YubiKey 5C NFC používateľská príručka

verzia 1.00



Univerzálny bezpečnostný token s rozhraním USB-C a NFC čipom, podporujúci protokoly **FIDO2 (bezheslové overovanie)**, **OTP**, **PIV (Smart Card)** a **OpenPGP**. Pomocou neho môžete maximálne zabezpečiť svoj e-mail, sociálne siete, kryptomenovú burzu alebo prístup k počítaču. Jediným dotykom prsta prakticky eliminujete hrozbu phishingových útokov.

Popis YubiKey 5C NFC

Čo je to YubiKey

YubiKey sú univerzálne bezpečnostné tokeny vyrobené švédskou spoločnosťou Yubico. Najčastejšie sa používajú na
zabezpečenie prihlasovania do služieb a aplikácií na internete (napríklad emailové služby, sociálne siete, kryptomenové zmenárne) a to pomocou dodatočného stlačenia tlačidla, ktorým je token vybavený. Ak daná služba
podporuje tokeny YubiKey ako tzv. "druhý faktor overenia", útočníci nemajú šancu nabúrať sa k dátam používateľa
(emaily, fotky, kryptomeny). V opačnom prípade možno informácie odcudziť a to pomocou jednoduchých alebo
sofistikovaných techník, ktoré môžu prekvapiť aj profesionálnych používateľov internetu. Stačí, aby si útočník vybral
vhodnú chvíľu na útok.

Dnes stále populárne SMS kódy s obmedzenou platnosťou, ktoré musí používateľ prepisovať do prihlasovacieho formulára,
sú jednou z mnohých obľúbených overovacích metód. Bohužiaľ všetky tieto staršie metódy sú úplne bezradné proti útočnej technike zvanej "phishing". Spoľahlivým nástupcom sú bezpečnostné tokeny a špecializované aplikácie v mobilnom telefóne (často už využívané niektorými bankami). Bezpečnostné tokeny však na rozdiel od
mobilných aplikácií nepotrebujú na svoje fungovanie telefón, nemusia sa inštalovať a aktualizovať a sú opätovne použiteľné pre ľubovoľné množstvo služieb, nielen pre jednu konkrétnu.

YubiKey tokeny podporujú niekoľko spôsobov moderného overovania (alebo "autentizácie"), vždy záleží na konkrétnej službe, aký variant protokolu FIDO2 ponúkne.



Silný druhý faktor
Používateľ zadáva meno a heslo a potom potvrdzuje stlačením tlačidla na tokene



Silný multi-faktor
Používateľ zadáva meno a heslo, potom odomyká token PINom a potvrdzuje stlačením jeho tlačidla



Bezheslové overovanie
Používateľ bez zadania prihlasovacích údajov rovno odomyká token PINom, potvrdzuje stlačením jeho tlačidla

YubiKey modely sa od seba mierne líšia, v prvom rade konektorom, ktorým sa pripájajú k počítačom, notebookom či tabletům a potom tiež drobne funkčnou výbavou a princípom potvrdzovania. Tomu tiež zodpovedá odlišná cena.

V čom sa Yubikey líši od ostatných tokenov

Na trhu je k dispozícii celý rad produktov od rôznych výrobcov. Vzhľadom na to, že užívateľ zabezpečuje svoje súkromie a citlivé dáta, mal by si zodpovedať na nasledujúce otázky:

- Chcem si tokenom zabezpečiť čo najväčší počet služieb a aplikácií?
- Chcem mať istotu, že token, na ktorom bude závisieť moja bezpečnosť, nemá zadné vrátka, ktoré sa dajú zneužiť?
- Potrebujem, aby token fungoval za každého počasia a bol vyrobený z overených a kvalitných čipov a súčiastok?
- Keď už investujem čas a úsilie do používania bezpečnostného tokenu, existuje nejaké ďalšie jeho využitie?

Pre užívateľov, ktorí si na všetky tieto otázky odpovedia "**áno**", neexistuje iná voľba než tokeny YubiKey.

Ďalšie funkcie YubiKey tokenov

- Zabezpečenie prihlasovania k počítačom, notebookom, tabletom a serverom
- Zabezpečenie prihlasovania do VPN a vzdialenej plochy
- Uchovávanie privátnych kľúčov pre šifrovanie, dešifrovanie a podpisovanie dokumentov
- Fyzický prístup do budovy, kde YubiKey nahradí vstupnú kartu
- Ľahko nasaditeľné riešenie pre firmy, ktorým sa výrazne znížia náklady na prevádzku a zjednodušia sa procesy spojené s prihlasovaním používateľov ako napríklad obnovenie hesla, registrácia nových používateľov alebo rozlišovanie úrovne prístupov pre jednotlivých zamestnancov

Čísla a fakty

- 9 z 10 top IT firiem na svete zaviedlo YubiKey tokeny na overovanie svojich zamestnancov (Google, Facebook, Microsoft)
- Spoločnosť Yubico založená v roku 2007 je spoluautorom štandardu U2F (Universal 2nd Factor) a protokolu
- CTAP v rámci FIDO Alliance a štandardu WebAuthn v rámci konzorcia W3C S YubiKey je proces overovania 4x rýchlejší v porovnaní so SMS a OTP kódmi
- Firmám, ktoré zaviedli YubiKey, klesol počet incidentov spojených s heslami v priemere o 92%

Čo YubiKey token naopak nie je?

YubiKey nie je flash disk. Nie je možné naň nahrávať používateľské súbory (fotky, videá, hudbu, dokumenty).
YubiKey nie je ani kryptopeňaženka a nie je v ňom možné držať ani bitcoin, ani iné kryptomeny.

Princíp potvrdzovania

YubiKey 5 NFC disponuje kovovým tlačidlom, ktoré používateľ stlačí a tým potvrdí vykonávanú operáciu (nemusí byť vždy vyžadované). Token rozlišuje medzi dlhým a krátkym stlačením. Tlačidlo je čisto mechanické, odtlačok prsta sa nesníma. Okrem stlačenia tlačidla používateľ zadáva aj číselný PIN, ak je to potrebné (analógiou je platobná karta pri výbere z bankomatu).

Technické parametry

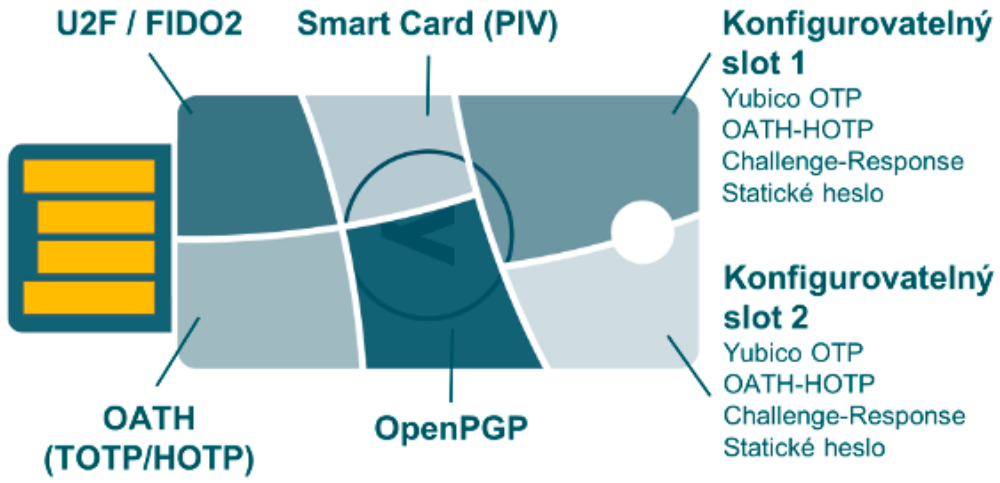
Základné parametre	
Názov produktu	YubiKey 5C NFC
Rozhranie	USB 2.0 (USB-A), NFC
Princíp potvrdzovania	Mechanický dotyk tlačidla
Funkcionalita	
Autentifikačné metódy	Passwordless, Strong Two Factor, Strong Multi-Factor
Funkcie	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F), Smart card (PIV-compatible), Yubico OTP, OATH – HOTP (Event), OATH – TOTP (Time), Open PGP, Secure Static Password
Certifikácie	FIDO2 Certified, FIDO Universal 2nd Factor (U2F) Certified

Kryptografia	RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384
Typ zariadenia	FIDO HID Device, CCID Smart Card, HID Keyboard

Technické vlastnosti	
Stupeň krytia	IP68
Odolnosť	Neobsahuje batérie, neobsahuje pohyblivé časti, vysoká mechanická odolnosť, vodoodolnosť
Farba	Čierna
Rozmery	18 mm × 45 mm × 3,7 mm
Hmotnosť	4 g
Prevádzková teplota	0 °C - 40 °C
Skladovacia teplota	-20 °C - 85 °C
Rozmery balenia	55 mm × 85 mm × 5 mm
Hmotnosť vrátane balenia	8 g
Obsah balenia	1 token

Ďalšie informácie	
EAN	5060408462331
Krajina pôvodu	Vyrobené v USA a Švédsku
Výrobca	Yubico
Záruka	24 mesiacov

Odkazy	
Technický manuál výrobcu „YubiKey 5“ (v angličtine)	Dokumentácia Yubico



Funkce

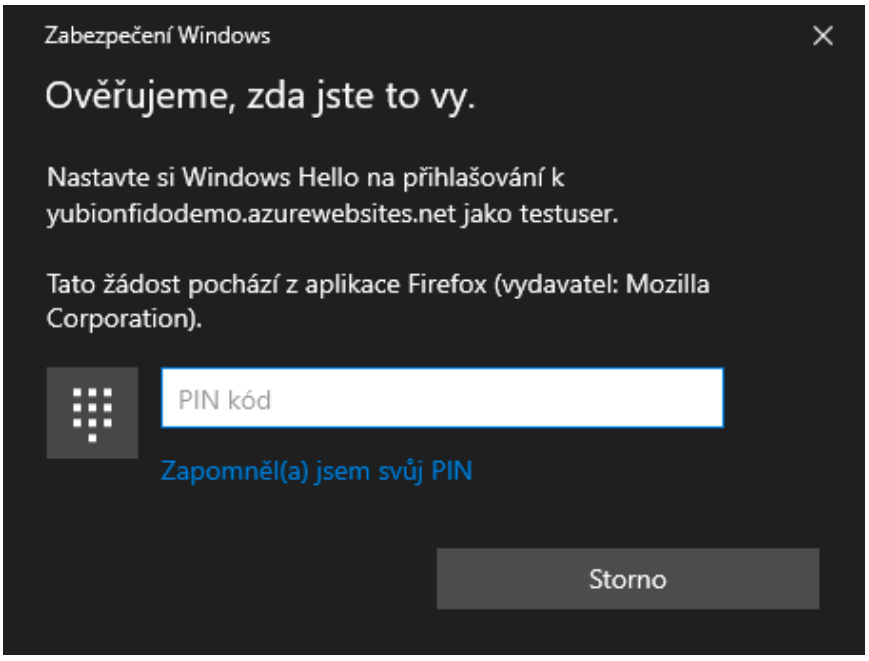
YubiKey 5 NFC disponuje šiestimi oddelenými funkčnými modulmi. Každý modul poskytuje inú funkcionalitu. S počítačom, tabletom alebo telefónom tieto moduly komunikujú cez 3 rozhrania:

- OTP rozhranie sa v počítači hlási ako obyčajná USB klávesnica (HID alebo Human Interface Device). Odoslané dáta tokenom do počítača sú
potom simuláciou stlačení klávesov na virtuálnej klávesnici. Z tohto dôvodu nie je potrebné inštalovať žiadne špeciálne ovládače, podpora je naprieč
platformami.
- FIDO rozhranie sa tiež hlási ako HID klávesnica, avšak je tu navyše potrebná podpora špeciálneho FIDO protokolu. Tou disponujú všetky zariadenia s prehliadačom podporujúcim protokol WebAuthn (na iOS od verzie 13)
- CCID rozhranie dokáže YubiKey premeniť na čítačku smartkariet a aplikácie na tokene sa potom hlásia ako jednotlivé smartkarty. Podpora je na
Windows (s minidriverom) a MacOS, na Linuxe (s PC/SC) a Androide. Na iOS je potrebné Yubico iOS SDK.

FIDO2

FIDO2 projekt predstavuje spoločné úsilie FIDO Alliance a združenia W3C a výsledkom tohto je silný autentizačný protokol, ktorého základy tvoria
štandard WebAuthn (štandardizuje autentizáciu na webe) a protokol CTAP2 (zaisťuje komunikáciu medzi klientom, typicky webovým prehliadačom a
overovacím prostriedkom, napr. bezpečnostným tokenom, pri ktorom je navyše definovaná nutnosť potvrdenia akcie, t. j. napríklad stlačenie tlačidla, zadanie
PINu alebo potvrdenie odtlačku prsta). FIDO2 je nasledovníkom štandardu U2F a je spätne kompatibilný.

FIDO2 prihlasovací proces je konfigurovateľný a záleží na prevádzkovateľovi danej služby, ktorú variantu zvolí. Pre lepšiu predstavu uvádzame niekoľko možných scenárov. Ak máte na svojom Windows PC aktívny Windows Hello, bude na vás pravdepodobne pred výzvou na zapojenie YubiKey vyskakovať výzva, ktorú je potrebné stornovať.

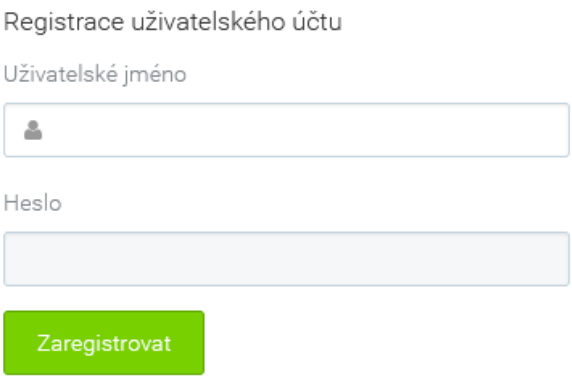


Tradičné 2FA

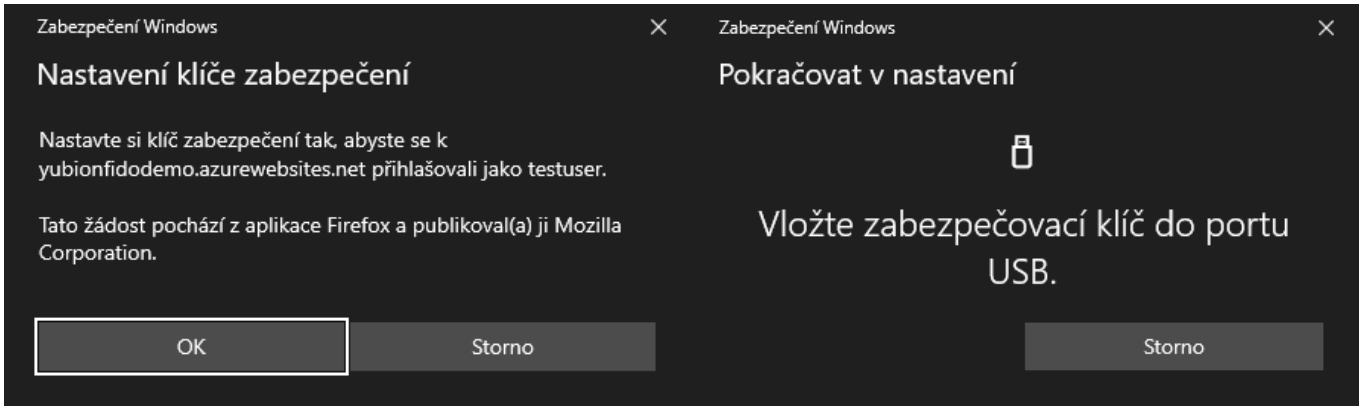
Klasické prihlasovanie s heslom, keď token slúži ako druhý faktor na overenie. Možno vyskúšať demo. Počet spárovaných služieb využívajúcich token týmto
scenárom nie je nijako obmedzený kapacitou tokenu (keďže sa v tokene neukladajú žiadne informácie o službe).

Fáza registrácie

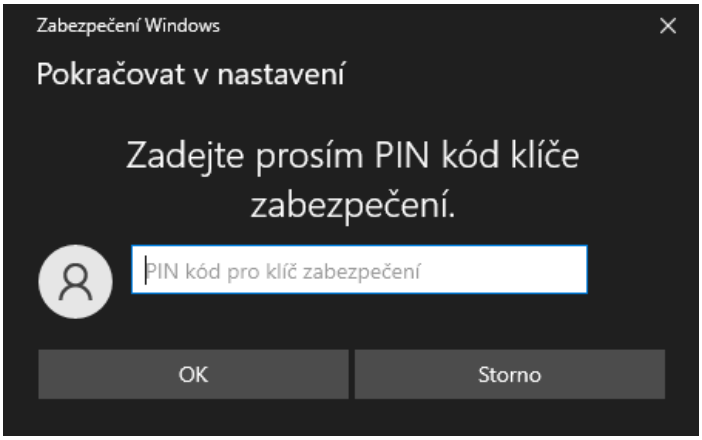
1. Používateľ zvolí používateľské meno a heslo



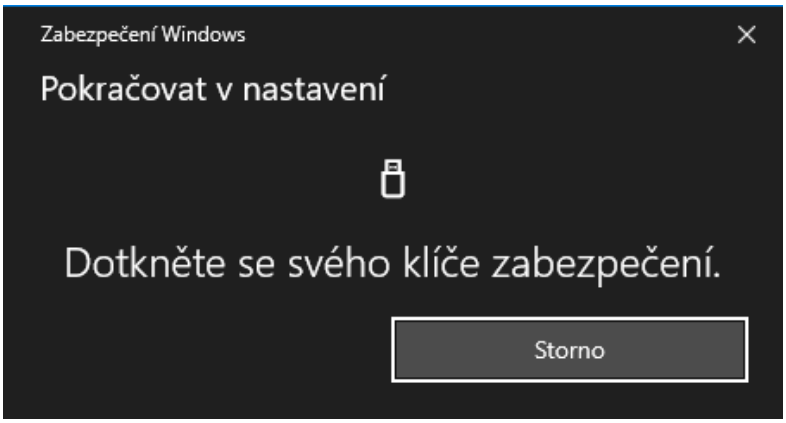
2. Používateľ je vyzvaný, aby pripojil YubiKey



