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.

- Authy - **Android**, **iOS**
- Aegis Authenticator - **Android**
- Google Authenticator - **Android**, **iOS**
- 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

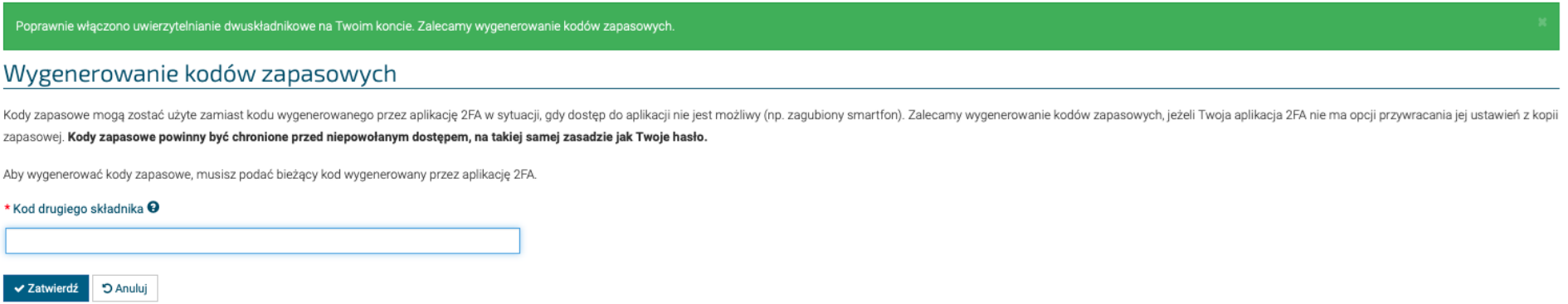
Potwierdzenie

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



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.

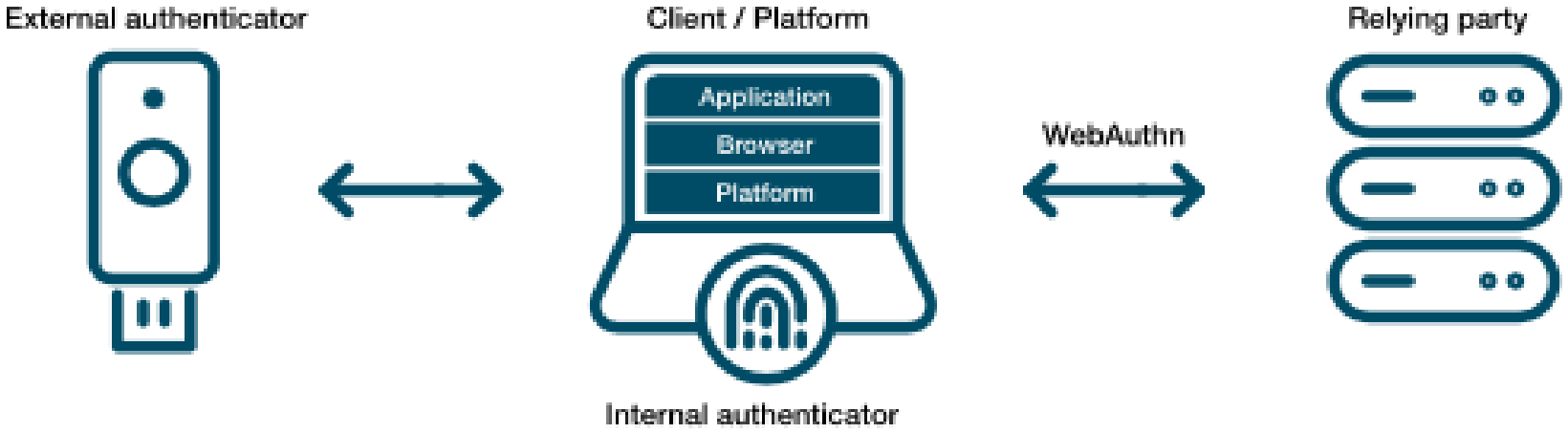
YubiKey NFC

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)

