

Instrukcja konfiguracji wieloskładnikowego uwierzytelniania Multi-Factor Authentication (MFA)

Spis treści

1. Informacje ogólne	1
2. Konfiguracja wieloskładnikowego uwierzytelniania (MFA)	1
a. Konfiguracja aplikacji uwierzytelniania – MFA.....	3
b. Konfiguracja numeru telefonu – MFA.....	6
3. Konfiguracja wielu metod dwuskładnikowego uwierzytelniania.....	8
4. Zmiana domyślnego składnika uwierzytelniania.....	8

1. Informacje ogólne

Multi-factor Authentication (MFA) jest dodatkową procedurą zabezpieczenia dostępu do zasobów uczelnianych. Oprócz podania danych logowania użytkownik w kolejnym etapie podaje jednorazowy kod zabezpieczający przesłany w wiadomości SMS lub wygenerowany za pomocą specjalnej aplikacji (dostępnej dla wszystkich systemów mobilnych).

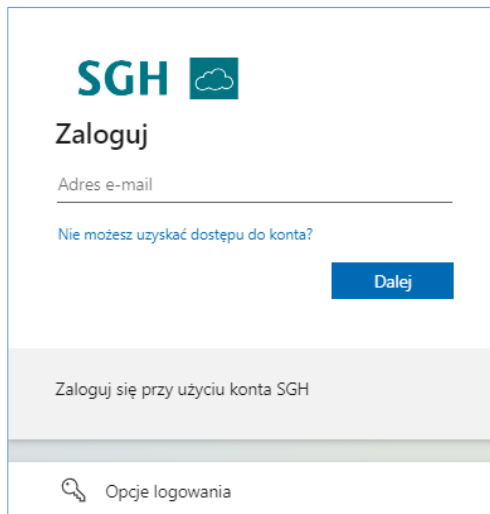
Można ustawić kilka metod uwierzytelniania oraz wybrać jedną domyślną metodę.

Wieloskładnikowe uwierzytelnianie jest ustawiane podczas pierwszego logowania do konta SGH. Po ustawieniu wieloskładnikowego uwierzytelniania, można wprowadzać zmiany w konfiguracji na stronie <https://mfa.sgh.waw.pl>

2. Konfiguracja wieloskładnikowego uwierzytelniania (MFA)

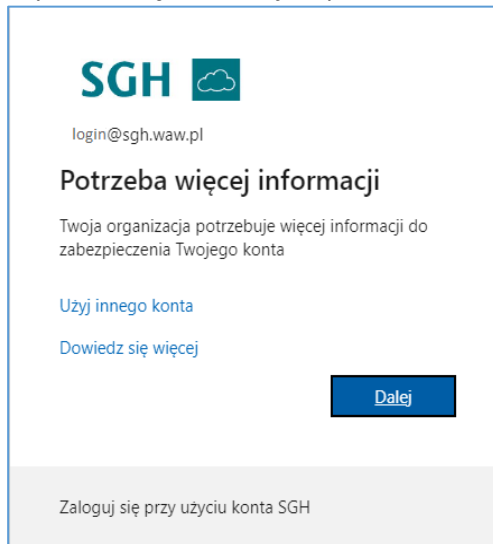
W celu konfiguracji wieloskładnikowego uwierzytelniania (MFA – Multi-factor authentication):

1. należy wejść na stronę <https://mfa.sgh.waw.pl> i zalogować się na swoje konto SGH



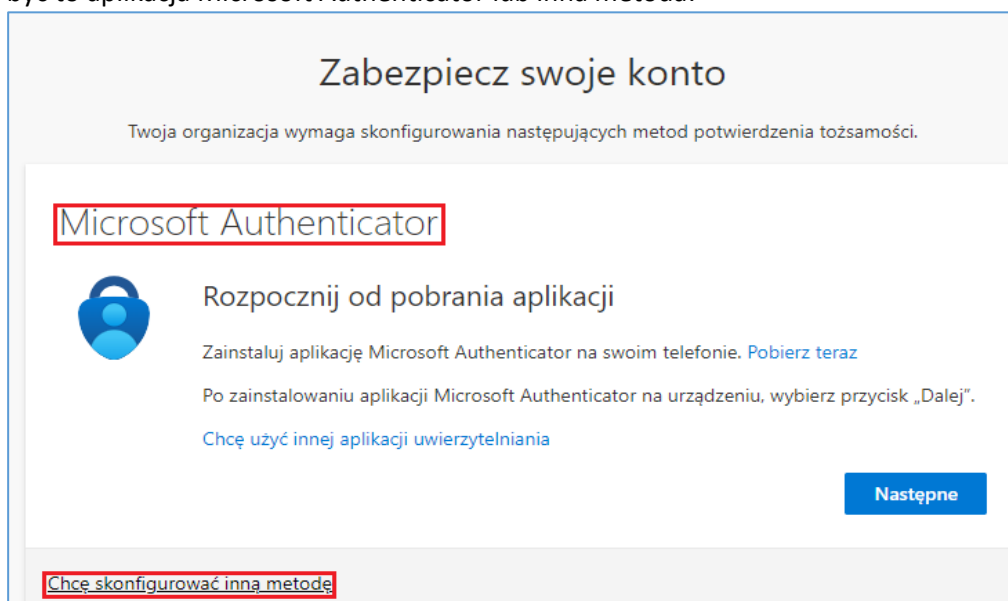
The screenshot shows the SGH login interface. At the top left is the SGH logo. Below it, the word "Zaloguj" is displayed. There is a text input field labeled "Adres e-mail". Below the input field, there is a link that says "Nie możesz uzyskać dostępu do konta?". To the right of the input field is a blue button labeled "Dalej". At the bottom of the main content area, there is a grey bar with the text "Zaloguj się przy użyciu konta SGH". Below this bar is a link with a key icon and the text "Opcje logowania".