3. Ak má YubiKey nastavený PIN, používateľ je vyzvaný na jeho zadanie (inak sa tento krok preskočí)

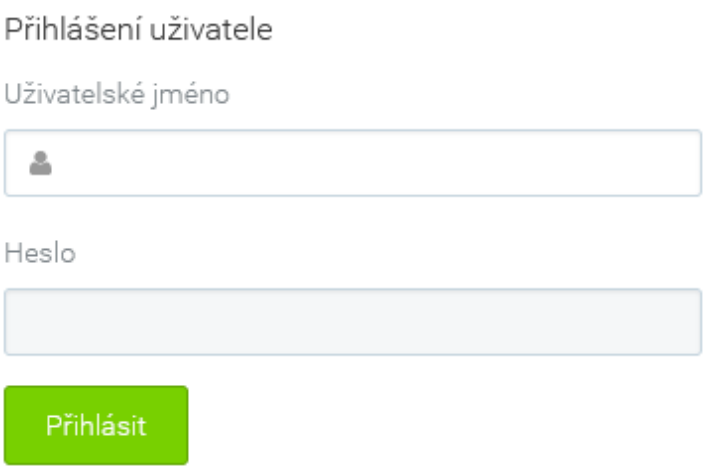


4. Používateľ dokončí registráciu stlačením tlačidla na YubiKey

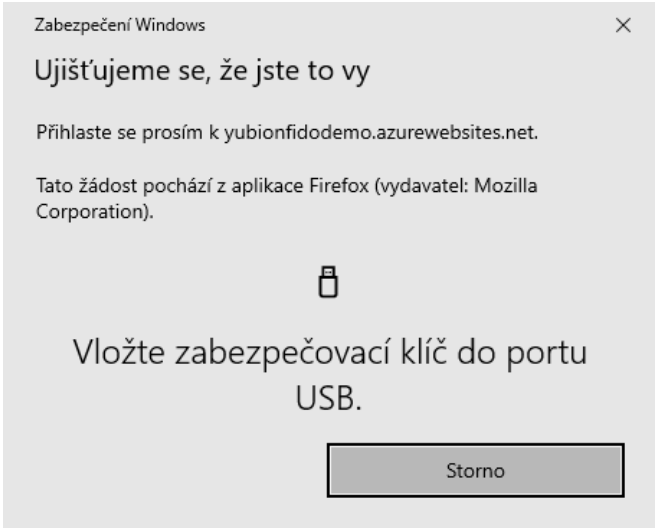


Fáza prihlásenia

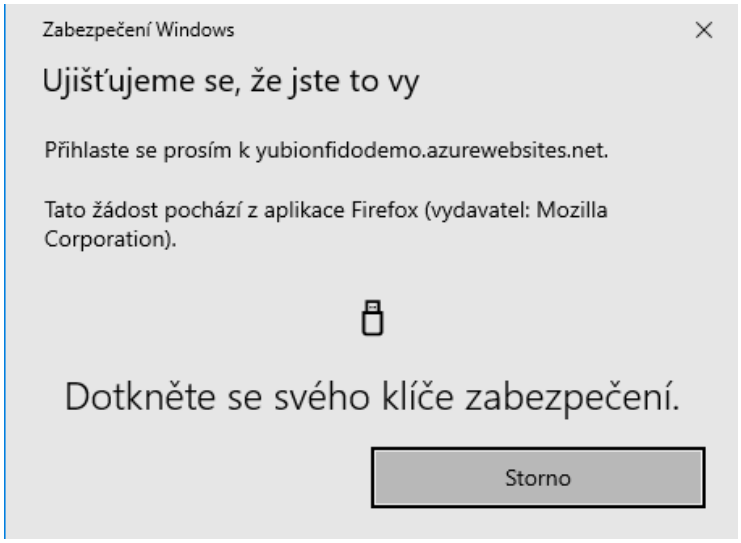
1. Používateľ zadá používateľské meno a heslo



2. Používateľ je vyzvaný, aby pripojil YubiKey



3. Používateľ dokončí prihlasovanie stlačením tlačidla na YubiKey

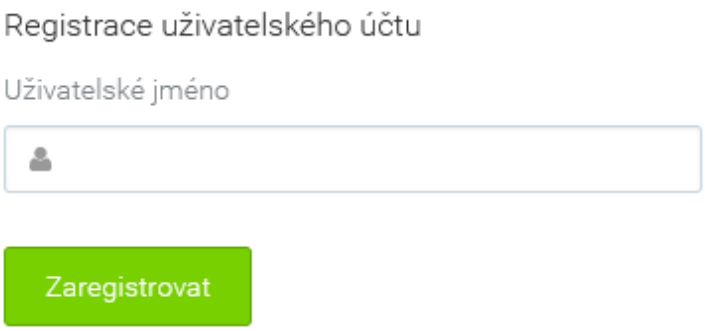


Bezheslové (passwordless) prihlásenie s používateľským menom

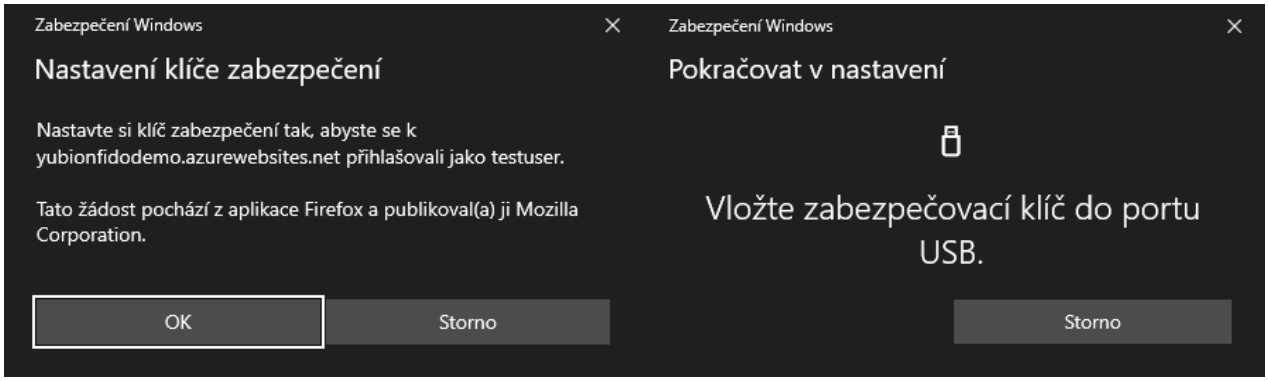
Bezheslové prihlasovanie s používateľským menom, keď token slúži ako druhý faktor na overenie. Možno vyskúšať demo. Počet spárovaných služieb
využívajúcich token týmto scenárom nie je nijako obmedzený kapacitou tokenu (keďže sa v tokene neukladajú žiadne informácie o službe)

Fáza registrácie

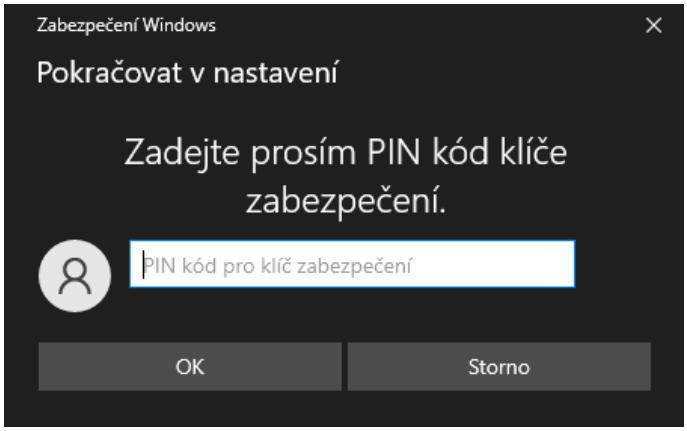
1. Používateľ zvolí používateľské meno



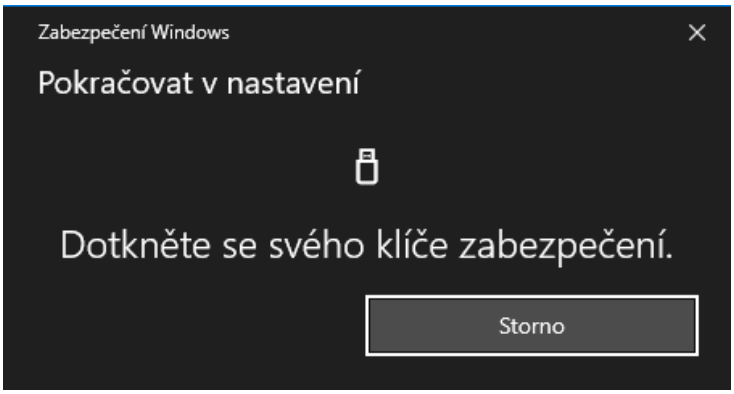
2. Používateľ je vyzvaný, aby pripojil YubiKey



3. Ak má YubiKey nastavený PIN, používateľ je vyzvaný na jeho zadanie (inak sa tento krok preskočí)

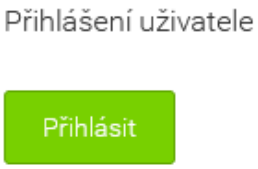


4. Používateľ dokončí registráciu stlačením tlačidla na YubiKey

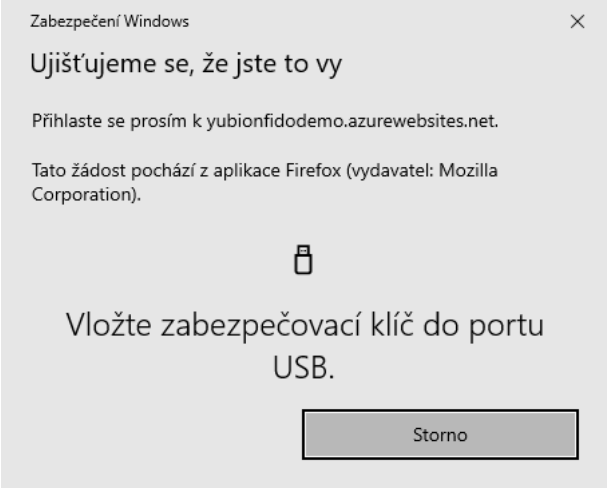


Fáza prihlásenia

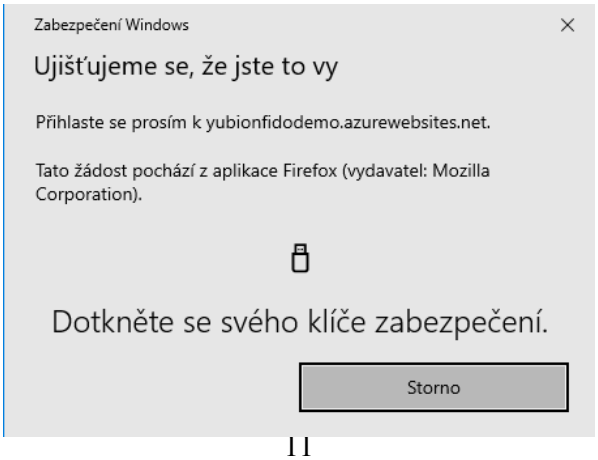
1. Používateľ nezadáva žiadne prihlasovacie údaje a rovno stlačí tlačidlo prihlásiť



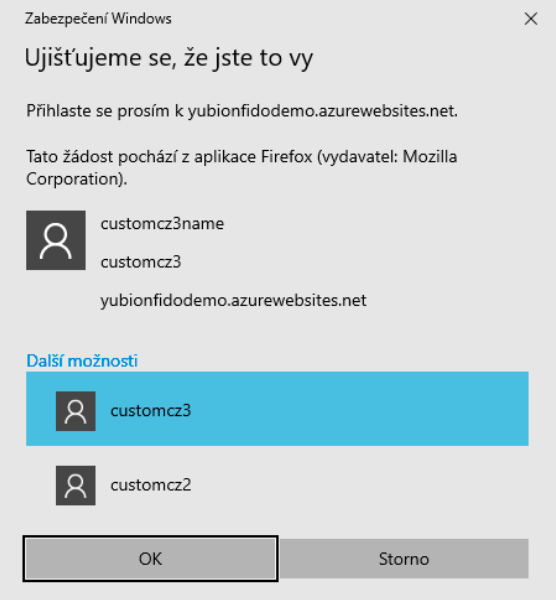
2. Používateľ je vyzvaný, aby pripojil YubiKey



3. Používateľ potvrdí prihlasovanie stlačením tlačidla na YubiKey



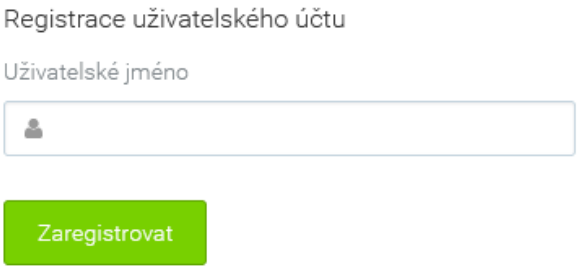
4. Ak existuje viac registrovaných používateľských mien k danému YubiKey, používateľ je vyzvaný na výber jedného z nich (inak sa tento krok
preskočí)



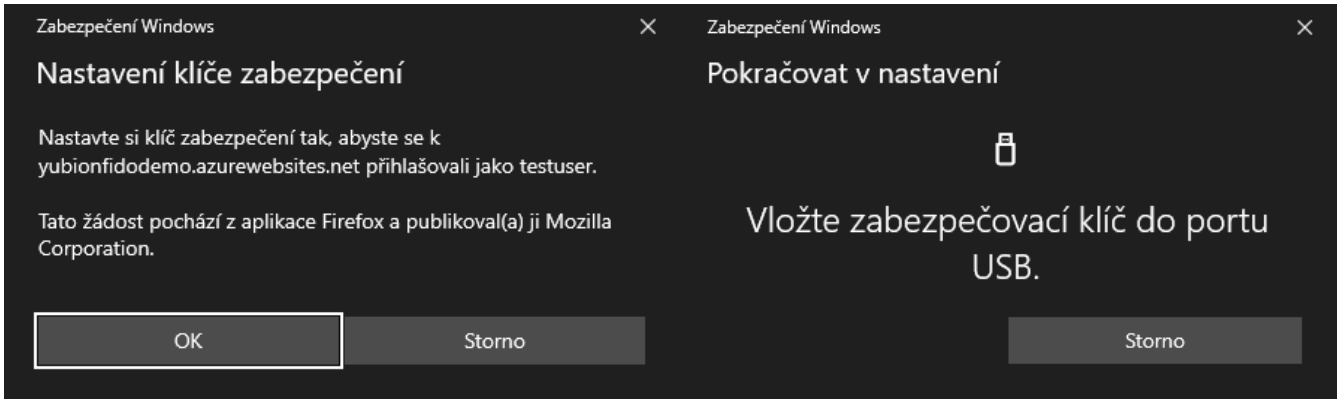
MFA bezheslové (passwordless) prihlásenie s používateľským menom
Bezheslové prihlasovanie s používateľským menom, keď token slúži ako multi-faktor na overenie (zadáva sa aj PIN). Možno vyskúšať demo. Počet
spárovaných služieb využívajúcich token týmto scenárom nie je nijako obmedzený kapacitou tokenu (keďže sa v tokene neukladajú žiadne informácie o službe).

Fáza registrácie

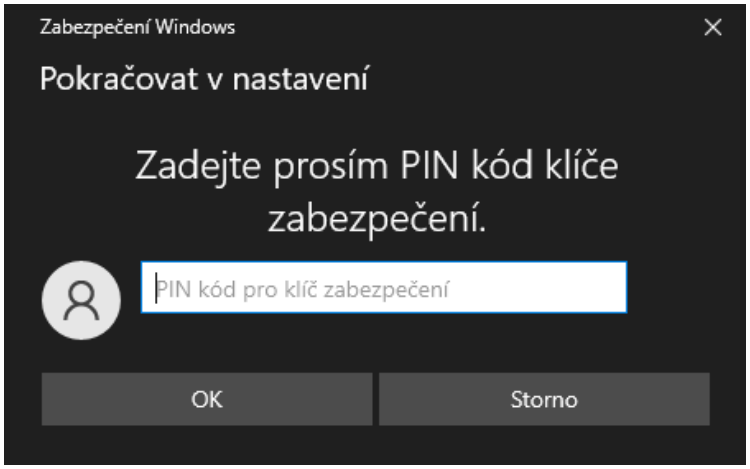
1. Používateľ zvolí používateľské meno



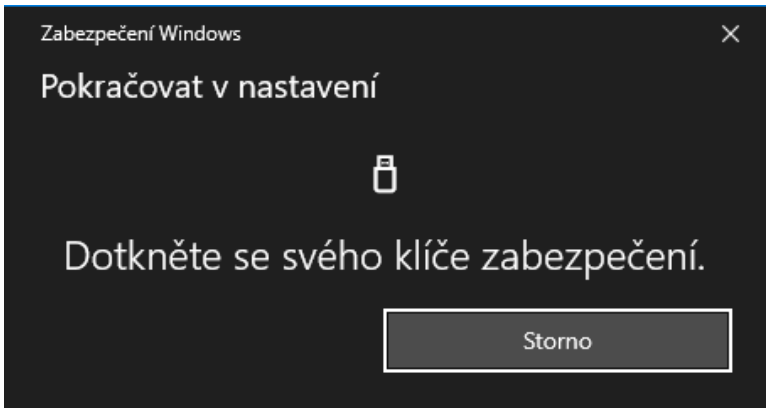
2. Používateľ je vyzvaný, aby pripojil YubiKey



3. Ak má YubiKey nastavený PIN, používateľ je vyzvaný na jeho zadanie, ak nie, je vyzvaný na jeho vytvorenie (vrátane dodatočného stlačenia tlačidla YubiKey)



4. Používateľ dokončí registráciu stlačením tlačidla na YubiKey

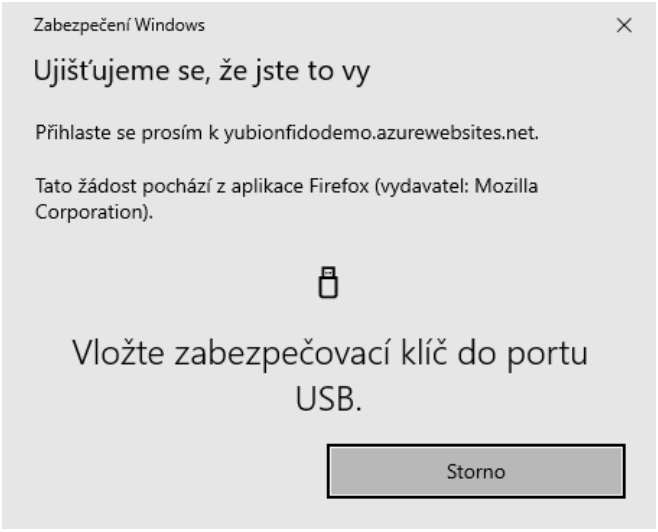


Fáza prihlásenia

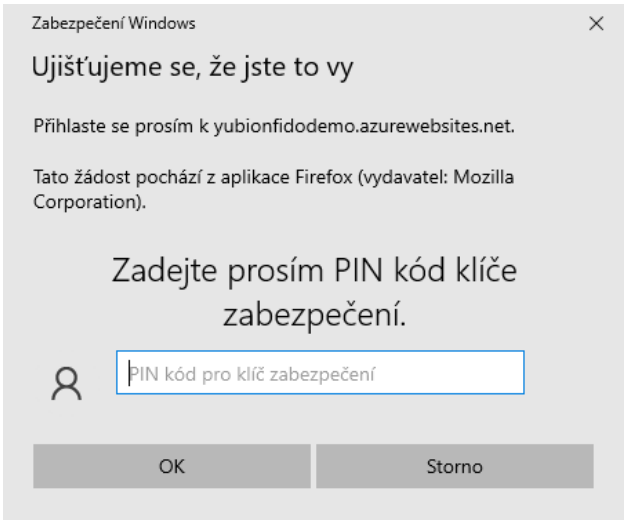
1. Používateľ zadá používateľské meno



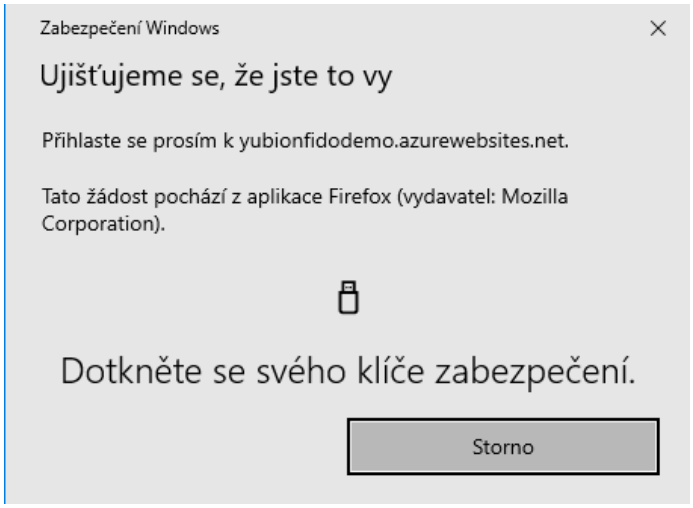
2. Používateľ je vyzvaný, aby pripojil YubiKey



