

System Centralnego Uwierzytelniania

INSTRUKCJA KONFIGURACJI DRUGIEGO SKŁADNIKA UWIERZYTELNIANIA (2FA)

Spis treści

1.	Rejestr zmian	2
2.	Cel	3
3.	Definicje	3
4.	Blokowy schemat działania	4
5.	Wybór drugiego składnika logowania	5
6.	Wybór metody uwierzytelniania	6
7.	Logowanie z użyciem aplikacji OTP	7
7.1	Rejestracja aplikacji	7
7.2	Kody zapasowe	7
7.3	Aktywacja	7
7.4	Kolejne logowania	9
8.	Logowanie z użyciem klucza sprzętowego (FIDO)	9
8.1	Rejestracja	9
8.2	Konfiguracja w systemie Windows	9
8.3	Zakończenie	11
	Kolejne logowania	11
9.	Zmiana metody uwierzytelniania	12
9.1	Zmiana MFA	12
9.2	Usunięcie zapisanych urządzeń logowania dwuskładnikowego	13
10.	Przykładowe aplikacje OTP	14
10.1	dla systemu Android	14
10.2	dla systemu iOS	14
10.3	dla systemu Windows	15
10.4	dla systemu Linux	16

1. Rejestr zmian

<i>Nr wersji</i>	<i>Data</i>	<i>Zmiana</i>
1.01S	29.04.2026	Utworzenie dokumentu
1.02S	05.05.2026	Aktualizacja informacji zawartych w instrukcji. Dodanie informacji w zakresie wykorzystania Klucza tajnego do zarejestrowania w aplikacji OTP oraz konieczności synchronizacji czasu na urządzeniu generującym kody.

2. Cel

Celem wprowadzenia autoryzacji dwuskładnikowej jest znaczące podniesienie poziomu bezpieczeństwa dostępu do systemów i danych poprzez zastosowanie dodatkowego, niezależnego mechanizmu potwierdzania tożsamości użytkownika. Dzięki wykorzystaniu dwóch różnych kategorii czynników uwierzytelniania 2FA minimalizuje ryzyko nieuprawnionego dostępu wynikającego z przechwycenia, odgadnięcia lub wycieku hasła. Wprowadzenie 2FA wzmacnia ochronę zasobów Uczelni, ogranicza skutki potencjalnych incydentów bezpieczeństwa oraz zwiększa odporność środowiska na ataki socjotechniczne i cyberzagrożenia.

Należy pamiętać, że żadna metoda zabezpieczeń nie gwarantuje pełnej ochrony. Zastosowanie dodatkowego składnika uwierzytelniania znacząco jednak podnosi poziom bezpieczeństwa i utrudnia nieautoryzowany dostęp.

