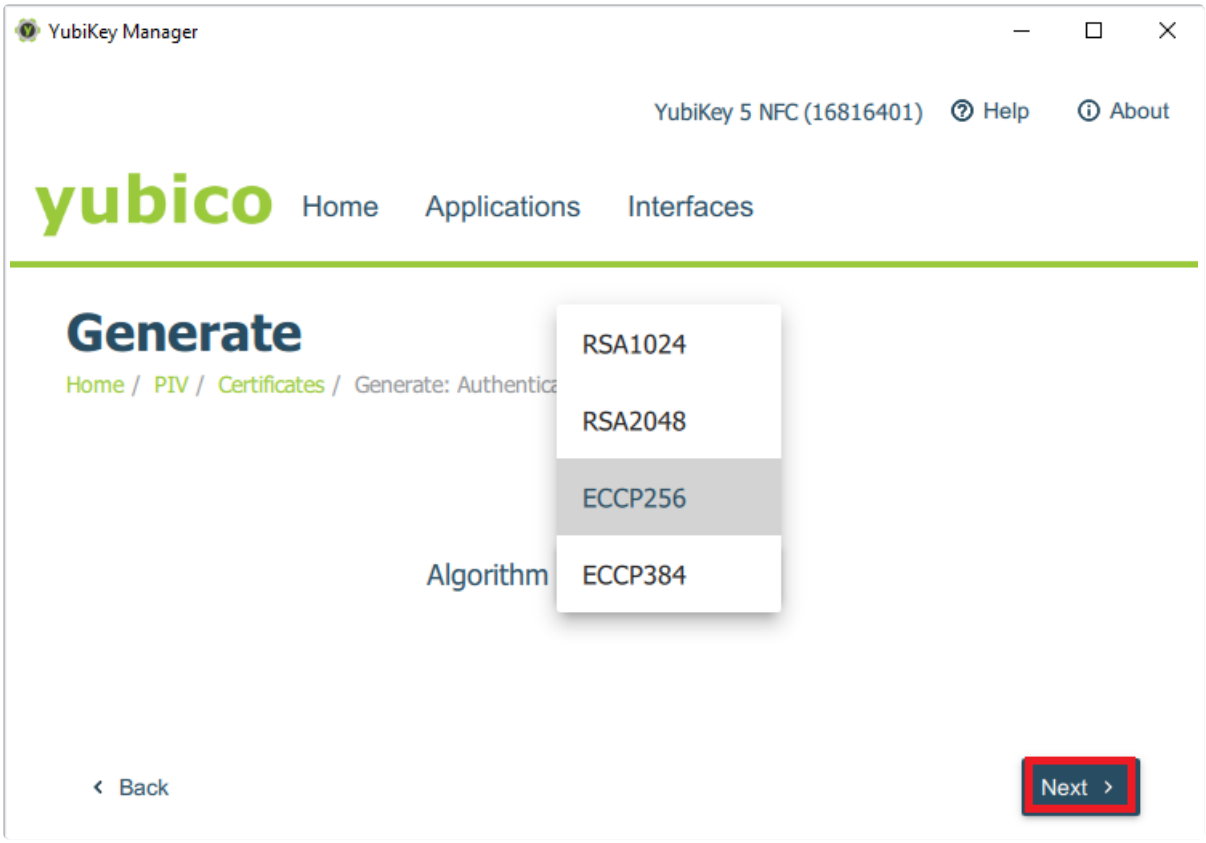
4. Vybereme *Authentication (Slot 9a)* certifikát a klikneme na *Generate*.