3. Používateľ je vyzvaný, aby zadal PIN kód k YubiKey



4. Používateľ potvrdí prihlasovanie stlačením tlačidla na YubiKey

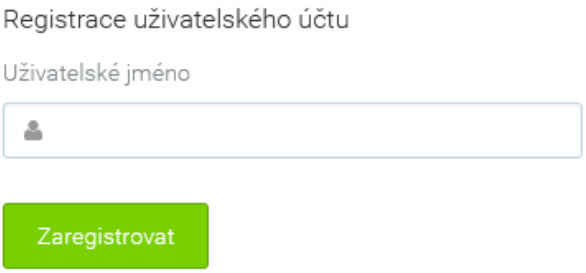


MFA bezheslové (passwordless) prihlásenie bez používateľského mena

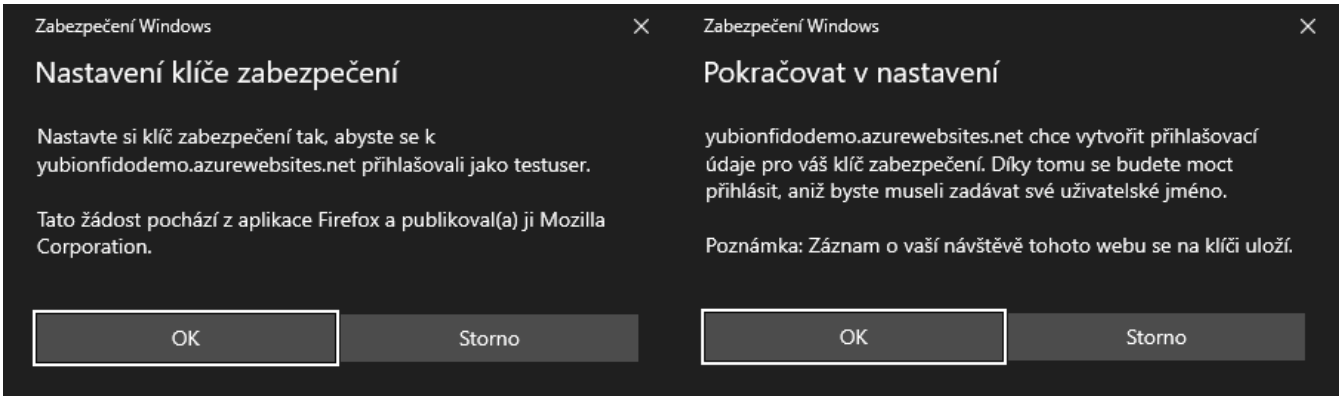
Bezheslové prihlasovanie bez používateľského mena, keď token slúži ako multi-faktor na overenie (zadáva sa aj PIN). Možno vyskúšať demo (zaškrtnúť pri
registrácii requireResidentKey a zvoliť userVerification: required pri registrácii aj autentizácii). Počet spárovaných služieb využívajúcich token týmto
scenárom je obmedzený kapacitou tokenu na 25 (v tokene sa ukladá používateľské meno a všeobecné informácie o službe).

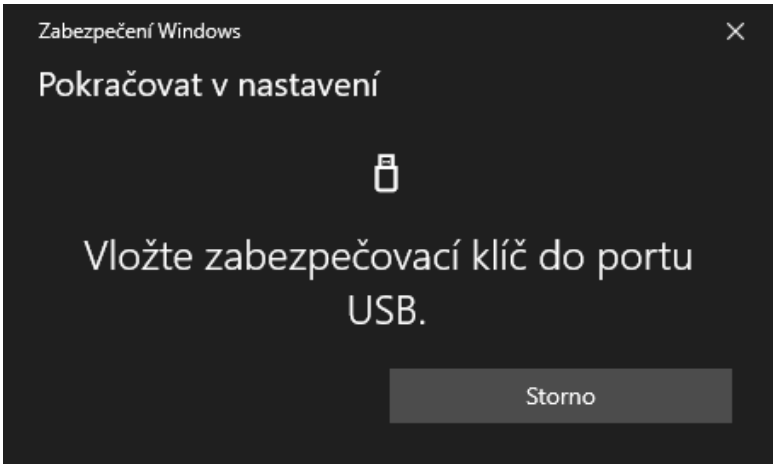
Fáza registrácie

1. Používateľ zvolí používateľské meno

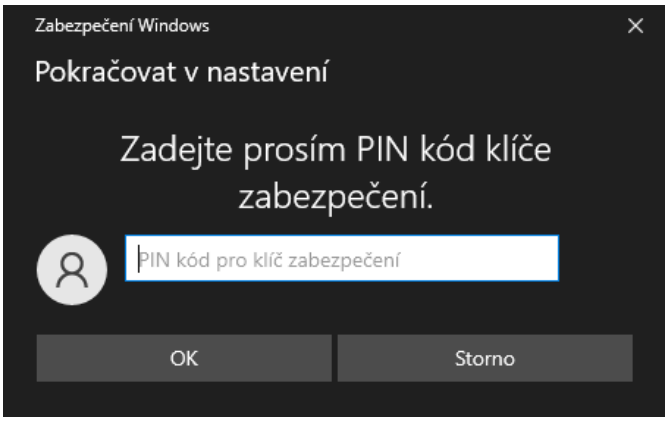


2. Používateľ je vyzvaný, aby pripojil YubiKey

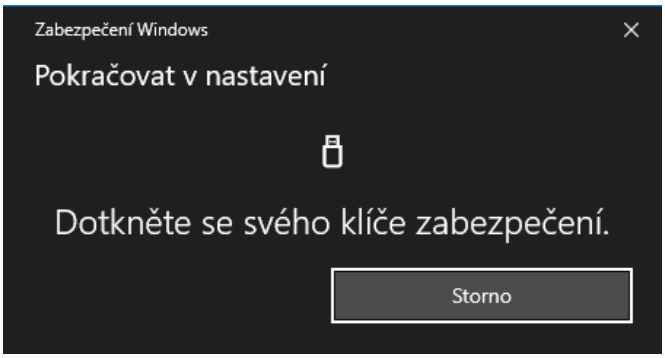




3. Ak má YubiKey nastavený PIN, používateľ je vyzvaný na jeho zadanie, ak nie, je vyzvaný na jeho vytvorenie (vrátane dodatočného stlačenia tlačidla YubiKey)

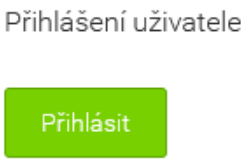


4. Používateľ dokončí registráciu stlačením tlačidla na YubiKey

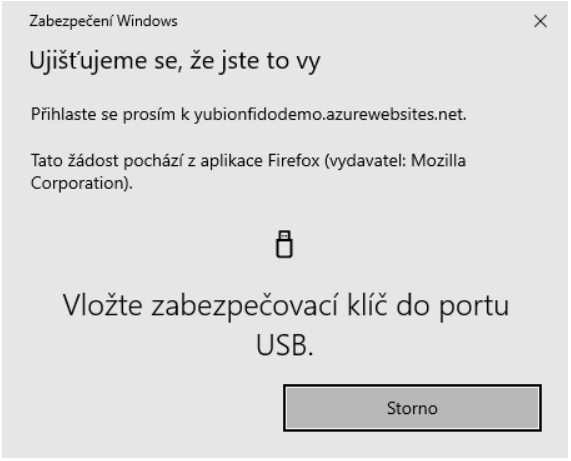


Fáza prihlásenia

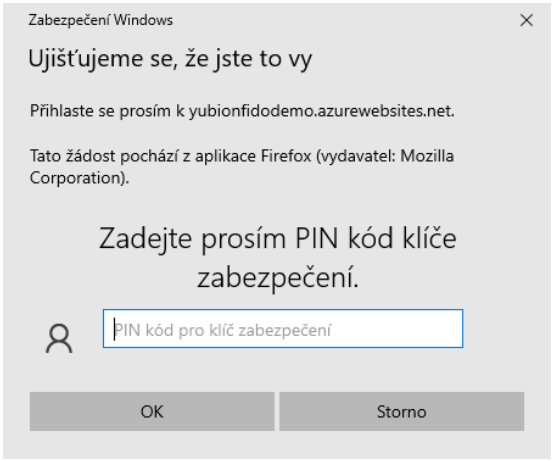
1. Používateľ nezadáva žiadne prihlasovacie údaje a rovno stlačí tlačidlo prihlásiť



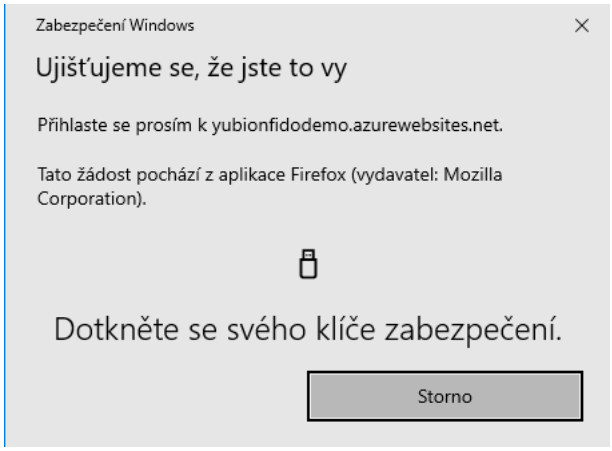
2. Používateľ je vyzvaný, aby pripojil YubiKey



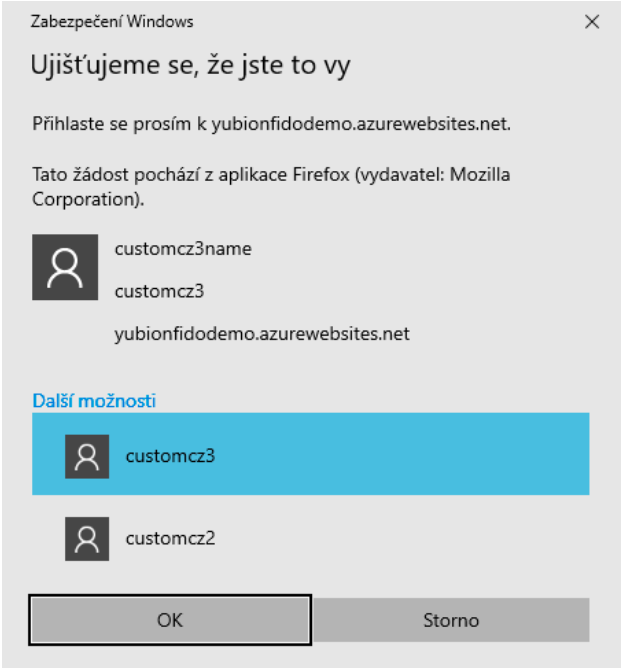
3. Používateľ je vyzvaný, aby zadal PIN kód k YubiKey



4. Používateľ potvrdí prihlasovanie stlačením tlačidla na YubiKey



5. Ak existuje viac registrovaných používateľských mien k danému YubiKey, používateľ je vyzvaný na výber jedného z nich (inak sa tento krok
preskočí)



FIDO2 technické informácie

Parameter	Hodnota
USB rozhranie	FIDO
Maximálny počet spárovaných služieb	Neobmedzene, 25 s uloženým používateľským menom
PIN	Predvolená hodnota: nie je nastavená 4 až 63 znakov Po nastavení je možné PIN zmeniť po jeho zadaní Odstrániť ho možno resetovaním celého modulu FIDO2 Ak je PIN 3× po sebe zadaný nesprávne, je potrebné token odpojiť a znova pripojiť do USB. Neúspešné pokusy sa započítavajú. Ak je PIN 8× po sebe zadaný nesprávne, modul FIDO2 sa zablokuje a je potrebné ho resetovať. Počet zostávajúcich pokusov je možné zobraziť pomocou aplikácie YubiKey Manager.
Reset	Možno vykonať pomocou aplikácie YubiKey Manager. Token bude potrebné znovu zaregistrovať vo všetkých službách. Reset nevykonávajte bez záložného tokenu, inak dôjde k strate prístupu k registrovaným službám. Automaticky sa vyresetujú aj všetky registrované služby U2F.
Certifikácia	FIDO 2 Level 1 (FIDO® Certified)
Testovacia stránka Yubico na vyskúšanie protokolu	Yubico FIDO2 Test
Najznámejšie globálne služby podporujúce FIDO2	Zobraziť aplikácie
Najznámejšie české služby podporujúce FIDO2	mojeID – úroveň značná
Registrácia záložného tokenu	Odporúča sa vykonať ihneď pri registrácii primárneho tokenu, no je možná kedykoľvek neskôr bez obmedzení.

Kompatibilita

Položka	Hodnota
Podpora v prehliadačoch	Stránky Yubico (v angličtine)
Prehľad podpory v prehliadačoch	Prehľad kompatibility (v angličtine)

Odkazy

Názov	Odkaz
Technický manuál – FIDO2	Stránky Yubico (v angličtine)
Technický manuál – WebAuthn	Stránky Yubico (v angličtine)
Domovská stránka FIDO2	FIDO Alliance (v angličtine)
Popis WebAuthn	Stránky Yubico (v angličtine)

U2F

U2F je skratka pre **Universal 2nd Factor** a predstavuje otvorený štandard navrhnutý organizáciou FIDO Alliance v roku 2014. Tento štandard bol neskôr nahradený výrazne robustnejším štandardom FIDO2.

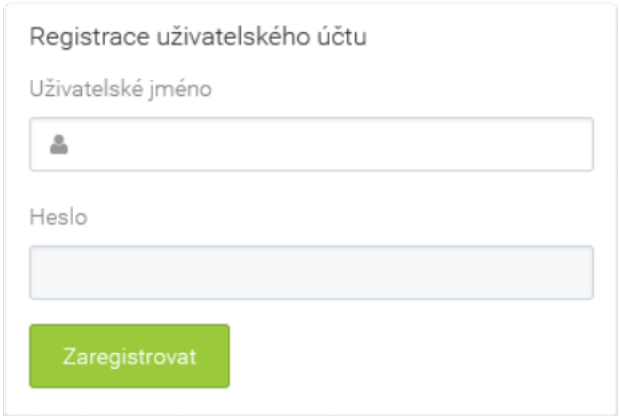
Proces U2F je, podobne ako FIDO2, rozdelený na dve fázy: registračnú a prihlasovaciu. Na rozdiel od FIDO2 nie je tak variabilný a vôbec nepoužíva PIN.

Tradičné 2FA

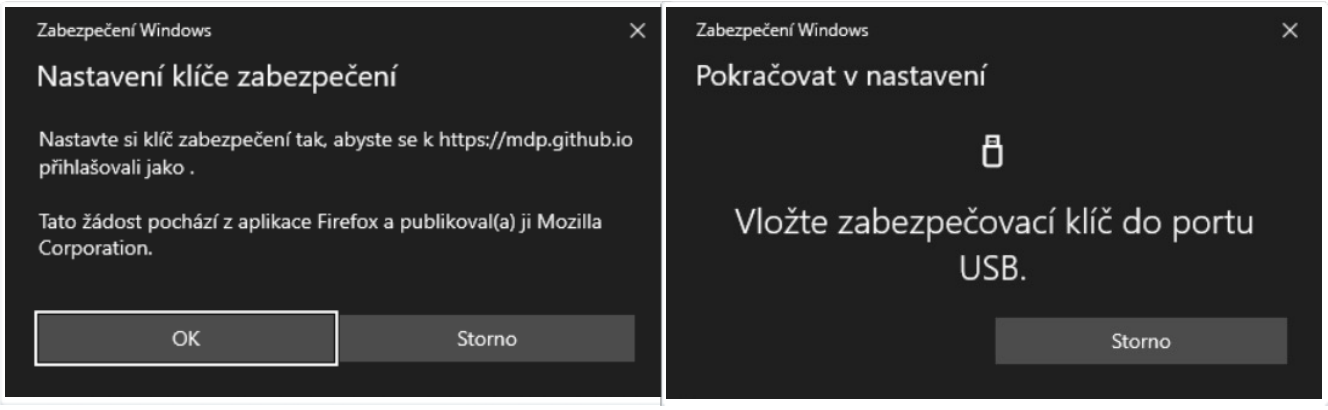
Klasické prihlasovanie s heslom, keď token slúži ako druhý faktor na overenie. Možno vyskúšať na demo alebo na demo. Počet spárovaných služieb využívajúcich token týmto scenáromnie je nijako obmedzený kapacitou tokenu (keďže sa v tokene neukladajú žiadne informácie o službe).