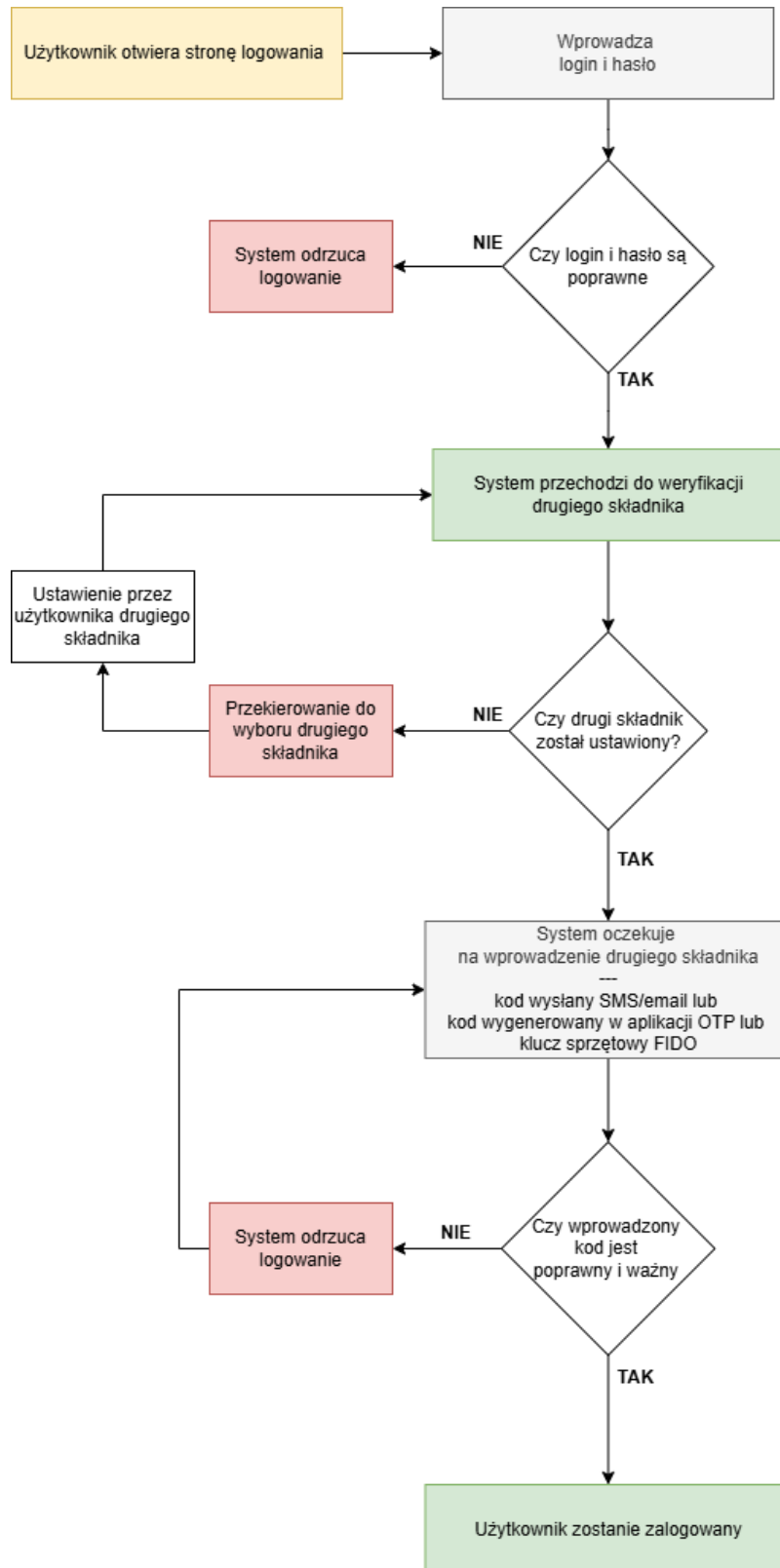
3. Definicje

- a) **System Centralnego Uwierzytelniania** (Central Authentication Service) – to scentralizowany system uwierzytelniania, który umożliwia użytkownikom jednokrotne logowanie (Single Sign-On, SSO) do wielu niezależnych aplikacji i usług. Aplikacja CAS działa jako zaufany pośrednik między użytkownikiem a aplikacjami, zapewniając bezpieczne przekazywanie informacji o tożsamości bez konieczności ponownego podawania danych logowania.
- b) **Uwierzytelnianie dwuskładnikowe** (2FA, Two-Factor Authentication) to metoda uwierzytelniania, w której użytkownik potwierdza swoją tożsamość za pomocą dwóch niezależnych czynników pochodzących z różnych kategorii:
 - coś, co zna (np. hasło, PIN),
 - coś, co posiada (np. klucz FIDO, telefon z aplikacją OTP),
 - coś, czym jest (np. odcisk palca, rozpoznawanie twarzy).

Zastosowanie dwóch odrębnych czynników znacząco zwiększa poziom bezpieczeństwa, ponieważ przejęcie jednego z nich nie umożliwia uzyskania dostępu do systemu. 2FA ogranicza ryzyko nieautoryzowanego logowania wynikającego z wycieku haseł, ataków phishingowych czy przechwycenia danych.