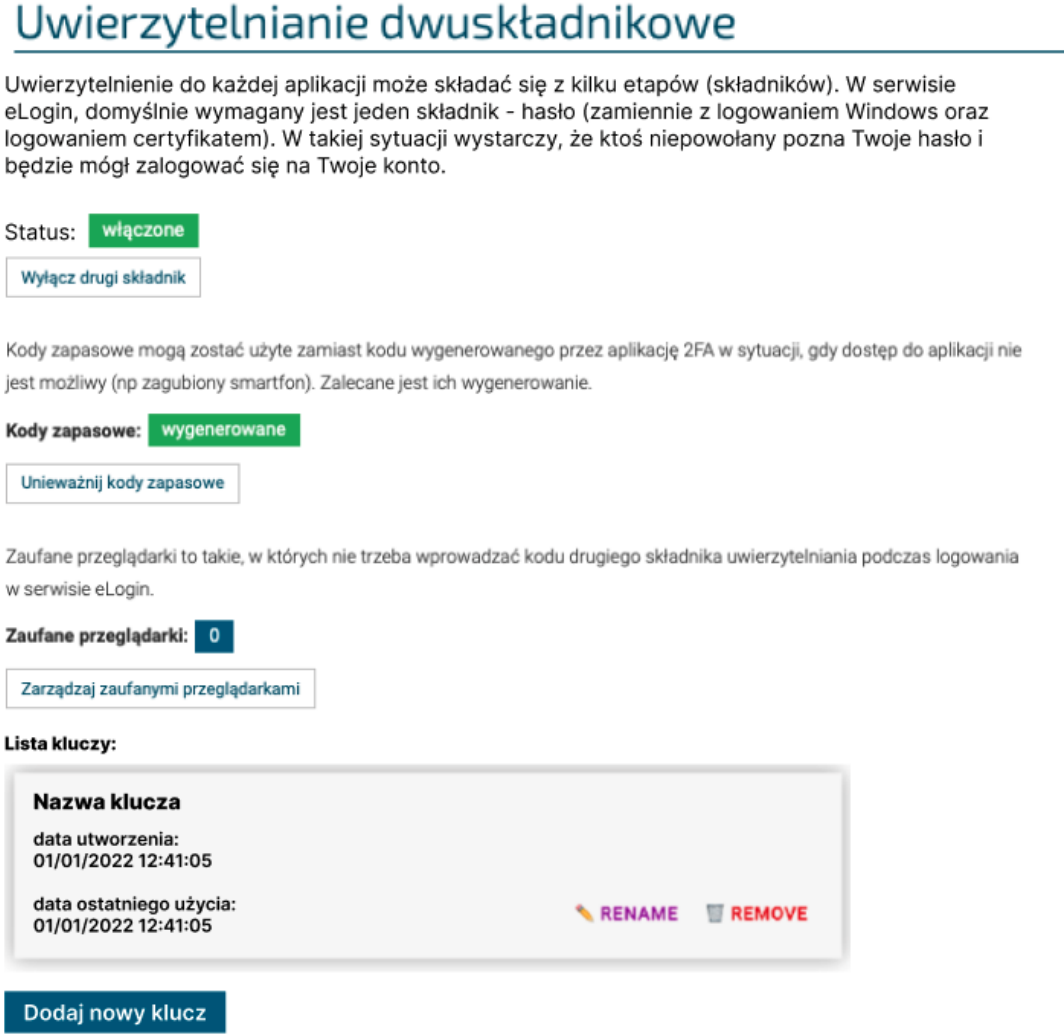
WebAuthn


External authenticator
Client / Platform
Relying party
Application
Browser
Platform
WebAuthn
Internal authenticator

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

Ekran konfiguracji



Ekran konfiguracji