Fáza registrácie

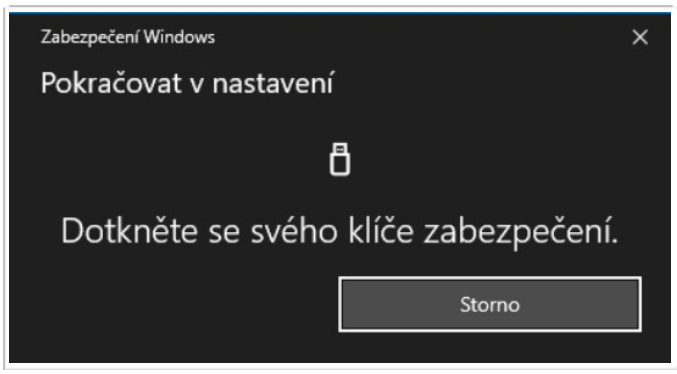
1. Užívateľ zvolí používateľské meno a heslo



2. Používateľ je vyzvaný, aby pripojil YubiKey

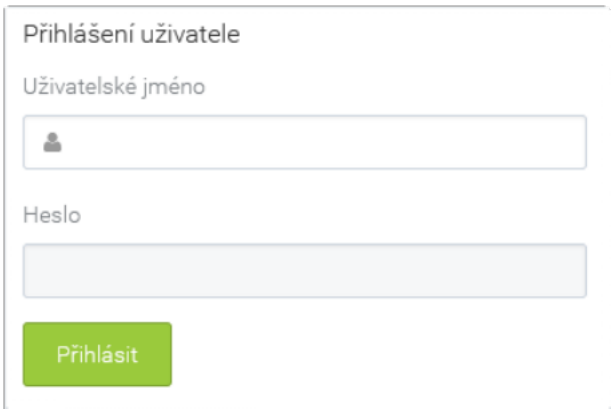


3. Užívateľ dokončí registráciu stlačením tlačidla na YubiKey

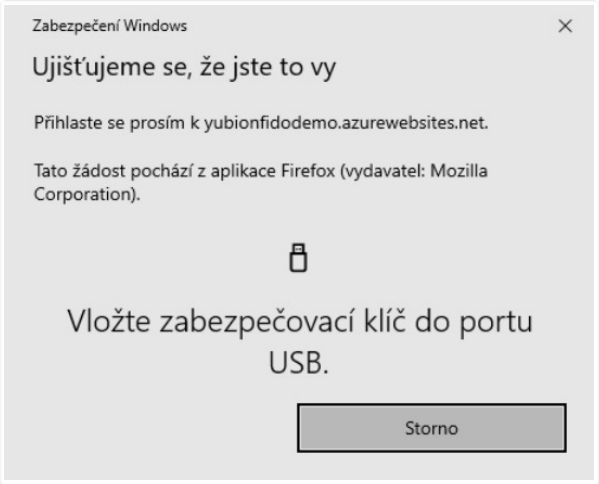


Fáza prihlásenia

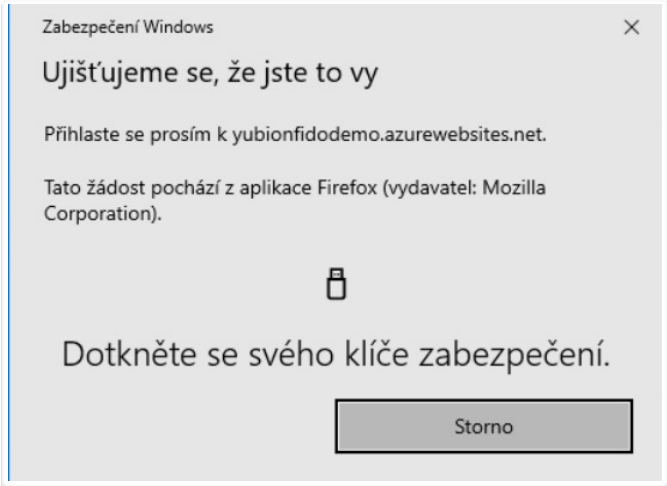
1. Užívateľ zadá používateľské meno a heslo



2. Používateľ je vyzvaný, aby pripojil YubiKey



3.Používateľ dokončí prihlasovanie stlačením tlačidla na YubiKey



U2F technické informácie	
USB rozhranie	FIDO
Maximálny počet spárovaných služieb	neobmedzene
PIN	nepoužíva sa
Reset	možno vykonať prostredníctvom aplikácie **YubiKey Manager** token bude potrebné znova zaregistrovať vo všetkých službách nevykonávať bez záložného tokenu, inak dôjde k strate prístupu k registrovaným službám automaticky vyresetuje aj všetky služby zaregistrované cez FIDO2
Najznámejšie globálne služby podporujúce U2F	Zobraziť aplikácie
Postup registrácie záložného tokenu	odporúča sa vykonať ihneď pri registrácii primárneho tokenu, ale je možné ho zaregistrovať kedykoľvek neskôr bez obmedzení

OTP

Modul OTP zahŕňa 2 samostatné konfigurovateľné sloty, na ktoré je možné podľa preferencií používateľa nastaviť tieto funkcionality:

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

Konfiguráciu je možné vykonať cez YubiKey Manager alebo prostredníctvom YubiKey Personalization Tool . Funkcionalitu jednotlivých slotov je potom možné vyvolať rôzne dlhým stlačením tlačidla. Sloty je tiež možné chrániť samostatným heslom (pri jeho strate je možné slot prepísať, nie však editovať konfiguráciu).

- krátkymstlačenímtlačidla - vyvolá funkcionalitu na slote 1
- 3 sekundy dlhýmstlačenímtlačidla - vyvolá funkcionalitu na slote 2

Yubico OTP

Ide o mechanizmus overovania vo forme webovej služby s veľmi vysokou dostupnosťou od spoločnosti Yubico. Prevádzkovatelia služieb tak môžu jednoducho rozšíriť svoje aplikácie o druhý faktor (prihlasovanie, potvrdzovanie dôležitých operácií) bez toho, aby museli nakupovať špecializovaný softvér alebo obstarávať licencie.

Yubico OTP je predvolene prednastavené na slote číslo 1.

HMAC-SHA1 Challenge-Response

Tento typ overovania sa najčastejšie používa na o fline autentizáciu. Aplikácia zašle do YubiKey tokenu výzvu (challenge) a overí, že token očakávaným spôsobomodpovedal. Odoslanie odpovede je možné podmieniť stlačením tlačidla. Ak token výzvu nedostane, neexistuje žiadny iný spôsob, ako získať odpoveď.

Static password

Static password je najtriviálnejšou funkciou celého tokenu a ako názov napovedá, ide o stále rovnakú statickú frázu, ktorú token generuje. Nejde o bezpečnú metódu overovania, ale v niektorých prostrediach, kde sa používatelia stále stretávajú s historickými aplikáciami, môže táto funkcia uľahčiť trápenie.

Statické heslo je možné využiť na zadávanie dlhých hesiel. Token je potom možné použiť ako generátor statického prefixu hesla (napríklad prvých 10 znakov), pričom ďalších 8 znakov vždy zadáva používateľ. Výsledkom je dlhé heslo, ktoré si používateľ nemusí celé pamätať. Zároveň zlodej, ktorý odcudzí jeho token, stále nepozná celé heslo.

OATH-HOTP

Generátor HOTP kódov, ktoré token emituje stlačením tlačidla (na rozdiel od AUTH modulu, kde sú HOTP kódy viditeľné iba prostredníctvom Yubico Authenticator).

OTP technické informácie	
USB rozhranie	OTP
PIN	nepoužíva sa
Heslo	predvolená hodnota: nie je nastavené každý slot má vlastné heslo po nastavení je možné ho zmeniť alebo odstrániť po jeho zadaní v aplikácii **YubiKey Personalization Tool** možno ho odstrániť prepísaním daného slotu
Najznámejšie globálne služby podporujúce OTP	• Zobraziť aplikácie podporujúce Challenge-Response • Zobraziť aplikácie podporujúce Yubico OTP • Zobraziť aplikácie podporujúce HOTP
Postup registrácie záložného tokenu	odporúča sa vykonať ihneď pri registrácii primárneho tokenu
Poznámky	Vývojári Apple: Challenge-Response v systéme iOS vyžaduje Yubico iOS SDK

OATH

OATH je skratkou pre Open Authentication a v tokenoch YubiKey 5 označuje samostatný modul, ktorý slúži ako úložisko pre celkovo 32 jednorazových číselných hesiel, čiže OTP (one-time password) kódov. Rozlišujeme dva druhy, OTP kódy generované pomocou algoritmu TOTP (Time-based One-Time Password), kde je výsledný kód platný iba krátky časový úsek. Po uplynutí času kód prestáva platiť a je potrebné vygenerovať nový. Naproti tomu OTP kódy generované algoritmom HOTP (HMAC-based One-time Password) sú platné iba raz a každý ďalší kód je odvodený od predchádzajúceho (laicky povedané, výpočet je závislý od nejakej internej inkrementovanej hodnoty)

Tieto OTP kódy je možné zobrazovať cez Yubico Authenticator . Aplikáciu je možné používať buď na počítači alebo notebooku (desktopová verzia) alebo na telefóne (mobilná verzia). Nasleduje popis desktopovej verzie. Mobilná verzia funguje totožne, akurát aktivácia neprebieha zasunutím YubiKey do USB, ale priložením tokenu cez NFC rozhranie telefónu.

Fáza nastavenia

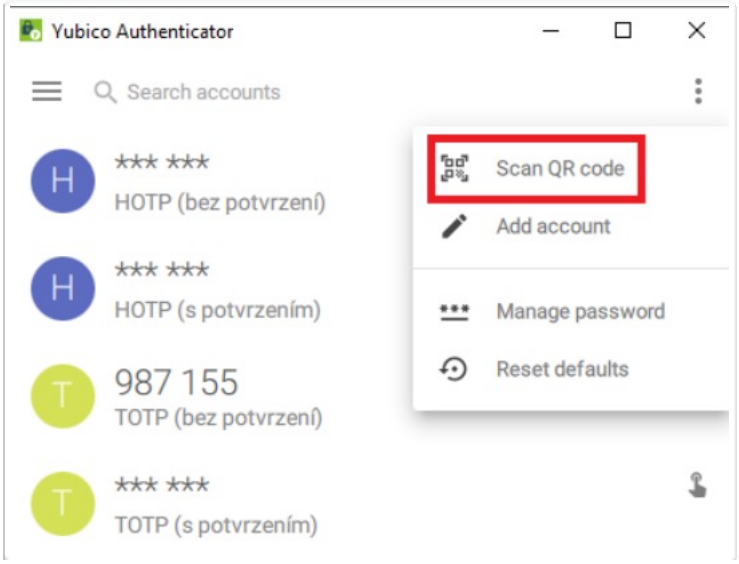
1.Užívateľ si vo vybranej službe zvolí dvojfaktorové overovanie pomocou OTP kódov.
Najprv je vyzvaný na naskenovanie QR kódu. QR kód obsahuje informáciu o názve služby, názve konkrétneho účtu, seede a nastavení OTP.



Tento QR kód si nikde neukladajte (úložisko, počítač, mobil), pretože je to jedna z prvých vecí, ktoré vyhľadáva malvér.

Ak si tento QR kód vytlačíte na papier ako zálohu, najprv si overte, že sa vaše vytlačené dokumenty neukladajú do logu.

2. Používateľ vloží YubiKey do USB a otvorí si Yubico Authenticator, kde zvolí Scan QR code. Aplikácia automaticky deteguje QR kód zobrazený na monitore a spracuje ho, čo predvyplní údaje o Poskytovateľovi služby (Issuer), názov účtu (Account name). Voľba Require touch je voliteľná a určuje, či má byť OTP kód viditeľný ihneď po otvorení Yubico Authenticatoru, alebo či bude ešte potrebné potvrdiť zobrazenie stlačením tlačidla YubiKey

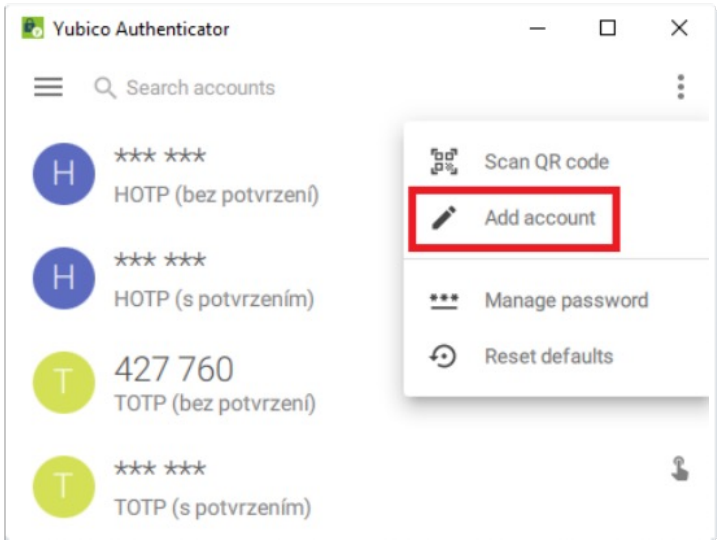


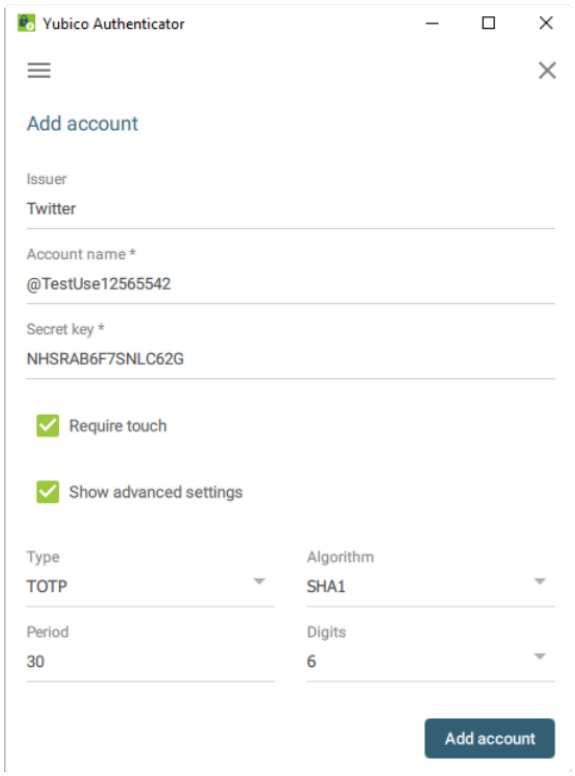
Ak QR kód nie je viditeľný na monitore alebo je práve prekrytý aplikáciou Yubico Authenticator, aplikácia oznámi, že QR kód nenašla. Posuňte okno aplikácie mimo QR kódu.

3. Každá služba ponúka aj alternatívnu metódu, ak nejde QR kód naskenovať, a to prepísanie seedu (a prípadne ďalších parametrov). V Yubico Authenticatori je to potom voľba Add account. Seed sa zadáva do poľa Secret key. Pomocou Show advanced settings možno meniť parametre generovacieho algoritmu. Najbežnejšie sa používa 6-miestny TOTP, ktorý je predvyplnený, ak služba vyžaduje niečo špeciálne, používateľa pravdepodobne upozorní.

Táto možnosť sa hodí najmä z dôvodu vytvorenia zálohy. Ak si používateľ prepíše seed (a prípadne ďalšie parametre) a uloží všetko na bezpečné miesto, bude kedykoľvek schopný nastaviť akýkoľvek prostriedok (YubiKey, Google Authenticator) tak, aby mu začal generovať platné OTP kódy. Rovnako tak to však bude môcť urobiť útočník, ak sa zmocní prepísaných údajov.
Druhou a bezpečnejšou stratégiou je v tejto fáze nastaviť 2 YubiKey tokeny. Záložný token potom uschovať na bezpečné miesto. V prípade straty jedného tokenu však bude potrebné celý registračný proces zopakovať, čiže prihlásiť sa do služby zostávajúcim tokenom, zrušiť OTP overovanie a nastaviť OTP overovanie znova.





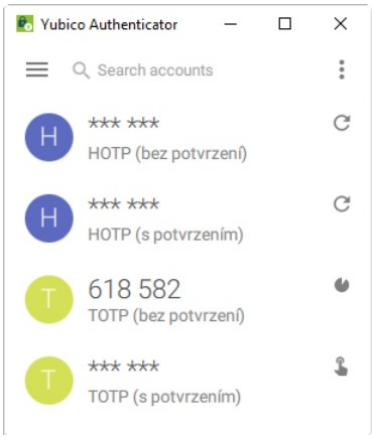


4. Ako potvrdenie úspešného nastavenia vás služba požiada o vloženie aktuálneho OTP kódu. Ak ide o TOTP kódy, ktoré majú obmedzenú časovú platnosť, je potrebné stihnúť platný kód prepísať počas jeho platnosti.



Služba môže mať implementovanú určitú toleranciu, takže aj kód, ktorému vypršala platnosť, bude ešte nejaký čas prijatý.

5. Podľa typu OTP kódu a nastaveného spôsobu zobrazovania možno rozlíšiť 4 situácie



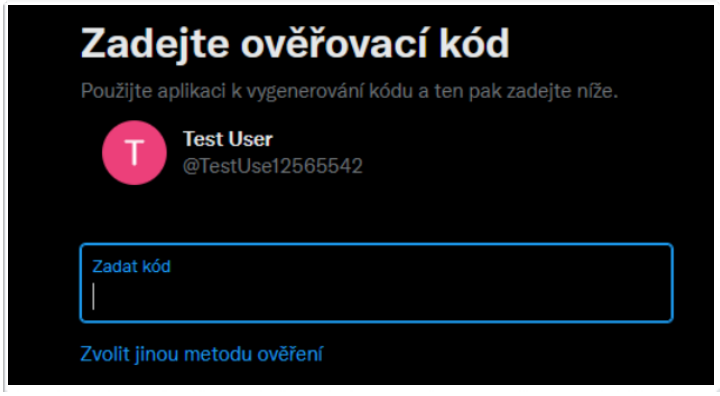
- **TOTP bez potvrdenia** sa ihneď zobrazí a po uplynutí časového intervalu, ktorý definuje životnosť aktuálneho kódu, sa nahradí novým kódom
- **TOTP s potvrdením** sa zobrazí len keď používateľ akciu potvrdí dodatočnýmstlačením tlačidla YubiKey, a to iba do uplynutia časového intervalu, ktorý definuje životnosť aktuálneho kódu
- **HOTP bez potvrdenia** sa zobrazí potom, čo používateľ klikne na daný kód, ten potom zostane zobrazený, kým používateľ nevygeneruje ďalší
- **HOTP s potvrdením** sa zobrazí potom, čo používateľ klikne na daný kód a potvrdí akciu dodatočnýmstlačením tlačidla YubiKey, kód potom zostane zobrazený, kým používateľ nevygeneruje ďalší

Fáza prihlásenia

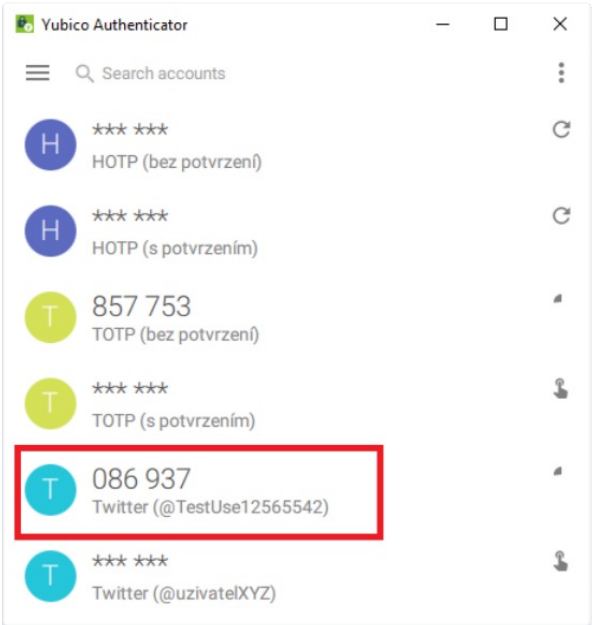
1.Používateľ zadá používateľské meno a heslo



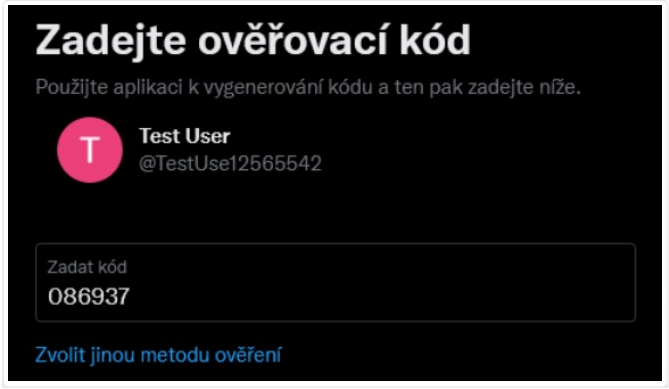
2. Používateľ je vyzvaný, aby zadal OTP kód



3. Používateľ si otvorí Yubico Authenticator a vyberie príslušný OTP kód



4. Užívateľ zadá OTP kód



OATH technické informácie	
USB rozhranie	CCID
Maximálny počet kódov	32
Konfigurácia TOTP a HOTP	Algoritmy: SHA1, SHA256, SHA512 Počet číslic: 6, 7, 8
PIN	nepoužíva sa
Heslo	predvolená hodnota: nie je nastavené po nastavení ho možno zmeniť alebo odstrániť po jeho zadaní v aplikácii **Yubico Authenticator** možno ho odstrániť resetovaním celého modulu OATH
Reset	možno vykonať prostredníctvom aplikácie **Yubico Authenticator** token bude potrebné znova zaregistrovať vo všetkých službách nevykonávať bez záložného tokenu, inak dôjde k strate prístupu k registrovaným službám
Najznámejšie globálne služby podporujúce OTP	• Zobraziť aplikácie podporujúce TOTP • Zobraziť aplikácie podporujúce HOTP
Postup registrácie záložného tokenu	odporúča sa vykonať ihneď pri registrácii primárneho tokenu
Poznámky	Vývojári Apple: V systéme iOS je vyžadované Yubico iOS SDK

PIV (Smart Card)

YubiKey disponuje funkcionalitou čipovej karty (smart card) podľa amerického vládneho štandardu PIV (alebo tiež FIPS 201). Token podporuje algoritmy ECC a RSA zo sveta asymetrickej kryptografie. Používateľ tak môže podpisovať a šifrovať pomocou privátneho kľúča uloženého v tokene prostredníctvom štandardizovaného rozhrania PKCS#11.