- c) **Aplikacja OTP** (One-Time Password) – to aplikacja generująca jednorazowe hasła służące do uwierzytelniania dwuskładnikowego (2FA) lub wieloskładnikowego (MFA). OTP jest hasłem ważnym tylko przez krótki czas lub jednorazowe użycie, co znacząco zwiększa bezpieczeństwo logowania do systemów i usług.
- d) **Klucz sprzętowy** - Urządzenie fizyczne zgodne ze standardami FIDO (Fast IDentity Online), służący do silnego, kryptograficznego uwierzytelniania użytkownika bez użycia haseł lub jako drugi czynnik w procesie logowania. Klucz sprzętowy wykorzystuje mechanizmy kryptografii asymetrycznej, generując unikalną parę kluczy dla każdej usługi, co zapewnia wysoki poziom ochrony przed phishingiem, przechwyceniem danych i atakami typu man-in-the-middle.

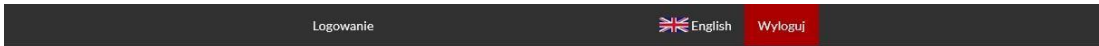
4. Blokowy schemat działania




5. Wybór drugiego składnika logowania

Podczas pierwszego logowania do Systemu Centralnego Uwierzytelniania przy użyciu loginu i hasła, lub każdorazowo przy zmianie drugiego składnika wywołanej przez użytkownika zostanie wyświetlony komunikat o konieczności wyboru drugiego składnika uwierzytelniania.

Jeżeli drugi składnik został już wcześniej skonfigurowany, proces logowania będzie kontynuowany zgodnie z konfiguracją ustawioną wcześniej przez użytkownika.





Wybór drugiego składnika uwierzytelniającego.

Logowanie zostało wstrzymane. W celu zwiększenia bezpieczeństwa konta wymagane jest włączenie uwierzytelniania dwuskładnikowego (2FA). Oznacza to, że oprócz hasła konieczne będzie potwierdzenie logowania przy użyciu dodatkowej metody weryfikacji.

Dostępne metody uwierzytelniania

- SMS / E-mail Po wybraniu tej metody zostaniesz wylogowany, a przy następnym logowaniu otrzymasz jednorazowy kod w wiadomości SMS i/lub na prywatny adres e-mail. Kod należy przepisać w formularzu logowania, aby potwierdzić dostęp do konta. Opcja dostępna tylko dla użytkowników, którzy mają zapisany numer telefonu lub prywatny adres e-mail w systemie kadrowym Uczelni.
- Aplikacja uwierzytelniająca (OTP) Specjalna aplikacja na telefonie komórkowym, która generuje jednorazowe kody zmieniające się co kilkadziesiąt sekund. Podczas logowania należy wpisać aktualny kod wyświetlany w aplikacji (np. Microsoft Authenticator, Google Authenticator, etc.). Po wybraniu tej opcji przy następnym logowaniu zostaniesz poproszony o skonfigurowanie tej Aplikacji OTP.
- Klucz sprzętowy (FIDO) Fizyczny klucz bezpieczeństwa (np. USB lub NFC), który po podłączeniu do komputera lub zbliżeniu do telefonu potwierdza tożsamość użytkownika i umożliwia dokończenie procesu logowania.

Wybierz preferowaną metodę uwierzytelnienia dwuskładnikowego:

OTP autetykator Klucz sprzętowy

6. Wybór metody uwierzytelniania

Logowanie zostanie wstrzymane do momentu wyboru metody 2FA.

Studenci mają do wyboru 2 metody uwierzytelniania.

