

Czy YubiKey NFC można użyć w eLoginie?



Politechnika Poznańska

Wydział Informatyki i Telekomunikacji

Autor

141327

15 czerwca 2023 r.



Ekran konfiguracji 2FA:

Włączenie uwierzytelniania dwuskładnikowego

Proces włączania drugiego składnika uwierzytelniania składa się z trzech kroków: zainstalowania aplikacji do obsługi 2FA, dodania Twojego konta do tej aplikacji i potwierdzenia za pomocą wygenerowanego przez aplikację kodu. Postępuj zgodnie z poniższymi instrukcjami.

Instalacja aplikacji 2FA

Aby skorzystać z uwierzytelniania drugim składnikiem, należy zainstalować na smartfonie specjalną aplikację. Poniżej znajduje się lista najpopularniejszych aplikacji do obsługi 2FA, wybierz jedną z nich, zainstaluj i skonfiguruj.

- o Authy - **Android, iOS**
- o Aegis Authenticator - **Android**
- o Google Authenticator - **Android, iOS**
- o Microsoft Authenticator - **Windows, Android, iOS**

Dodanie konta do aplikacji 2FA

Dodanie konta w aplikacji 2FA wiąże się ze zeskanowaniem kodu QR zawierającego specjalny klucz konfiguracyjny oraz dodatkowe informacje o koncie (nazwa i login). Jeśli nie masz możliwości zeskanowania kodu QR, aplikacja powinna umożliwić ręczne wprowadzenie klucza konfiguracyjnego - skopiuj go korzystając z przycisku poniżej (nazwę i login musisz wpisać we własnym zakresie).

Zeskanuj



lub

 Skopiuj klucz konfiguracyjny

Potwierdzenie

Aplikacja 2FA co pół minuty generuje nowy sześciocyfrowy kod dla Twojego konta. Aby potwierdzić, że konto zostało poprawnie dodane w aplikacji, wpisz poniżej bieżący kod i zatwierdź formularz.

* Kod drugiego składnika ⓘ

Zatwierdź

Anuluj



Kody zapasowe

Poprawnie włączono uwierzytelnianie dwuskładnikowe na Twoim koncie. Zalecamy wygenerowanie kodów zapasowych.

Wygenerowanie kodów zapasowych

Kody zapasowe mogą zostać użyte zamiast kodu wygenerowanego przez aplikację 2FA w sytuacji, gdy dostęp do aplikacji nie jest możliwy (np. zagubiony smartfon). Zalecamy wygenerowanie kodów zapasowych, jeżeli Twoja aplikacja 2FA nie ma opcji przywracania jej ustawień z kopii zapasowej. **Kody zapasowe powinny być chronione przed niepożądanym dostępem, na takiej samej zasadzie jak Twoje hasło.**

Aby wygenerować kody zapasowe, musisz podać bieżący kod wygenerowany przez aplikację 2FA.

* Kod drugiego składnika 

✓ Zatwierdź

↶ Anuluj



Zaufane przeglądarki

Zaufana przeglądarka to taka, w której nie trzeba wprowadzać kodu drugiego składnika uwierzytelniania podczas logowania w serwisie eLogin. Informacja ta przechowywana jest za pomocą mechanizmu ciasteczek (ang. cookies). Długo nieużywane przeglądarki będą automatycznie usuwane z listy zaufanych. Przeglądarkę do listy zaufanych możesz dodać podczas logowania, na etapie pytania o kod drugiego składnika uwierzytelniania.

YubiKey NFC

YubiKey NFC to fizyczny klucz USB/NFC, który zapewnia zaawansowaną ochronę przed phishingiem i służy do uwierzytelniania. Co więcej, eliminuje ryzyko przechwycenia kont w systemach komputerowych i usługach online. Ten klucz sprzętowy oferuje silne uwierzytelnianie jedno-, dwu- i wieloskładnikowe.





Kluczowe cechy

- Jeden klucz, który zabezpiecza wiele usług
- Silne uwierzytelnianie jedno-, dwu- i wieloskładnikowe
- Łatwe i szybkie uwierzytelnienie przy pomocy dotknięcia przycisku na kluczu YubiKey lub zbliżenia do urządzenia wspierającego NFC
- Wsparcie dla wielu protokołów z użyciem jednego klucza
- Cztery razy szybszy niż hasła jednorazowe (OTP)

WebAuthn

External authenticator



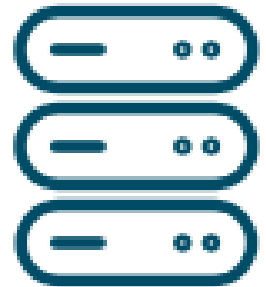
Client / Platform



Internal authenticator



Relying party





Założenia

- Możliwość dodania wielu kluczy,
- Kody zapasowe
- Zaufane przeglądarki
- TOTP powinno pozostać jako jedna z opcji 2FA, na równi z kluczami
- Możliwość użycia TOTP podczas logowania
- Możliwość wylistowania kluczy
- Możliwość zmiany nazwy klucza
- Możliwość usuwania kluczy



Uwierzytelnianie dwuskładnikowe

Uwierzytelnienie do każdej aplikacji może składać się z kilku etapów (składników). W serwisie eLogin, domyślnie wymagany jest jeden składnik - hasło (zamiennie z logowaniem Windows oraz logowaniem certyfikatem). W takiej sytuacji wystarczy, że ktoś niepowołany pozna Twoje hasło i będzie mógł zalogować się na Twoje konto.

Status: **włączone**

[Wyłącz drugi składnik](#)

Kody zapasowe mogą zostać użyte zamiast kodu wygenerowanego przez aplikację 2FA w sytuacji, gdy dostęp do aplikacji nie jest możliwy (np. zagubiony smartfon). Zalecane jest ich wygenerowanie.

Kody zapasowe: **wygenerowane**

[Unieważnij kody zapasowe](#)

Zaufane przeglądarki to takie, w których nie trzeba wprowadzać kodu drugiego składnika uwierzytelniania podczas logowania w serwisie eLogin.

Zaufane przeglądarki: **0**

[Zarządzaj zaufanymi przeglądarkami](#)

Lista kluczy:

Nazwa klucza

data utworzenia:
01/01/2022 12:41:05

data ostatniego użycia:
01/01/2022 12:41:05

 **RENAME**  **REMOVE**

[Dodaj nowy klucz](#)

Ekran konfiguracji



Ekran uwierzytelnienia drugim składnikiem

Wprowadź kod uwierzytelniający:

Użyj tego klucza

Wybierz klucz:

Nazwa klucza

data utworzenia:
01/01/2022 12:41:05

data ostatniego użycia:
01/01/2022 12:45:08

Użyj tego klucza

Nazwa klucza 2

data utworzenia:
07/02/2022 14:41:05

data ostatniego użycia:
01/01/2023 19:28:05

Użyj tego klucza

Skorzystaj z kodu zapasowego

Anuluj

Pomoc

Ekran konfiguracji