Kľúče a certifikáty sú uložené v tzv. slotoch a majú nastavené predvolené politiky (popis viď tabuľka nižšie), ktoré však možno zmeniť.

Aplikácia YubiKey Manager ponúka okrem iného tieto funkcie pre PIV modul:

- Nastavenie PINu, PUKu a Management kľúča
- Vygenerovanie certifikátov tokenomna sloty 9a, 9c, 9d a 9e
- Importovanie certifikátov do tokenu na sloty 9a, 9c, 9d a 9e
- Vyresetovanie PIV modulu

The YubiKey 5 podporujú rozšírené APDU: Answer To Reset (ATR), Answer To Select (ATS) - na iOS je potrebné Yubico iOS SDK.

Podpora na Windows

V operačnom systéme Windows možno PIV funkcionalitu ďalej rozšíriť pomocou špeciálneho ovládača YubiKey Smart Card Minidriver. Vďaka tomu budú dostupné aj tieto funkcie:

- Enro lment YubiKey tokenu štandardnými Windows nástrojmi
- Auto-enro lment, umožňujúci používateľovi self-provisioning YubiKey tokenu a automatické obnovenie
- Podpora viacerých autentizačných certifikátov na jednom YubiKey tokene
- Zmenu PINu z menu po stlačení Ctrl+Alt+Del
- Odblokovanie PINu pomocou PUK na prihlasovacej stránke Windows

Technické informácie	
USB rozhranie	CCID
PIN	predvolená hodnota: **123456**
PUK	predvolená hodnota: **12345678**
Management Key (3DES)	predvolená hodnota: 010203040506070801020304050607080102030405060708
RSA algoritmy	RSA 1024 RSA 2048
ECC algoritmy	ECC P-256 ECC P-384

Slot	**Popis**
Slot 9a: PIV Authentication	Certifikát a s ním asociovaný súkromný kľúč v tomto slote sa používajú na autentifikáciu používateľa (prihlasovanie do systémov). Pri prvej interakcii je vyžadovaný PIN.
Slot 9c: Digital Signature	Certifikát a s ním asociovaný súkromný kľúč v tomto slote sa používajú na digitálne podpisovanie (dokumentov, e-mailov a súborov). Pri každej interakcii je vyžadovaný PIN.

Slot 9d: Key Management	Certifikát a s ním asociovaný súkromný kľúč v tomto slote sa používajú na šifrovanie (e-mailov, súborov). Pri prvej interakcii je vyžadovaný PIN.
Slot 9e: Card Authentication	Certifikát a s ním asociovaný súkromný kľúč v tomto slote sa používajú na fyzický prístup do budov (kde sú použité zámky kompatibilné s PIV). Pri interakcii sa PIN nevyžaduje.
Sloty 82-95: Retired Key Management	Tieto sloty sa používajú pre predchádzajúce kľúče uložené v slote **9d: Key Management**. Vďaka tomu bude možné pomocou tokenu dešifrovať e-maily a dokumenty zašifrované staršími kľúčmi.
Slot f9: Attestation	Tento slot sa používa na atestáciu (attestation) ostatných kľúčov vygenerovaných tokenom, ktoré boli vytvorené pomocou inštrukcie **f9**. Tento slot sa nevymaže pri resetovaní. Slot je možné prepísať.

Politika	Popis
PIN Policy	Pre každý slot je možné určiť, či sa pri požiadavke na daný slot bude vyžadovať zadanie PIN-u. Musí byť nastavená pri generovaní alebo importe kľúča, neskôr ju už nie je možné meniť.
Touch Policy	Pre každý slot je možné určiť, či sa pri požiadavke na daný slot bude vyžadovať stlačenie tlačidla tokenu. Musí byť nastavená pri generovaní alebo importe kľúča, neskôr ju už nie je možné meniť.

Názov	Odkaz
Manuál pre PIV	Stránky Yubico (v angličtine)
Manuál k YubiKey Manageru	Stránky (v angličtine)
Minidriver vo firemnom prostredí	Stránky Yubico (v angličtine)

OpenPGP

OpenPGP je štandard používajúci asymetrickú kryptografiu. YubiKey 5 tokeny fungujú ako tzv. OpenPGP karta, čo je čipová karta kompatibilná podľa ISO/IEC 7816-4, -8, ktorú možno používať s PGP aplikáciami (napr. GnuPG (GPG)) a uložiť na ňu GPG kľúče na autentizáciu, podpisovanie a šifrovanie. Tokenu možno nastaviť pravidlá potvrdzovania tlačidlom pre každý kľúč zvlášť.
Od verzie YubiKey firmvéru 5.2.3 je implementovaná podpora OpenPGP karty vo verzii 3.4, ktorá priniesla množstvo vylepšení.

Na využitie OpenPGP v iOS je potrebné Yubico iOS SDK.

Technické informácie	
USB rozhranie	CCID
PIN	predvolená hodnota: **123456**
Admin PIN	predvolená hodnota: **12345678**
RSA algoritmy	RSA 1024 RSA 2048 RSA 3072 (vyžaduje GnuPG verzie 2.0 a vyššej) RSA 4096 (vyžaduje GnuPG verzie 2.0 a vyššej)
ECC algoritmy	Použitie pre Signature, Authentication a Decipher: • secp256r1 • secp256k1 • secp384r1 • secp521r1 • brainpoolP256r1 • brainpoolP384r1 • brainpoolP512r1 • curve25519 • x25519 (iba pre dešifrovanie) • ed25519 (iba pre podpis/autentifikáciu)

Odkazy	
Manuál pre OpenPGP	Stránky Yubico (v angličtine)
Špecifikácia OpenPGP Smart Card 3.4	PDF dokument (v angličtine)
Podpora špecifikácie 3.4	Stránky Yubico (v angličtine)

Záložný token

Pri kúpe hlavného (primárneho) tokenu **YubiKey** je vhodné zároveň zakúpiť minimálne jeden záložný token. Ak používateľ primárny token stratí, nepríde o prístup k svojim službám a následky nebudú kritické. Ideálnym riešením sú **dva záložné tokeny**.

Nasledujúca tabuľka pomôže majiteľovi tokenu **YubiKey 5 NFC** vybrať vhodného kandidáta na záložný token s prihliadnutím na obstarávaciu cenu.

Primárny token	Vhodný záložný token
 YubiKey 5 NFC	 YubiKey 5 NFC

Bezpečnostné zásady

Primárny token **YubiKey 5 NFC** má používateľ neustále pri sebe (napríklad pripnutý na zväzku kľúčov), zatiaľ čo záložný token má uložený na bezpečnom mieste (napríklad v trezore). Ak má používateľ viac záložných tokenov, odporúča sa uložiť ich na geograficky odlišných miestach.

V prípade straty primárneho tokenu by si mal používateľ okamžite objednať nový token. Dovtedy by mal veľmi obozretne používať záložný token. Ide o kritické a časovo obmedzené obdobie, najmä ak má používateľ iba jeden záložný token. Po doručení nového tokenu ho opätovne zaregistruje vo všetkých službách a vráti sa do štandardného režimu, teda primárny token nosí pri sebe a záložný token uchováva na bezpečnom mieste.

Registrácia tokenu

V závislosti od použitého protokolu môže byť záložný token identickou kópiou primárneho tokenu (napríklad pri generovaní OTP kódov) alebo samostatným sekundárnym tokenom spárovaným so službou. Služba potom vie, že konkrétny používateľ sa môže prihlasovať ktorýmkoľvek z týchto tokenov.

Vo všeobecnosti platí, že pri registrácii do novej služby by sa mali spárovať alebo nastaviť všetky tokeny naraz. Môže to byť nepraktické v prípade, že sú záložné tokeny už uložené na bezpečnom mieste v inej lokalite. Ide však o daň za vyššiu úroveň bezpečnosti.

Do aplikácií podporujúcich protokoly **FIDO2** a **U2F** je možné pridávať nové tokeny aj neskôr. Stačí sa štandardne prihlásiť do danej služby a zvyčajne je možné v nastaveniach používateľského profilu pridať nový token.

Pri protokoloch založených na **OTP** nie je dodatočná registrácia tokenov možná, pokiaľ používateľ nemá uložený tzv. **seed**. Podobné obmedzenie platí aj pre certifikáty vygenerované priamo tokenom, ktoré nie je možné žiadnym spôsobom exportovať. V sekcii funkcií je pri každom protokole podrobne uvedené, kedy vykonať registráciu záložných tokenov a aké obmedzenia daná technológia prináša.

Bez záložného tokenu

Ak si používateľ zaregistruje iba jeden token (napríklad z dôvodu úspory nákladov) a token stratí, s vysokou pravdepodobnosťou príde o prístup k službe. Ak ide napríklad o burzu, na ktorej má uložené bitcoiny, môže sa takáto úspora výrazne predražiť.

Ak si používateľ zaregistruje iba jeden token a zároveň si nastaví alternatívny spôsob prihlásenia pre prípad straty tokenu, síce ušetrí za záložný token, ale zníži úroveň bezpečnosti celého systému na úroveň tejto záložnej metódy. Napríklad ak bude záložnou metódou zadanie tzv. **recovery kódu**, vystavuje sa riziku phishingového útoku. Útočník ho môže presvedčiť, že primárny YubiKey nefunguje, a následne od neho vylákať recovery kód.

Celková bezpečnosť autentifikácie je vždy len taká silná, ako je silný jej najslabší článok.

Prvotné nastavenie YubiKey 5 NFC

Inštalácia nástrojov

Nainštalujte si nasledujúce aplikácie do počítača alebo notebooku:

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

Do mobilného telefónu si nainštalujte aplikáciu **Yubico Authenticator (Mobile verzia)**.

Nastavenie pre prvé použitie

- Nastavenie FIDO2 PIN-u v aplikácii YubiKey Manager
- Zmena predvoleného PIV PIN-u v aplikácii YubiKey Manager
- Zmena predvoleného PIV PUK kódu v aplikácii YubiKey Manager
- Nastavenie statického hesla do slotu 2 v aplikácii YubiKey Manager
- Vygenerovanie autentifikačného certifikátu v aplikácii YubiKey Manager

Nástroje pre YubiKey 5C NFC

Spoločnosť Yubico dodáva k tokenom aj softvér, ktorý je potrebný pre niektoré scenáre použitia. Všetky nižšie uvedené nástroje sú bezplatné a ich aktuálne verzie je možné stiahnuť na príslušných stránkach výrobcu. Ak tieto programy používate, vždy ich udržiavajte aktuálne.

YubiKey Manager

Pomocou aplikácie YubiKey Manager je možné konfigurovať funkcionality FIDO2, OTP a PIV alebo napríklad nastaviť PIN. Aplikácia je dostupná pre Windows, macOS a Linux.

Súčasťou balíka je aj nástroj **ykman** pre príkazový riadok.

Prejsť na domovskú stránku YubiKey Manager

YubiKey Personalization Tool

YubiKey Personalization Tool umožňuje nastavovať programovateľné sloty 1 a 2, zistiť verziu firmvéru tokenu alebo konfigurovať jeho správanie a pokročilé vlastnosti.

Prejsť na domovskú stránku YubiKey Personalization Tool

Yubico Authenticator

Aplikácia **Yubico Authenticator** (mobilná aj desktopová verzia) umožňuje zobrazovať časovo obmedzené jednorazové kódy (**TOTP**). Vďaka tomu je možné používať YubiKey ako alternatívu k mobilnému telefónu a aplikáciám typu Google Authenticator.

Prejsť na domovskú stránku Yubico Authenticator

Yubico Login

Aplikáciu **Yubico Login** možno využiť na zabezpečenie prístupu k počítaču, ktorý používa lokálne účty (nie doménové účty). Používateľ potom musí potvrdiť prihlásenie svojím tokenom.

Prejsť na domovskú stránku Yubico Login

Developer Resources

K dispozícii sú rôzne knižnice pre vývojárov, ktoré uľahčujú integráciu technológií Yubico do vlastných aplikácií.

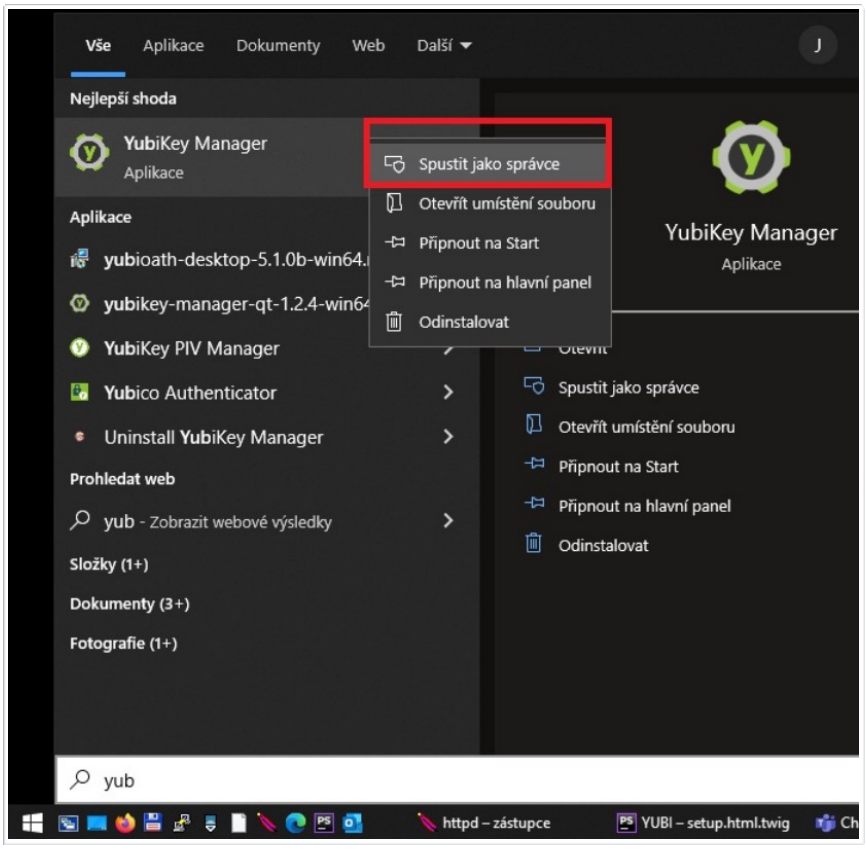
Prejsť na domovskú stránku Developer Resources

Návody pre YubiKey 5C NFC

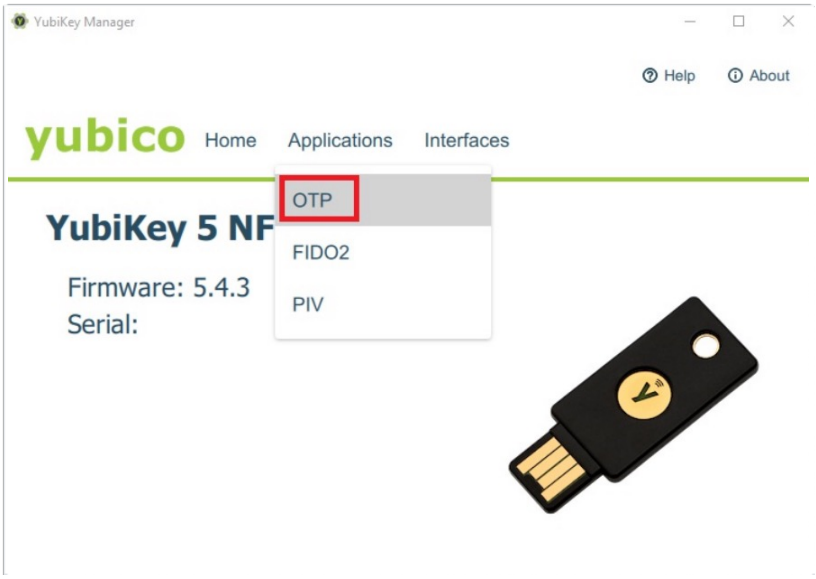
Statické heslo v slote 2 v aplikácii YubiKey Manager

Nastavíme dlhé stlačenie tokenu tak, aby generovalo statické heslo. Táto funkcia môže byť užitočná pre staršie aplikácie, v ktorých nie je možné nastaviť inú metódu prihlasovania.

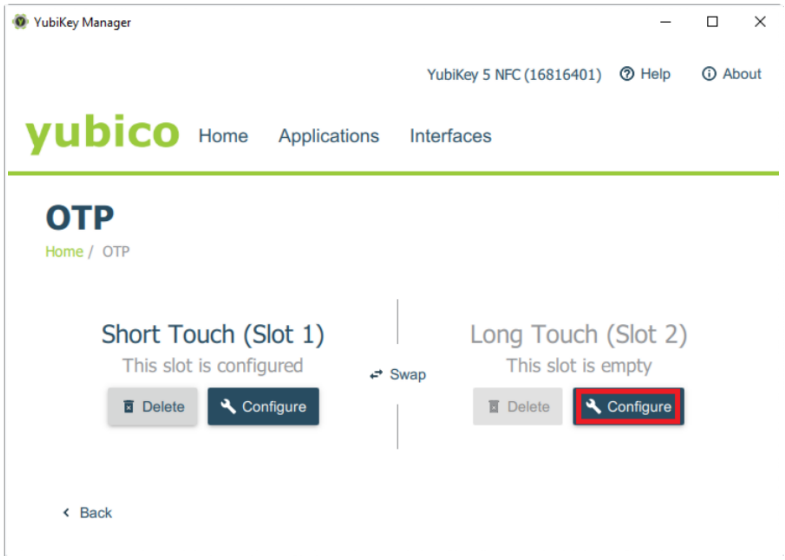
1. Spustíme aplikáciu **YubiKey Manager** s oprávneniami správcu pomocou voľby **Spustiť ako správca**.