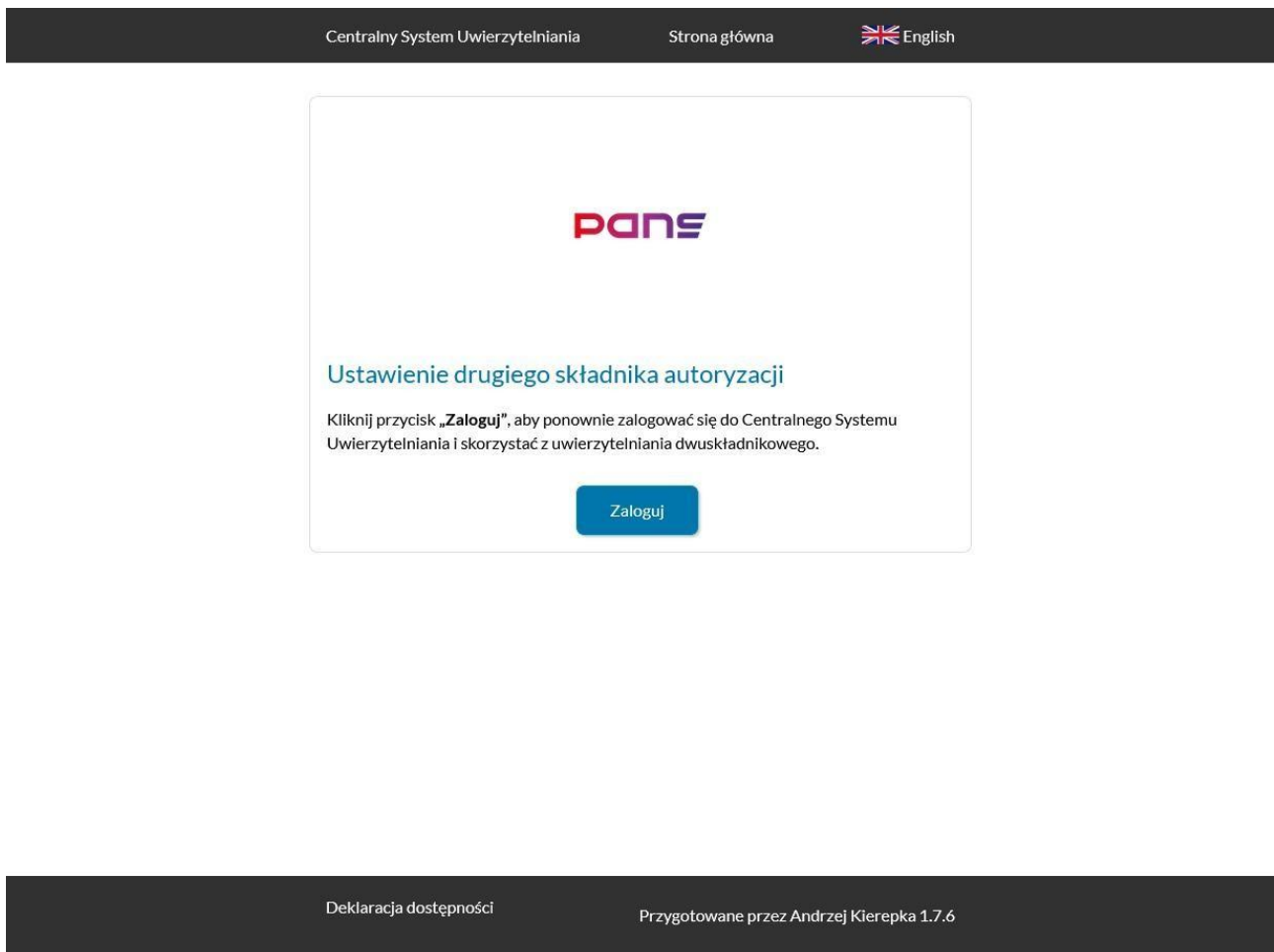
Dostępne metody:

- Aplikacja uwierzytelniająca (OTP)
- Klucz sprzętowy (FIDO)

⚠ Uwaga, wybranie drugiego składnika w postaci Aplikacji OTP lub Klucza sprzętowego i przerwanie procesu w trakcie (nie dokończenie procesu jego ustawiania), spowoduje brak możliwości zalogowania się do systemu SCU.

W takiej sytuacji prosimy o kontakt z Działem Bezpieczeństwa i Utrzymania Systemów Informatycznych (budynek J2 - wejście od strony parkingu, tel. 16 624 46 39) celem przywrócenia możliwości zalogowania.

Po wybraniu preferowanej metody użytkownik zostanie automatycznie wylogowany, a ustawienie zapisane w systemie.