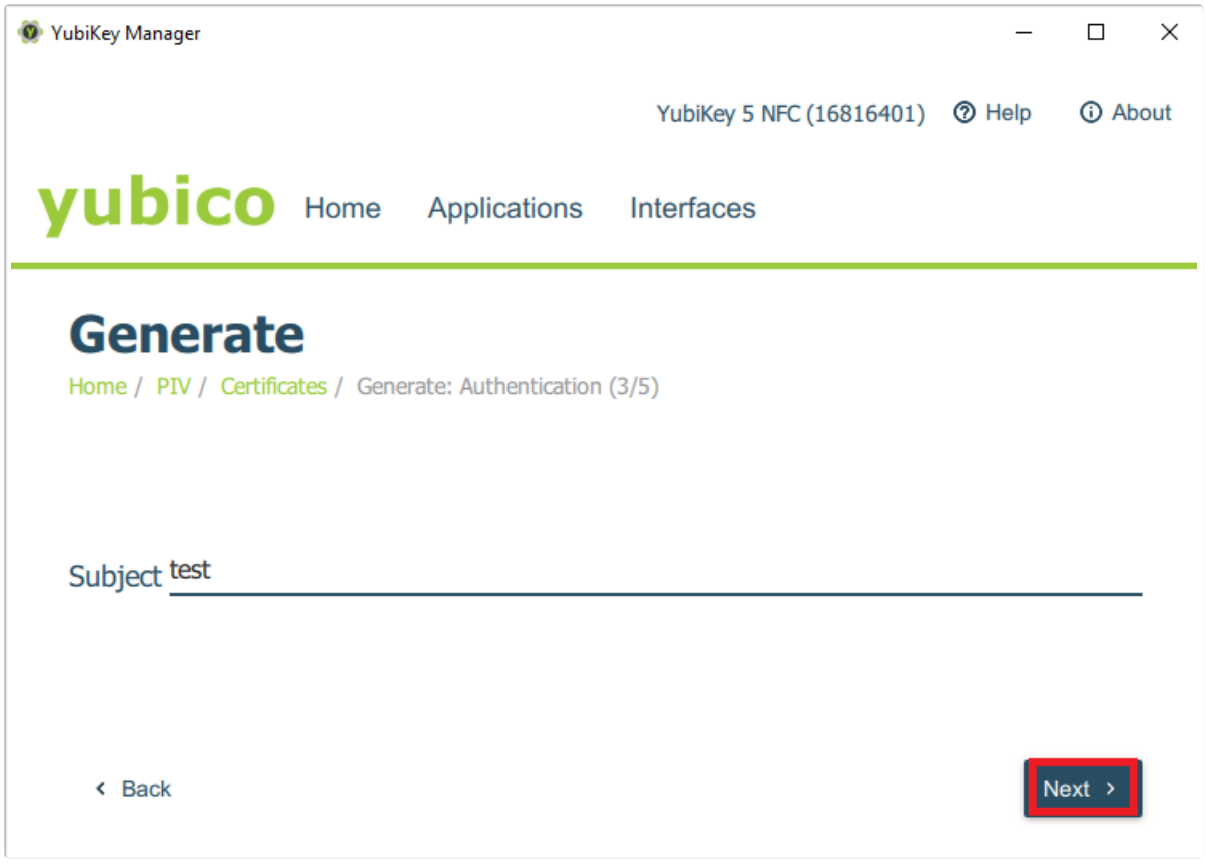
5. Vybereme *Self-signed certificate* a klikneme na *Next*.