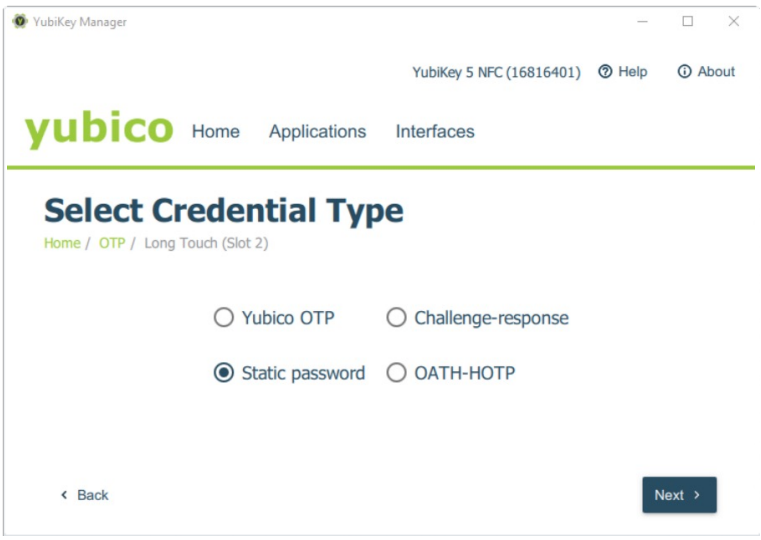
2. Zvolíme voľbu OTP.



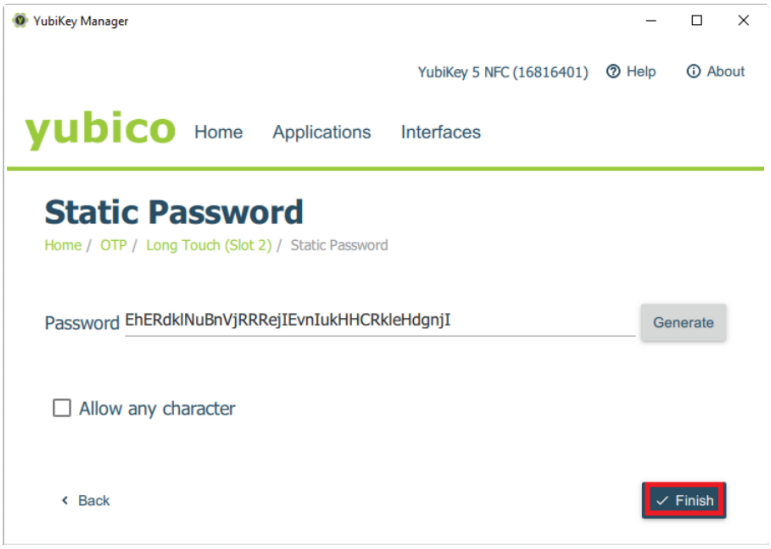
3. Klikneme na Configure vpravo pre Long Touch (dlhé stlačenie).



4. Vyberieme voľbu Static password a stlačíme tlačidlo Next.

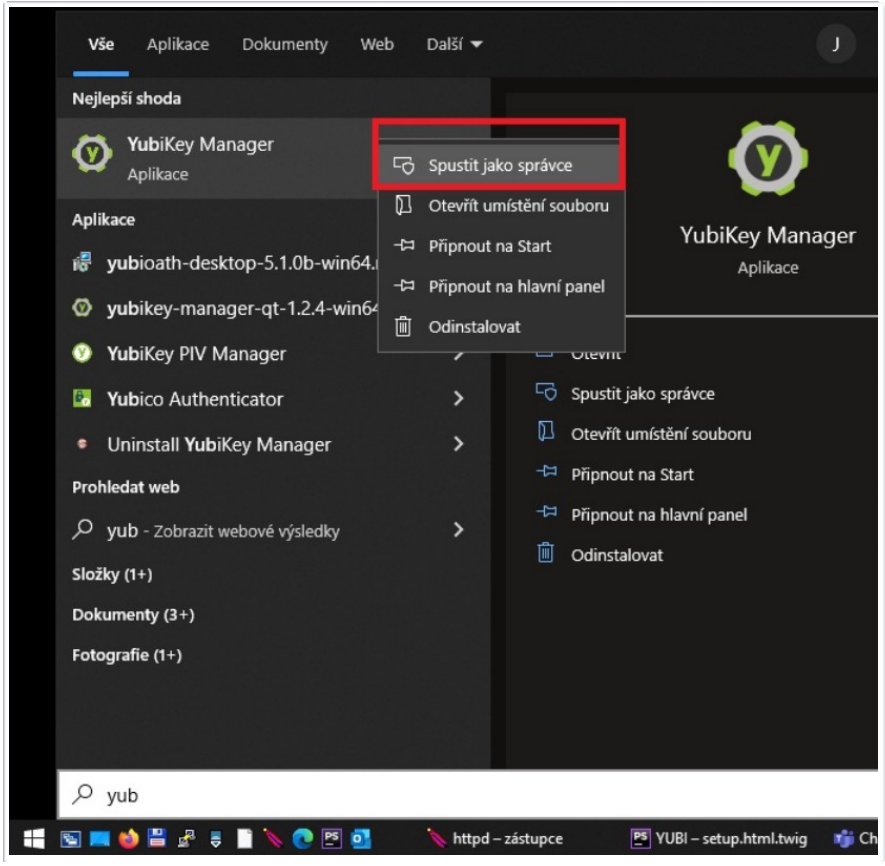


5. Klikneme na tlačidlo Generate, necháme si heslo vygenerovať a potvrdíme voľbu tlačidlom Finish (ak zaškrtneme voľbu Allow any character, vygenerovaná sekvencia znakov bude komplexnejšia, ale bude fungovať iba na anglickej klávesnici).

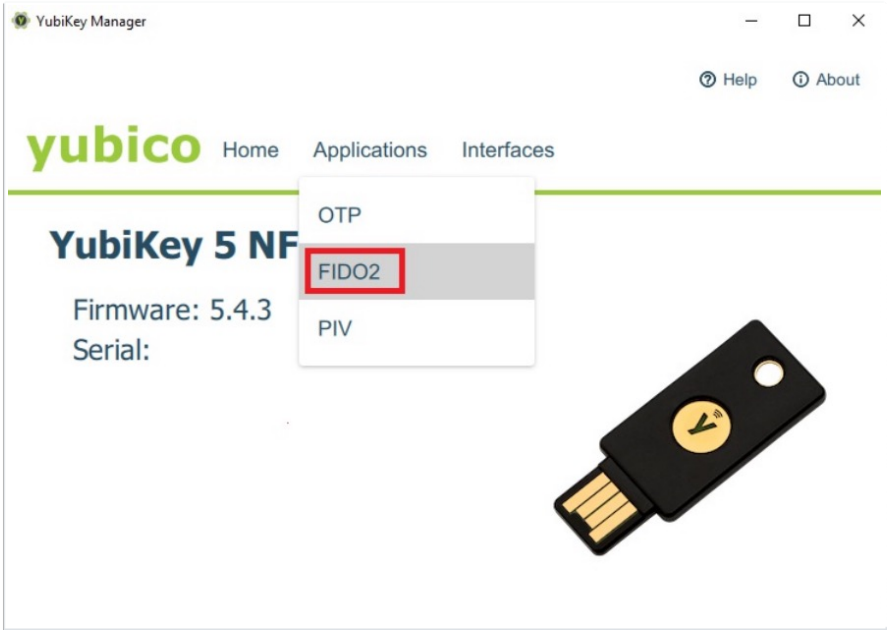


Nastavenie FIDO2 PINu v YubiKey Manageri

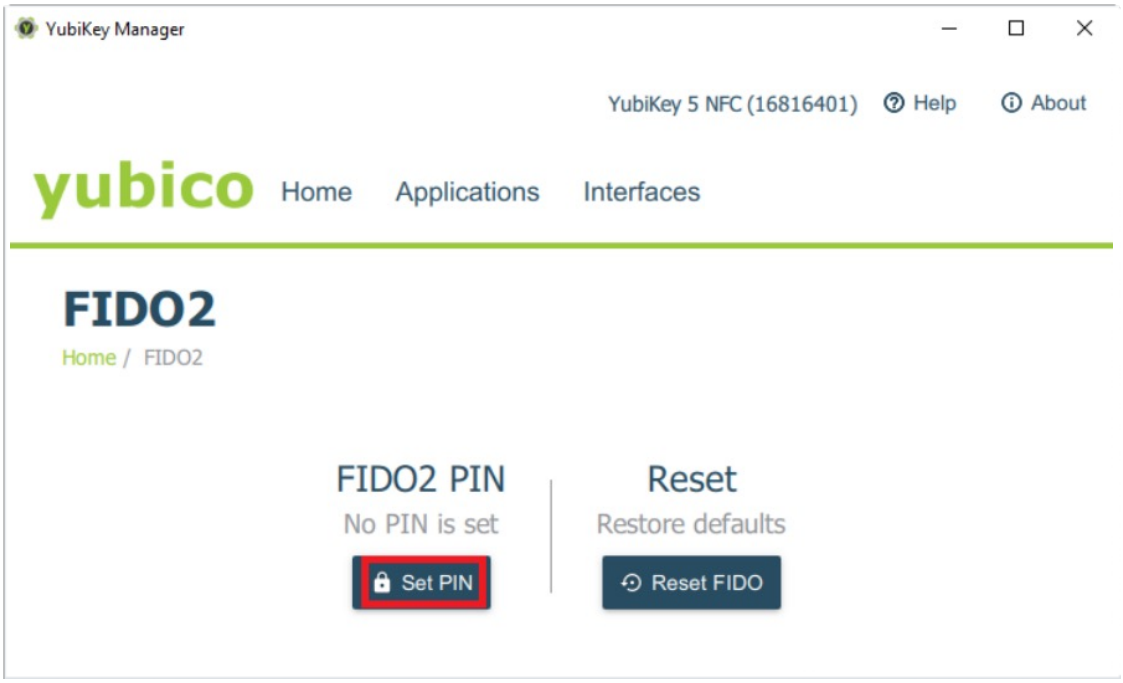
1. Spustíme YubiKey Manager ako správca pomocou Spustiť ako správca.



2. Zvolíme voľbu FIDO2.



3. Klikneme na *Set PIN*

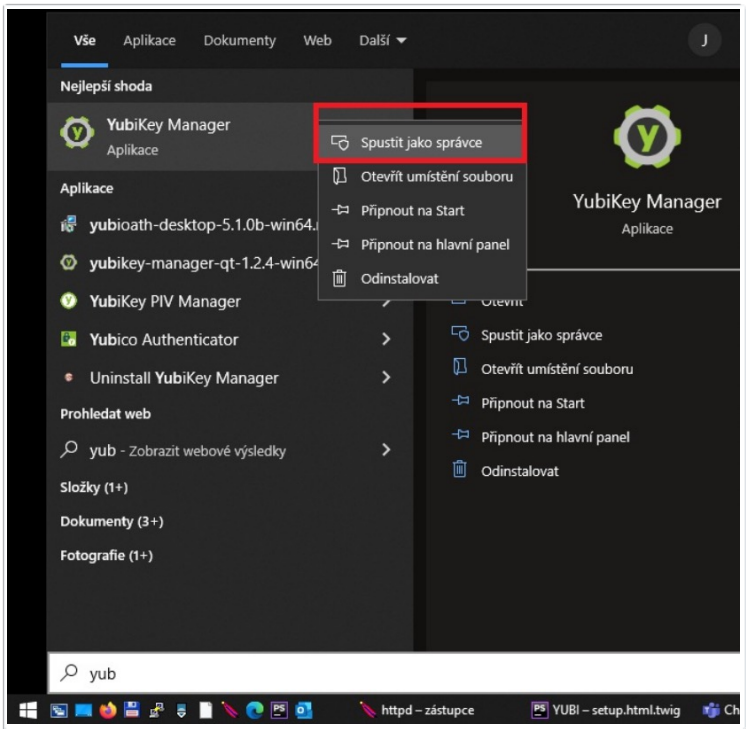


4. Zvolíme si alfanumerický PIN (minimálne 4 znaky) v poli New PIN, potvrdíme ho v poli Confirm PIN a uložíme pomocou tlačidla Set PIN.

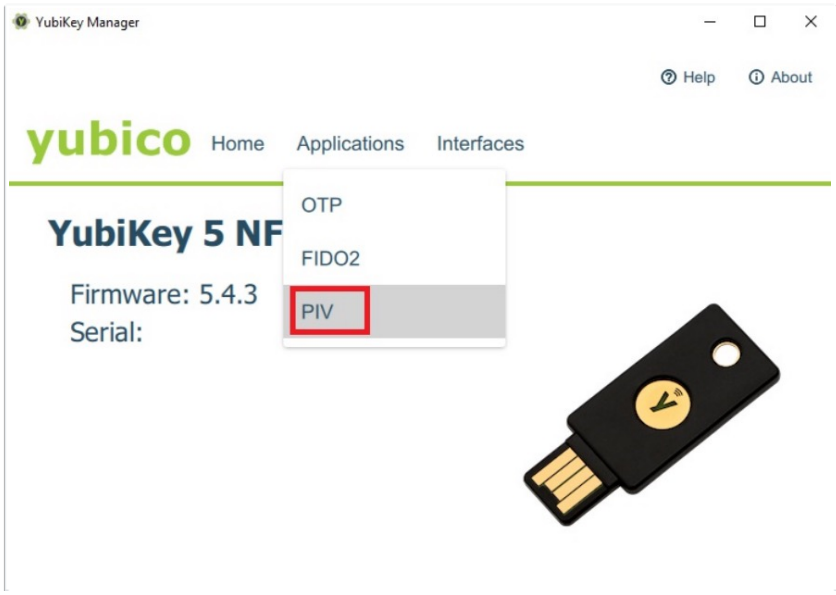

YubiKey Manager
YubiKey 5 NFC (16816401)
Help
About
yubico
Home
Applications
Interfaces
Set FIDO2 PIN
Home / FIDO2 / Set PIN
New PIN
Confirm PIN
Back
Set PIN

Zmena továrenského PIV PINu v YubiKey Manageri

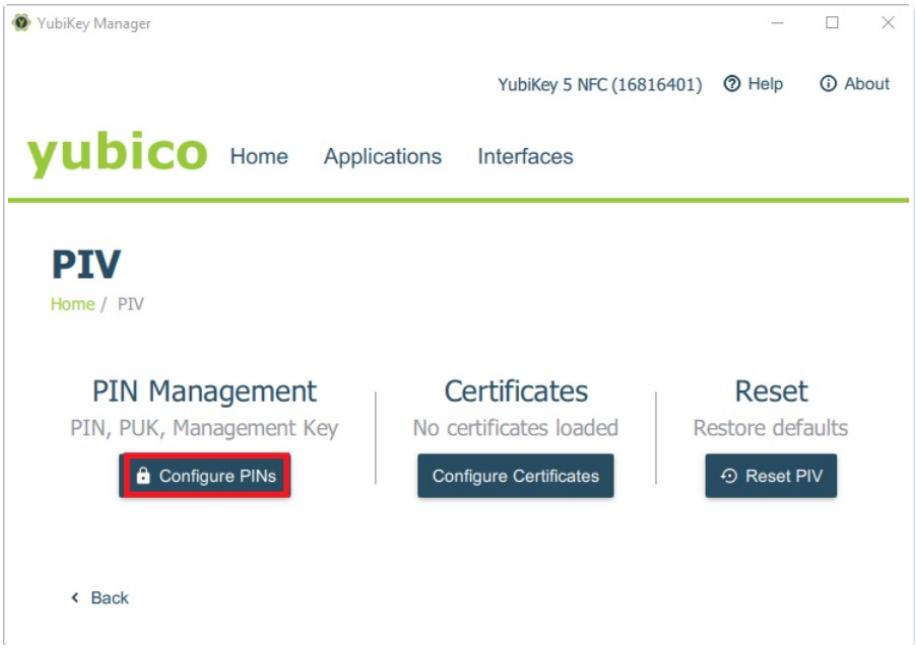
1. Spustíme YubiKey Manager ako správca pomocou Spustiť ako správca.



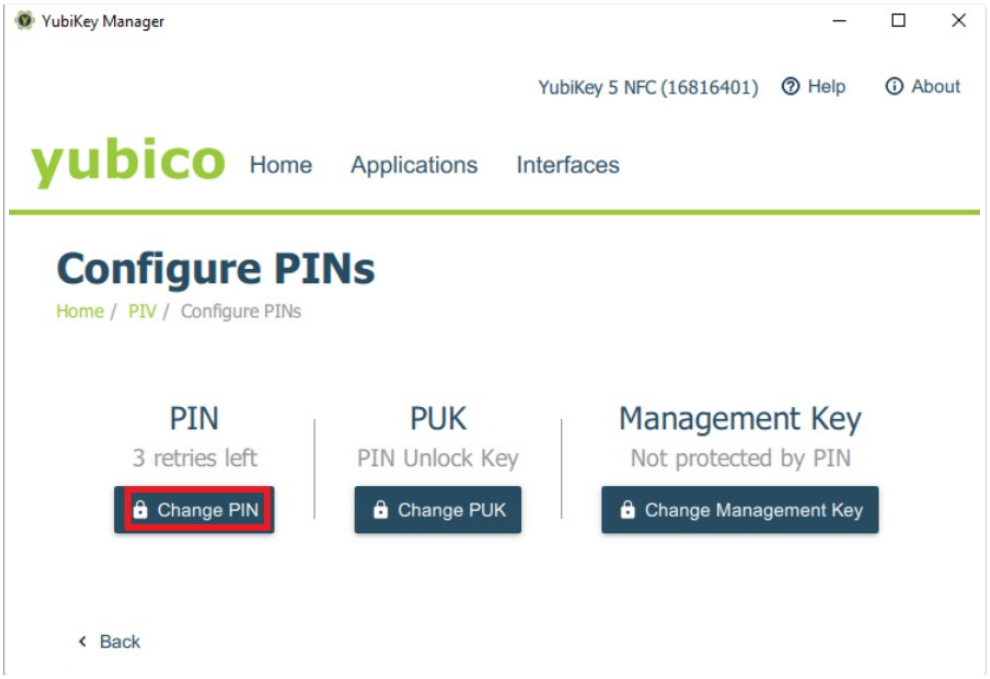
2. Zvolíme voľbu PIV.