The screenshot shows a dark navigation bar at the top with the text 'Centralny System Uwierzytelniania', 'Strona główna', and a language selector 'English' with a flag icon. The main content area is white and contains the PANS logo at the top. Below the logo, the heading 'Ustawienie drugiego składnika autoryzacji' is displayed. Underneath, there is a paragraph of text: 'Kliknij przycisk „Zaloguj”, aby ponownie zalogować się do Centralnego Systemu Uwierzytelniania i skorzystać z uwierzytelniania dwuskładnikowego.' At the bottom of this section is a blue button labeled 'Zaloguj'. At the bottom of the page, there is a dark footer bar containing the text 'Deklaracja dostępności' and 'Przygotowane przez Andrzej Kierepka 1.7.6'.

7. Logowanie z użyciem aplikacji OTP

7.1 Rejestracja aplikacji

Po ponownym zalogowaniu system wyświetli informację o braku rejestracji aplikacji OTP na koncie oraz kod QR do zeskanowania w aplikacji OTP (np. Google Authenticator, Microsoft Authenticator - Aplikacje należy pobrać na telefon lub komputer z miejsca właściwego dla danej platformy tzn. Google Play dla Androida, App Store dla iOS lub Microsoft Store dla Windowsa).

Uwaga: Kluczowe znaczenie ma prawidłowa synchronizacja czasu na urządzeniu, na którym generowane są kody. Maksymalna dopuszczalna rozbieżność wynosi 30. Przekroczenie tego limitu może skutkować odrzuceniem kodu – w przypadku większych różnic czasowych kod wygenerowany przez aplikację będzie uznany przez serwer za nieaktualny i nie zostanie zaakceptowany.

Wykaz przykładowych aplikacji znajduje i linków do nich znajduje się na końcu dokumentu.



PANS

Twoje konto nie jest zarejestrowane.

Zeskanuj poniższy kod query w aplikacji a następnie kliknij przycisk Potwierdź.



Tajny klucz do rejestracji to
DB3JJYQDAOVKLLINGFXIASNHJP7QKN

Kody zapasowe

Poniżej znajdziesz kody zapasowe, które możesz wykorzystać, jeśli nie masz dostępu do aplikacji OTP lub klucza bezpieczeństwa. Każdy kod może być użyty tylko raz. Zapisz je w bezpiecznym miejscu – np. w sejfie, menedżerze haseł lub wydrukuj. Uwaga: Jeśli stracisz dostęp do wszystkich kodów i drugiego składnika, konieczny będzie ponowne skonfigurowanie uwierzytelniania dwuskładnikowego.

97301126 57774254 61402945
95836123 47655770

Potwierdź Drukuj Anuluj

7.2 Kody zapasowe

System wygeneruje kody zapasowe, które należy zapisać (lub wydrukować). Umożliwią one logowanie w przypadku utraty dostępu do aplikacji lub telefonu.

Dokument jest poufny i powinien być przechowywany w

7.3 Aktywacja

1. Zeskanuj kod QR w aplikacji.

Uwaga: do rejestracji można również użyć tajnego klucza. Jeśli nie możesz zeskanować kodu QR, skopiuj ciąg znaków z pola „Tajny klucz” i wklej go do aplikacji uwierzytelniającej.

2. Kliknij „Potwierdź”.
3. Wprowadź:
 - kod (token) z aplikacji
 - przyjazną nazwę urządzenia (np. „Mój telefon”, możesz również zostawić nazwę podpowiedzianą przez system)

Potwierdź rejestrację konta

Potwierdź rejestrację konta, podając token z aplikacji uwierzytelniającej na swoim urządzeniu. Po zweryfikowaniu tokena rejestracja konta zostanie zakończona.

Token:*

Przyjazna nazwa
sleepy_jobs

Zarejestruj Anuluj

4. Kliknij „Zarejestruj”.
5. Następnie poczekaj, aż pojawi się nowy kod (nie używaj tego samego 6-cyfrowego kodu co w kroku 3.)
6. Wpisz aktualny kod z aplikacji i kliknij „Zaloguj się”.



PANS

Twoje wybrane urządzenie do dwuskładnikowej autentykacji to: sleepy_jobs.

Token:

Zaloguj się Anuluj

Możesz wybrać inne urządzenie do dwuskładnikowej autentykacji, jeżeli urządzenie sleepy_jobs nie jest prawidłowym urządzeniem.