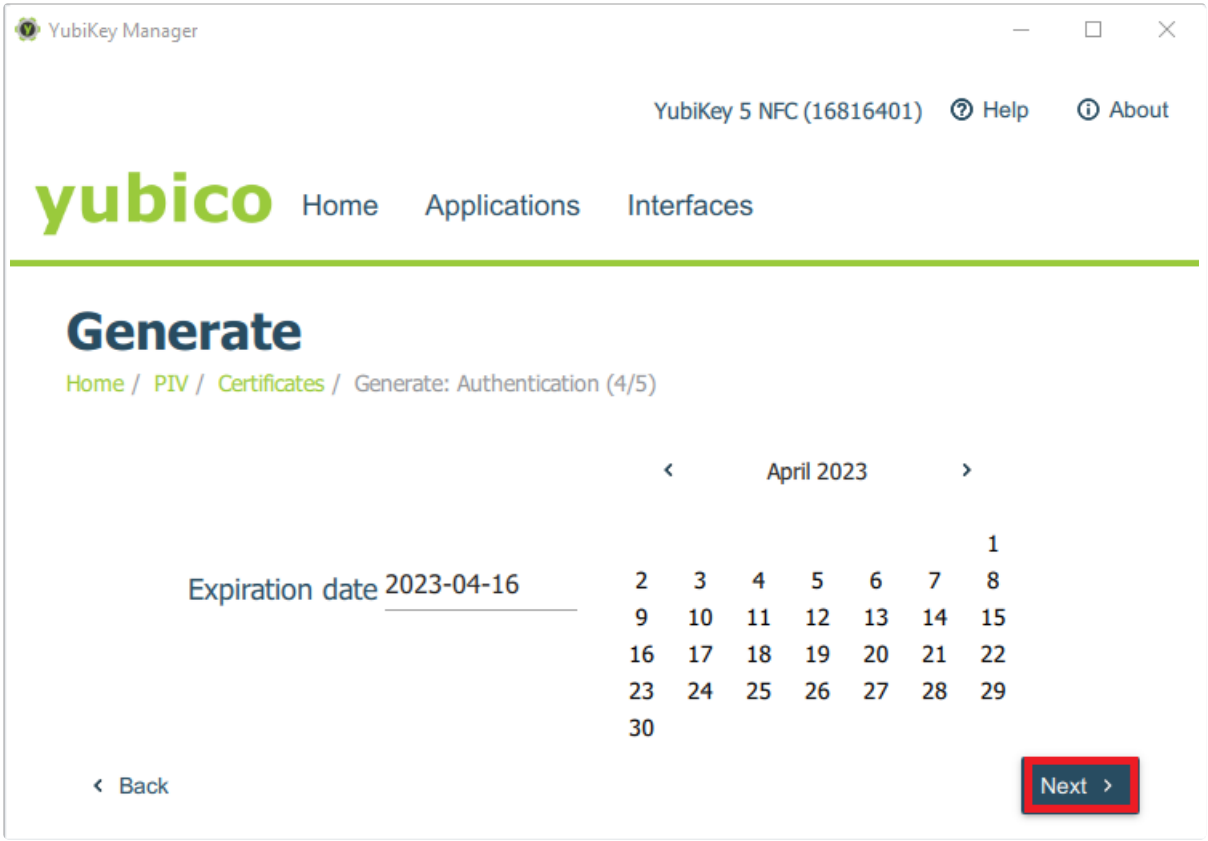
6. Vybereme *algoritmus* generování a klikneme na *Next*.



7. Zvolíme si *Subject* (ideálně vaše emailová adresa) a klikneme na *Next*.



8. Zvolíme datum expirace *Expiration date* a klikneme na *Next*.



9. Shrnutí potvrdíme tlačítkem *Generate*.

Často kladené dotazy

Lze na token uložit kvalifikovaný certifikát?

Bohužel zatím nikoliv.

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

Nikoliv, ale některé správce hesel podporují dvoufaktorové přihlašování a pomocí YubiKey 5 Nano lze zabezpečit přihlašování.

Lze na token uložit soubory?

Nikoliv, YubiKey 5 Nano není flash disk. Na token lze uložit pouze certifikáty a samozřejmě další data, které vyžadují podporované protokoly (např. OTP seed).

Lze na token uložit nějaké kryptoměny?

Nikoliv, YubiKey 5 Nano není kryptopeněženka. Pomocí YubiKey 5 Nano lze ale zabezpečit přihlašování do kryptoměnových burz, které podporují dvoufaktorové přihlašování pomocí bezpečnostního tokenu.

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 5 Nano jsem připojil(a) k zařízení, které mám připojené k PC a disponuje také USB portem. YubiKey 5 Nano ale nefunguje jak má.

Připojte YubiKey 5 Nano 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.