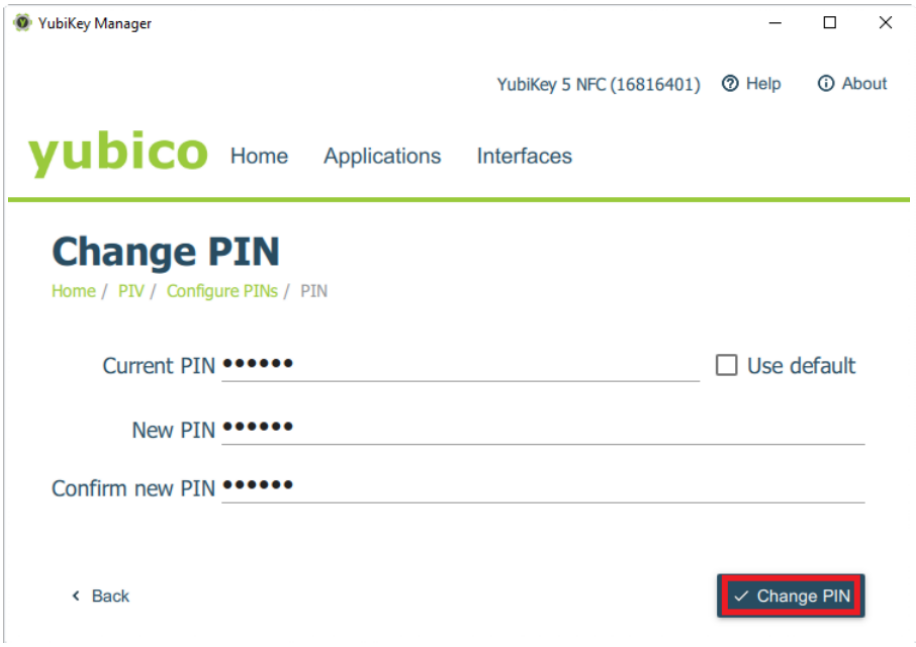
3. Klikneme na Configure PINs.



4. Klikneme na Change PIN.

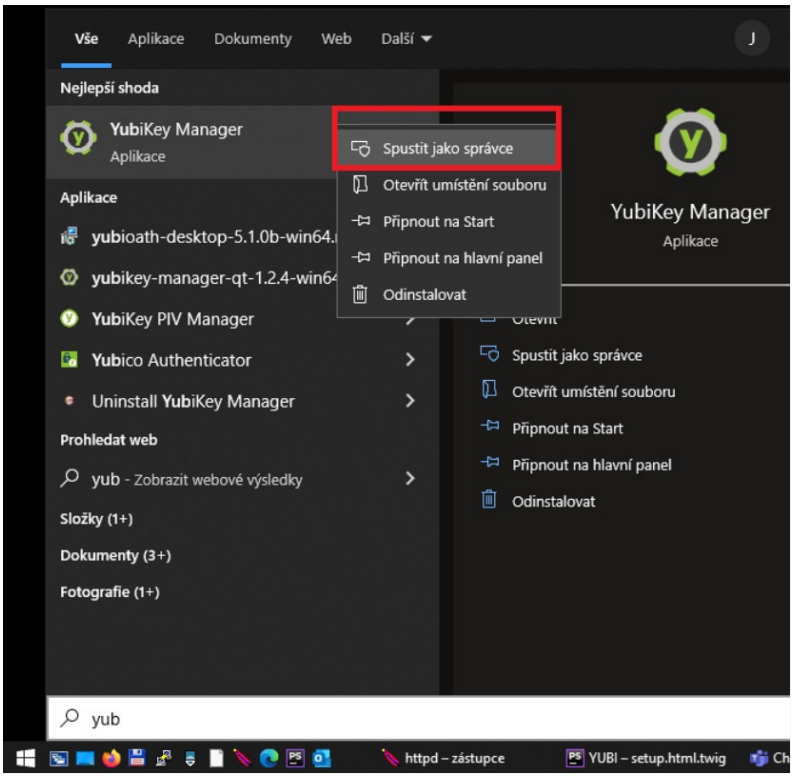


5. Do poľa Current PIN zadáme predvolený PIN (alebo zaškrtneme voľbu Use default), nový PIN (6-8 alfanumerických znakov) zadáme do poľa New PIN a potvrdíme v poli Confirm new PIN. Pomocou tlačidla Change PIN zmenu uložíme.

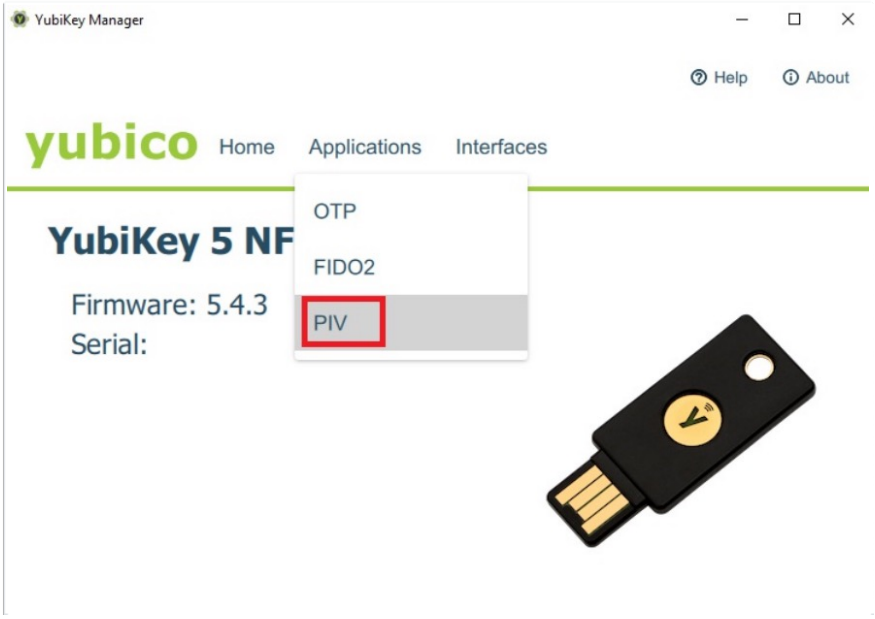


Zmena továrenského PIV PUK kódu v YubiKey Manageri

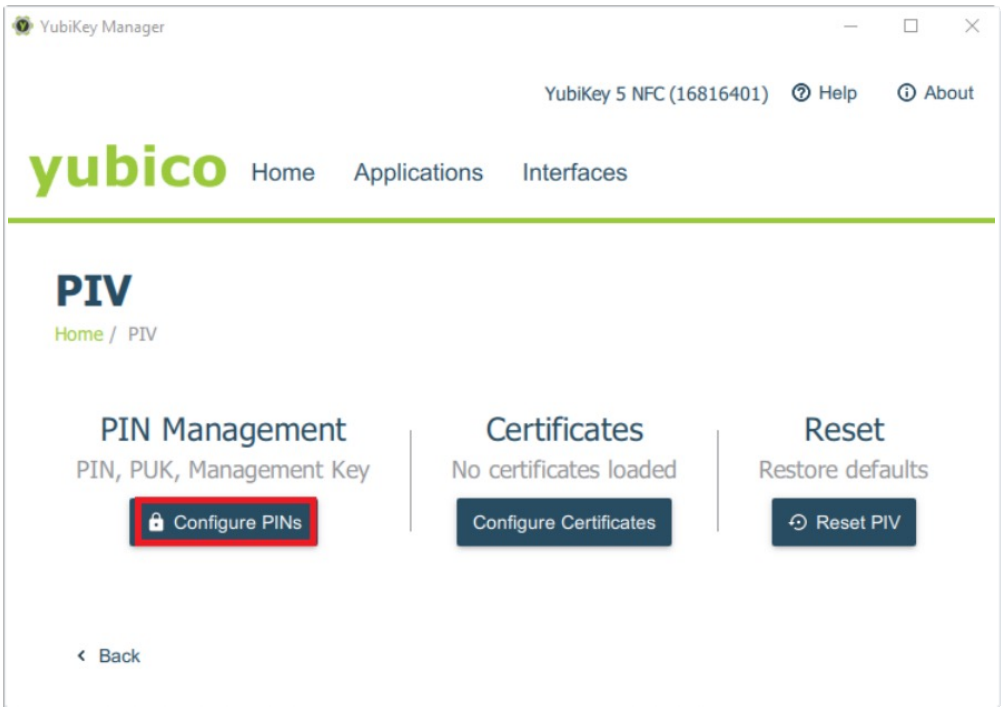
1. Spustíme YubiKey Manager ako správca pomocou Spustiť ako správca.



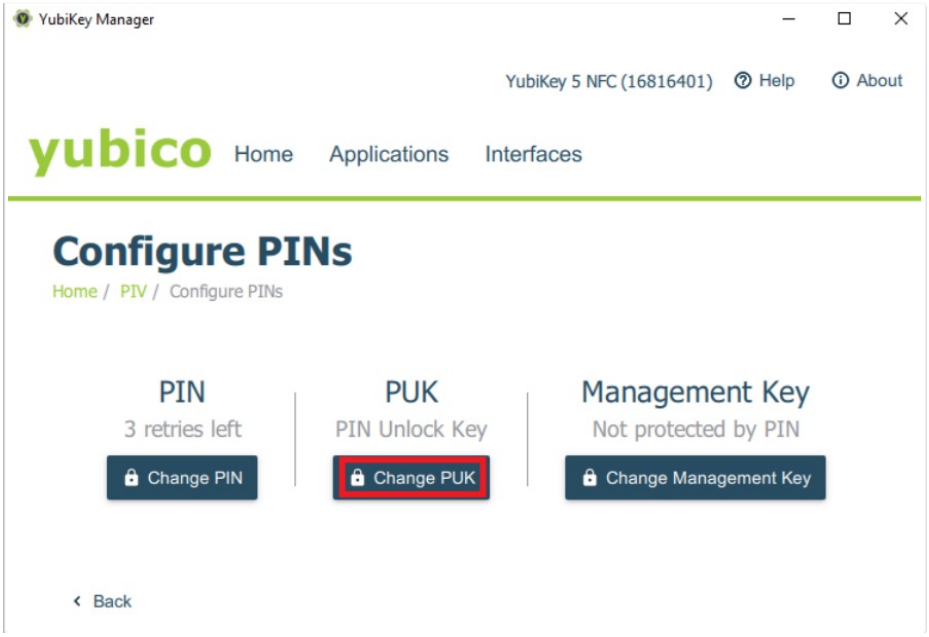
2. Zvolíme voľbu *PIV*.



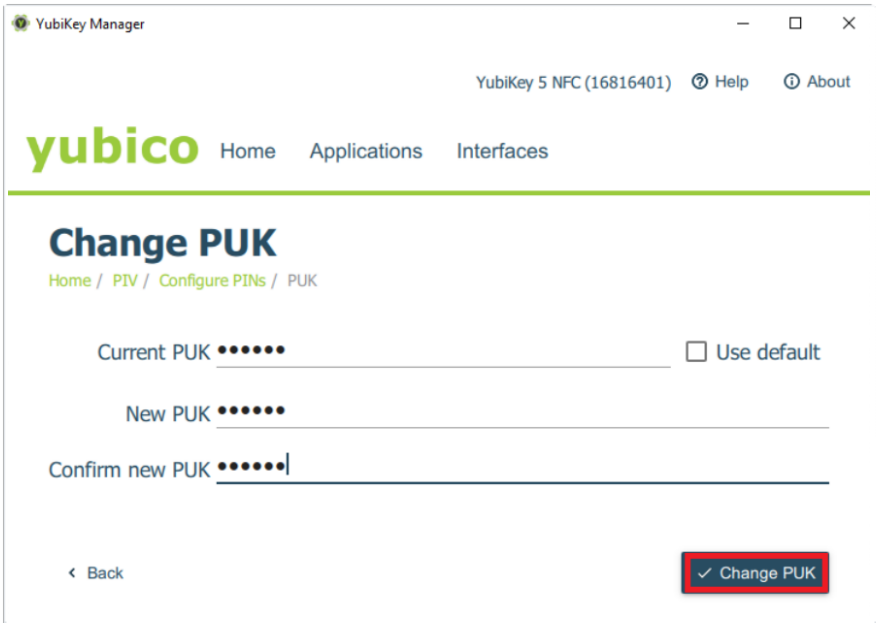
3. Klikneme na *Configure PIN*s.



4. Klikneme na *Change PUK*.

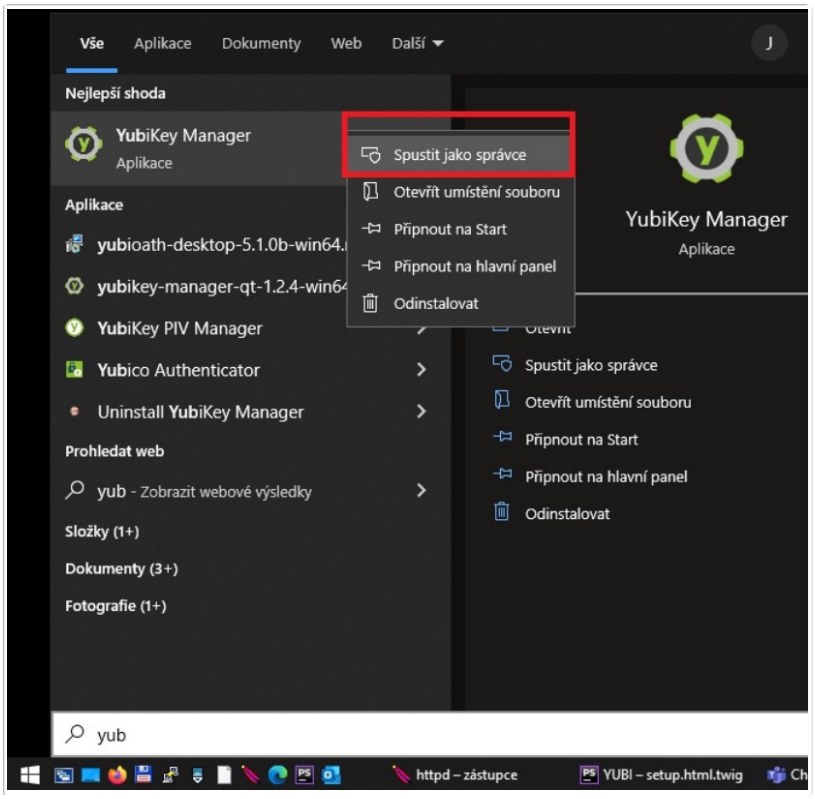


5. Do poľa Current PUK zadáme predvolený PUK (alebo zaškrtneme voľbu Use default), nový PUK (6-8 alfanumerických znakov) zadáme do poľa New PUK a potvrdíme v poli Confirm new PUK. Pomocou tlačidla Change PUK zmenu uložíme.

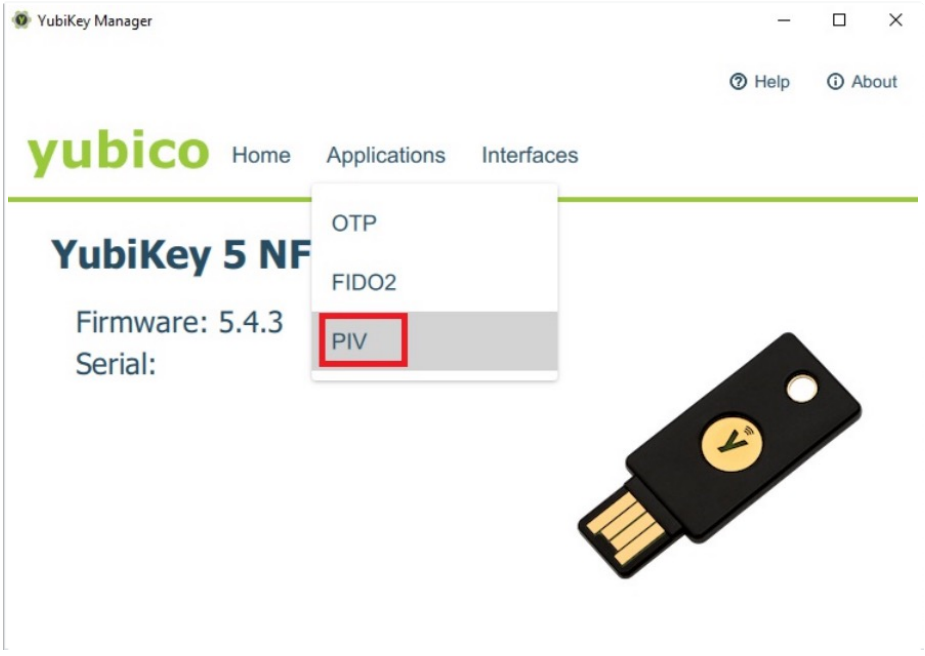


Zmena továrenského PIV Management Key v YubiKey Manageri

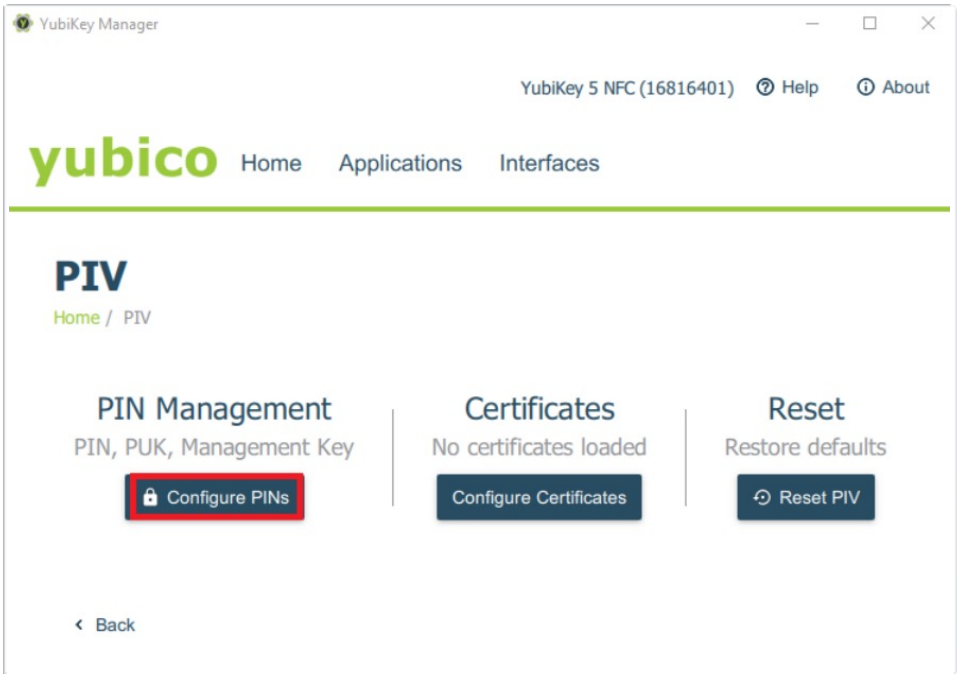
1. Spustíme YubiKey Manager ako správca pomocou Spustiť ako správca.