Wybierz urządzenie

7.4 Kolejne logowania

Każde logowanie będzie wymagało:

- loginu
- hasła
- kodu z aplikacji

8. Logowanie z użyciem klucza sprzętowego (FIDO)

8.1 Rejestracja

System wyświetli pole do nadania nazwy urządzenia (można pozostawić domyślną lub wpisać własną), a następnie należy kliknąć „Zarejestruj”.

The screenshot shows a web interface for FIDO2 registration. At the top, there is a dark navigation bar with 'Logowanie' on the left, a language selector for 'English' with a flag icon, and a 'Wyloguj' button on the right. The main content area has the PANS logo at the top, followed by the title 'Rejestracja urządzenia'. Below the title is a paragraph of instructions: 'Przypisz przyjazną nazwę swojemu urządzeniu obsługującemu FIDO2, a następnie zarejestruj je w CAS do uwierzytelniania wieloskładnikowego. Po pomyślnym zakończeniu rejestracji urządzenia zostaniesz automatycznie przekierowany do kolejnego kroku, aby załogować się przy użyciu tego urządzenia.' There is a text input field labeled 'Nazwa urządzenia*' containing the text 'unruffled_buck'. Below the input field is a blue button labeled 'Zarejestruj'. Underneath, there is a note: 'Możesz także zarejestrować urządzenie przy użyciu Discoverable Credentials / Resident Keys. Oznacza to, że klucz prywatny oraz powiązane metadane są przechowywane w pamięci trwałej na autentikatorze, a nie na serwerze CAS.' At the bottom of the form is a large blue button with the text 'Zarejestruj urządzenie z uwierzytelnianiem przy użyciu poświadczeń możliwych do odnalezienia'. At the very bottom of the page, there is a dark footer bar containing the text 'Deklaracja dostępności' and 'Andrzej Kierepka, Państwowa Akademia Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu'.

8.2 Konfiguracja w systemie Windows

- Wybierz opcję „Klucz zabezpieczeń”.

Potwierdź rejestrację konta

Potwierdź rejestrację konta, podając token z aplikacji uwierzytelniającej na swoim urządzeniu. Po zweryfikowaniu tokena rejestracja konta zostanie zakończona.

Token:*

Przyjazna nazwa
sleepy_jobs

Zarejestruj Anuluj

- Wprowadź PIN do klucza.

Zabezpieczenia Windows

Zapisz klucz dostępu

Klucz dostępu dla cas.pwste.edu.pl

Wprowadź numer PIN klucza zabezpieczeń

Kod PIN klucza zabezpieczeń

To zostanie zapisane na klucz zabezpieczeń. Zmień

OK Anuluj

- Kliknij „OK” i dotknij klucza fizycznego.

Zabezpieczenia Windows

Zapisz klucz dostępu

Klucz dostępu dla cas.pwste.edu.pl

Dotknij klucza zabezpieczeń.

To zostanie zapisane na klucz zabezpieczeń. Zmień

Anuluj

8.3 Zakończenie

Po poprawnej rejestracji użytkownik zostanie wylogowany.

Kolejne logowania

Każde logowanie będzie wymagało:

- loginu
- hasła
- PIN-u
- użycia klucza sprzętowego

9. Zmiana metody uwierzytelniania

Użytkownik w każdej chwili może dokonać zmiany wybranej metody uwierzytelniania dwuskładnikowego. W tym celu należy wejść na stronę aplikacji Systemu Centralnego Uwierzytelniania dostępnej pod adresem <https://cas.pwste.edu.pl/cas/account>

Po poprawnym zautoryzowaniu się użytkownik zobaczy panel zarządzania w którym dostępne są m.in. takie opcje jak **Zmiana hasła** oraz **Zmiana MFA**.

W lewym menu użytkownik ma również dostępne informacje o zarejestrowanych **Urządzeniach logowania dwuskładnikowego**.

The screenshot shows the top navigation bar with 'Logowanie', 'English', 'Zmiana hasła', 'Zmiana MFA', and 'Wyloguj'. The left sidebar contains menu items: 'Urządzenia logowania dwuskładnikowego', 'Twoje zaufane urządzenia', 'Lista aktualnie zalogowanych urządzeń', and 'Historia logowania'. The main content area displays the PANS logo and a message: 'Udane logowanie. Dla zachowania bezpieczeństwa, gdy zakończysz korzystanie z usług wymagających uwierzytelnienia, wyloguj się i zamknij przeglądarkę!'.