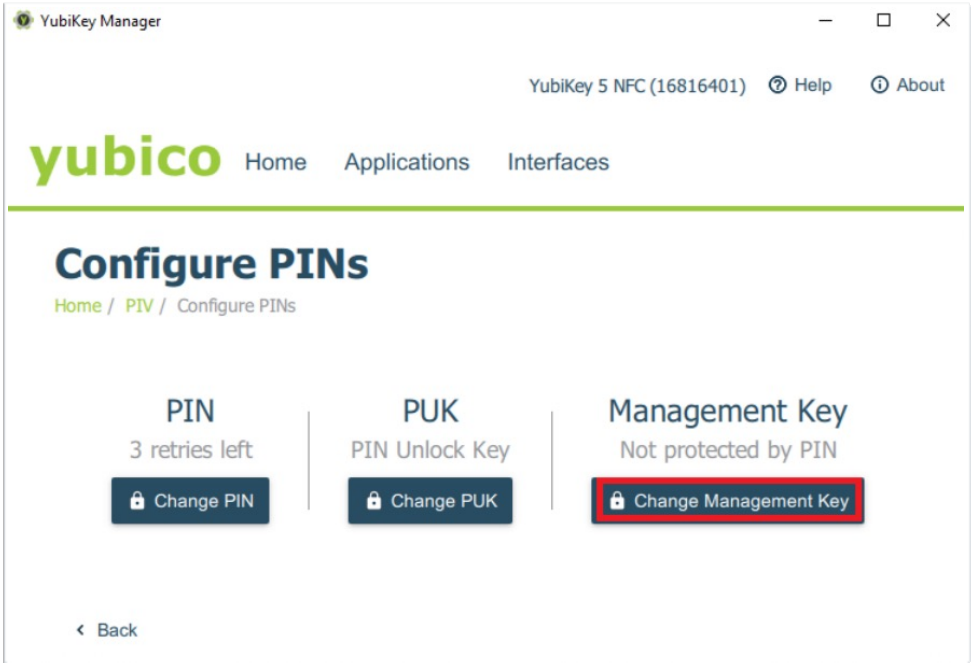
2. Zvolíme voľbu *PIV*.



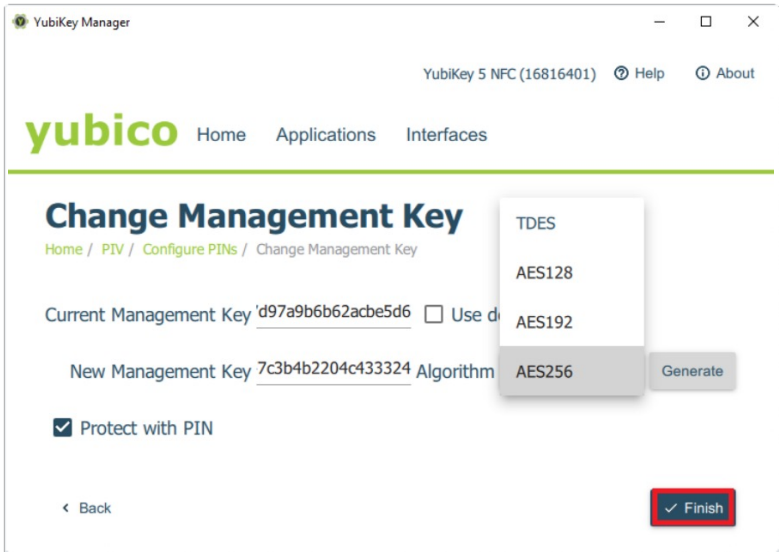
3. Klikneme na Configure PINs.



4. Klikneme na Change Management Key.

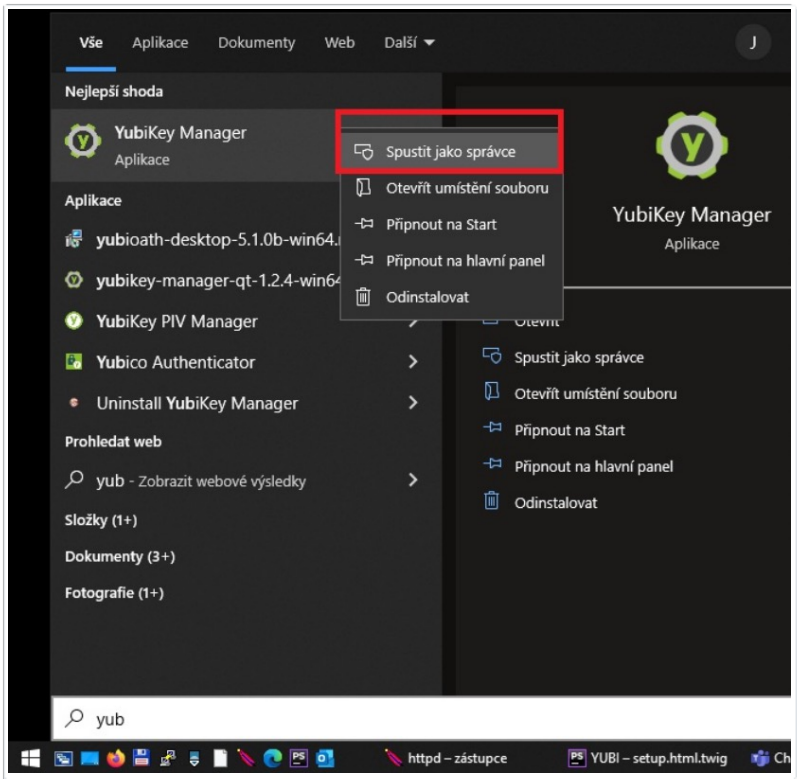


5. Do poľa *Current Management Key* zadáme predvolený Management Key (alebo zaškrtneme voľbu Use default), nový Management Key (48 hexadecimálnych znakov) zadáme do poľa *New Management Key*, prípadne pomocou tlačidla *Generate* si necháme kľúč vygenerovať - vo voľbe Algorithm si môžeme vybrať algoritmus, ktorým má byť kľúč vytvorený. Ak chceme zmenu tohto kľúča zabezpečiť PIV PINom, zaškrtneme voľbu Protect with PIN. Pomocou tlačidla *Finish* zmenu uložíme.



Vygenerování Authentication certifikátu v YubiKey Manageru

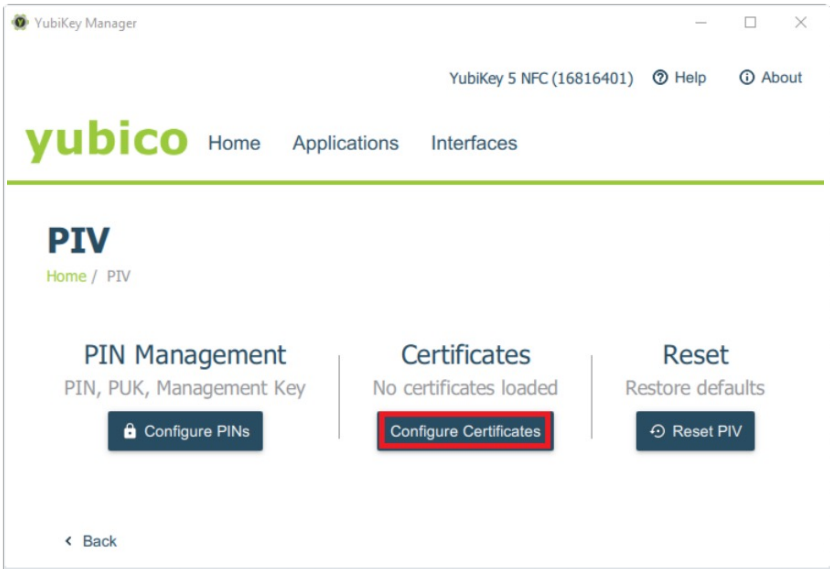
1. Spustíme YubiKey Manager jako správce pomocí *Spustit jako správce*.



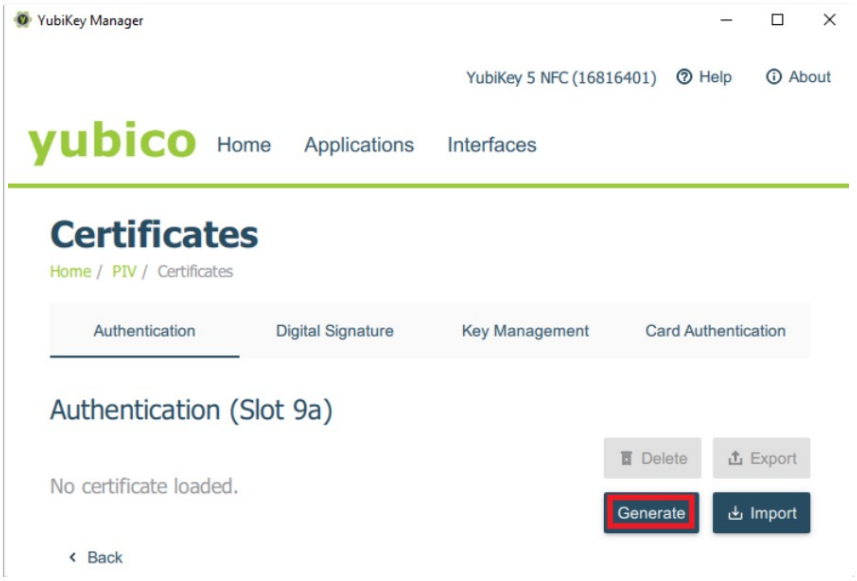
2. Zvolíme voľbu PIV.



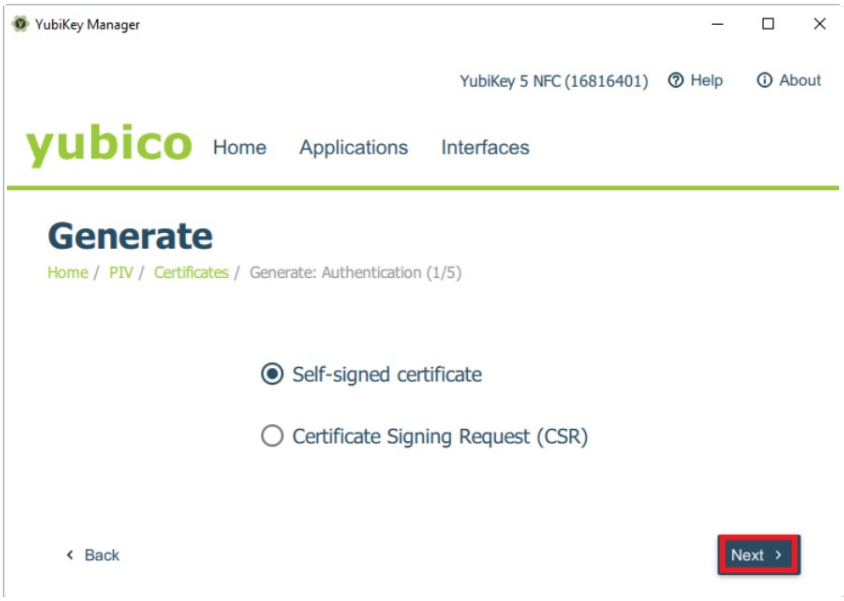
3. Klikneme na Configure Certificates.



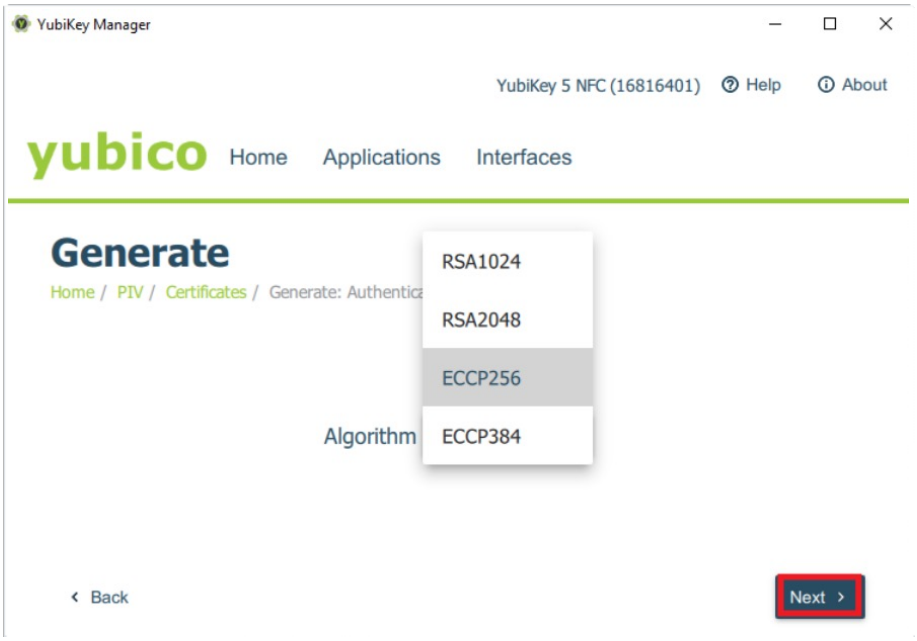
4. Vyberieme certifikát Authentication (Slot 9a) a klikneme na Generate.



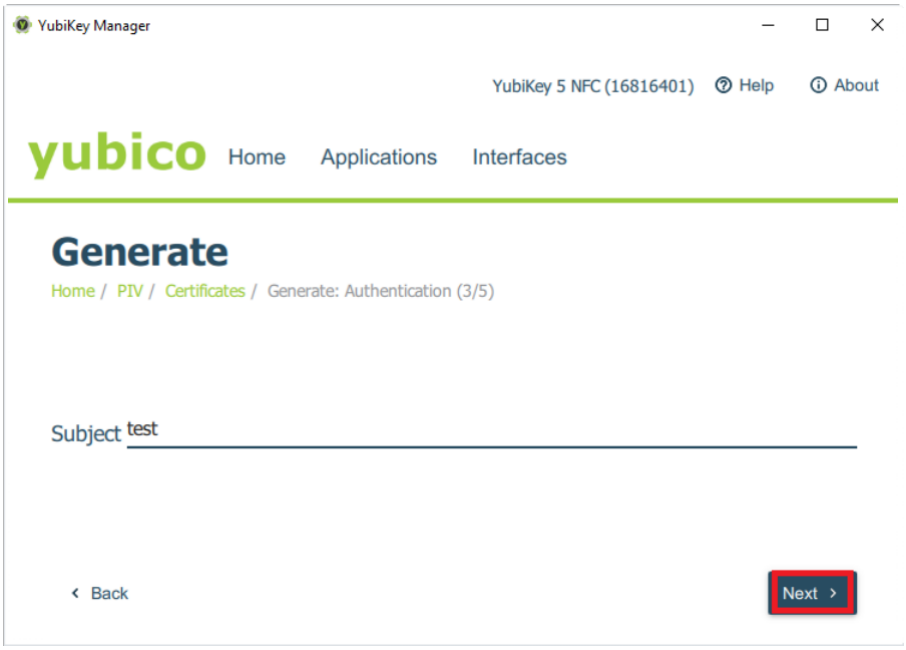
5. Vyberieme Self-signed certificate a klikneme na Next.



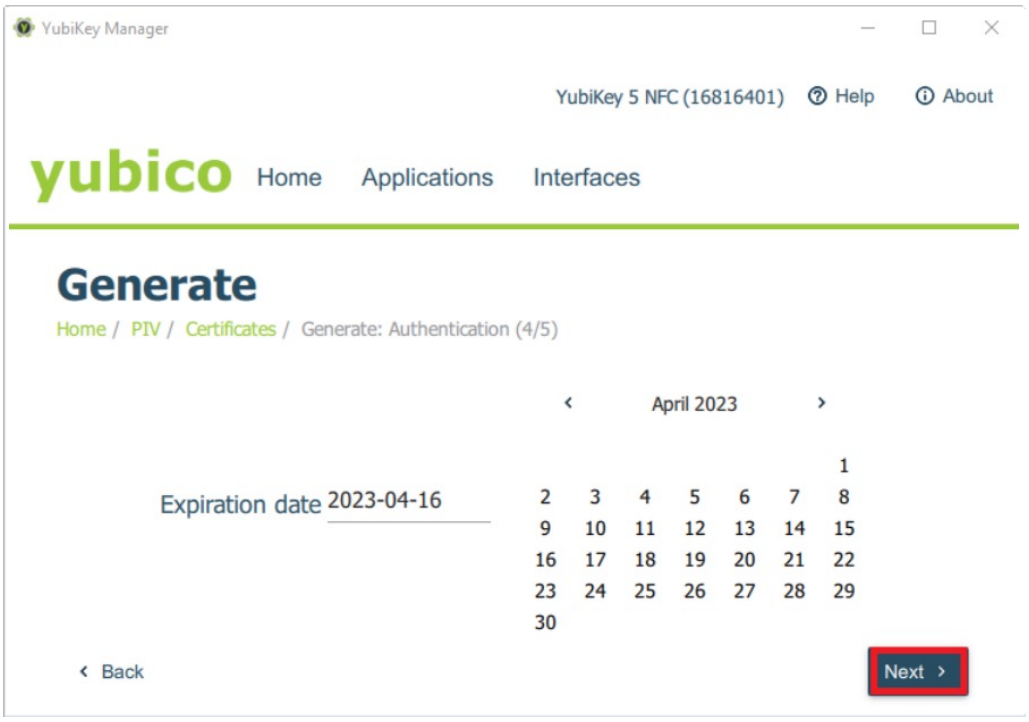
6. Vyberieme algoritmus generovania a klikneme na Next.



7. Zvolíme si Subject (ideálne vaša emailová adresa) a klikneme na Next.



8. Zvolíme dátumexpirácie Expiration date a klikneme na Next.



9. Zhrnutie potvrdíme tlačidlom Generate.

Často kladené otázky

Je možné na token uložiť kvalifikovaný certifikát?

- *Bohužiaľ zatiaľ nie.*

Je možné používať tokeny YubiKey ako správcu hesiel (password manager)?

- *Nie. Niektorí správcovia hesiel však podporujú dvojfaktorové prihlasovanie a pomocou tokenu **YubiKey 5C NFC** je možné zabezpečiť prístup k nim.*

Je možné na token ukladať súbory?

- *Nie. **YubiKey 5C NFC** nie je USB flash disk. Na token je možné ukladať iba certifikáty a ďalšie dáta vyžadované podporovanými protokolmi (napríklad OTP seed).*

Je možné na token uložiť kryptomeny?

- *Nie. **YubiKey 5C NFC** nie je kryptopeňaženka. Pomocou tokenu **YubiKey 5C NFC** je však možné zabezpečiť prihlasovanie do kryptomenových búrz, ktoré podporujú dvojfaktorové overovanie pomocou bezpečnostného tokenu.*

YubiKey Manager nerozpoznáva môj nový token. Prečo?

- *Spúšťate aplikáciu **YubiKey Manager** ako správca? Používate najnovšiu verziu aplikácie **YubiKey Manager**? Novšie vydané tokeny môžu vyžadovať novšiu verziu aplikácie.*

Pripojil(a) som YubiKey 5C NFC k zariadeniu, ktoré je pripojené k počítaču a má aj USB port. YubiKey 5C NFC však nefunguje správne.

- *Pripojte token **YubiKey 5C NFC** priamo do USB portu vášho počítača.*

YubiKey sa zobrazí v aplikácii Yubico Authenticator alebo YubiKey Manager, ale nefunguje správne.

- *Skontrolujte, či používate najnovšie verzie aplikácií **Yubico Authenticator** a **YubiKey Manager**. Ak problém pretrváva, odpojte token, pripojte ho priamo do USB portu počítača a skúste ho znovu načítať v aplikácii.*