9.1 Zmiana MFA

Wybranie opcji **Zmiana MFA** z górnego paska aplikacji SCU spowoduje, że dotychczasowy drugi składnik autoryzacji zostanie usunięty, a użytkownik zostanie wylogowany z systemu.

The screenshot shows the top navigation bar with 'Centralny System Uwierzytelniania', 'Strona główna', and 'English'. The main content area displays the PANS logo and a message: 'Drugi składnik autoryzacji. Poprawnie usunięto drugi składnik autoryzacji wyloguj się aby ponownie go ustawić'. A 'Wyloguj' button is visible at the bottom of the message box.

Ponowne zalogowanie do systemu przeniesie użytkownika bezpośrednio do ekranu wyboru drugiego składnika opisanego w punkcie 5 niniejszej instrukcji.

System zachowuje wszystkie wcześniej skonfigurowane metody uwierzytelniania. Oznacza to, że jeśli przy kolejnym logowaniu użytkownik ponownie wybierze aplikację OTP lub klucz sprzętowy, a dana metoda była już wcześniej skonfigurowana, system automatycznie wykorzysta ją ponownie.

9.2 Usunięcie zapisanych urządzeń logowania dwuskładnikowego

Użytkownik może w dowolnym momencie usunąć zapisane metody autoryzacji. W tym celu należy w panelu zarządzania wybrać z menu po lewej stronie pozycję „Urządzenia logowania dwuskładnikowego”.

Po jej otwarciu wyświetlona zostanie lista wszystkich skonfigurowanych metod. Kliknięcie ikony kosza przy wybranej metodzie spowoduje jej natychmiastowe usunięcie.

Ponowne skorzystanie z tej metody będzie wymagało jej ponownej konfiguracji zgodnie z krokiem 5 i kolejnymi niniejszej instrukcji.

Logowanie
English
Zmiana hasła
Zmiana MFA
Wyloguj

- [Urządzenia logowania dwuskładnikowego](#)
- 🔑 [Twoje zaufane urządzenia](#)
- 👤 [Lista aktualnie zalogowanych urządzeń](#)
- 🕒 [Historia logowania](#)

Multifactor Authentication Devices

The following devices are registered under your account and may be used for multifactor authentication.

entries per page

Search:

Source	ID	Name	Type	Model	Number	
G Google Authenti...	117	HM7	N/A	N/A	N/A	
🌐 Web Authn	HSN1LoMnnH8EzC0X...	YBK	N/A	N/A	N/A	

Showing 1 to 2 of 2 entries

« < 1 > »

You can also register another device to use for multifactor authentication.

↓ Zarejestruj

Deklaracja dostępności
Andrzej Kierepka. Państwowa Akademia Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu

10. Przykładowe aplikacje OTP

Użytkownicy mogą korzystać z dowolnej aplikacji OTP, która umożliwi dodanie aplikacji SCU i generowanie dla niej kodów jednorazowych.

Poniżej przedstawiamy przykładowe aplikacje, które można pobrać ze sklepów właściwych dla danego systemu operacyjnego.

10.1 dla systemu Android

Google Authenticator

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&pcampaignid=web_share



Microsoft Authenticator

https://play.google.com/store/apps/details?id=com.azure.authenticator&pcampaignid=web_share



10.2 dla systemu iOS

Google Authenticator

<https://apps.apple.com/pl/app/google-authenticator/id388497605?l=pl>



Microsoft Authenticator

<https://apps.apple.com/pl/app/microsoft-authenticator/id983156458?l=pl>



10.3 dla systemu Windows

Oracle Mobile Authenticator

<https://apps.microsoft.com/detail/9NBLGGH4NSH8?hl=neutral&gl=PL&ocid=pdfshare>



FortiToken for Windows

<https://apps.microsoft.com/detail/9P0TDH1J7WFZ?hl=neutral&gl=PL&ocid=pdfshare>



10.4 dla systemu Linux

Open Authenticator

<https://snapcraft.io/open-authenticator>