2. Wyświetli się informacja o potrzebie dodatkowych informacji od użytkownika

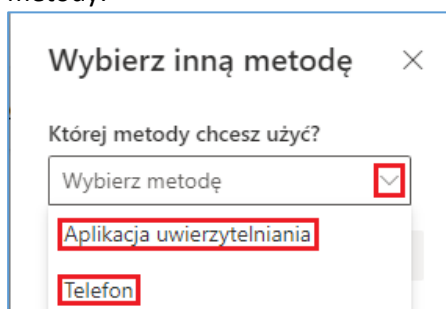


The screenshot shows a page from the SGH system. At the top left is the SGH logo. Below it, the email address "login@sgh.waw.pl" is displayed. The main heading is "Potrzeba więcej informacji". Below this heading, there is a message: "Twoja organizacja potrzebuje więcej informacji do zabezpieczenia Twojego konta". There are two links: "Użyj innego konta" and "Dowiedz się więcej". To the right of the "Dowiedz się więcej" link is a blue button labeled "Dalej". At the bottom of the main content area, there is a grey bar with the text "Zaloguj się przy użyciu konta SGH".

3. Po wybraniu „Dalej” otworzy się strona z możliwością wyboru metody weryfikacji. Może być to aplikacja Microsoft Authenticator lub inna metoda:



4. Gdy wybierzemy „Chcę skonfigurować inną metodę” wyświetli się okno do wyboru metody:

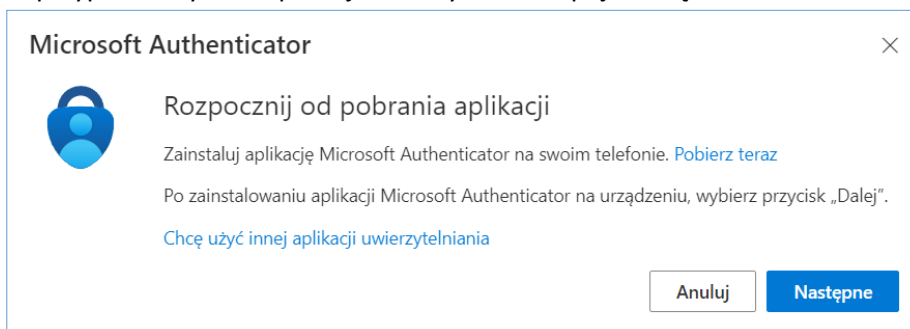


Po wybraniu metody należy potwierdzić wybór „Następne”/”Dalej” i postępować zgodnie z instrukcjami na ekranie.

a. Konfiguracja aplikacji uwierzytelniania – MFA

Aplikację Microsoft Authenticator można zainstalować na wielu urządzeniach mobilnych – konfiguracja dodatkowego urządzenia i zainstalowanie aplikacji odbywa się podobnie za każdym razem.

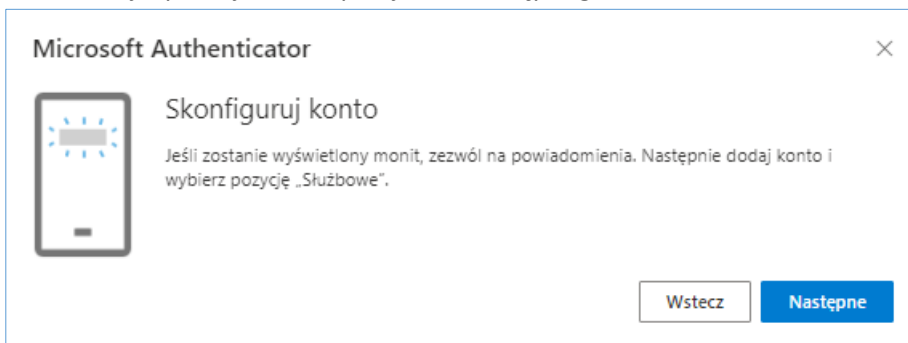
1. W przypadku wyboru aplikacji uwierzytelniania pojawi się komunikat:



Należy pobrać i zainstalować aplikację Microsoft Authenticator na urządzeniu mobilnym. Po

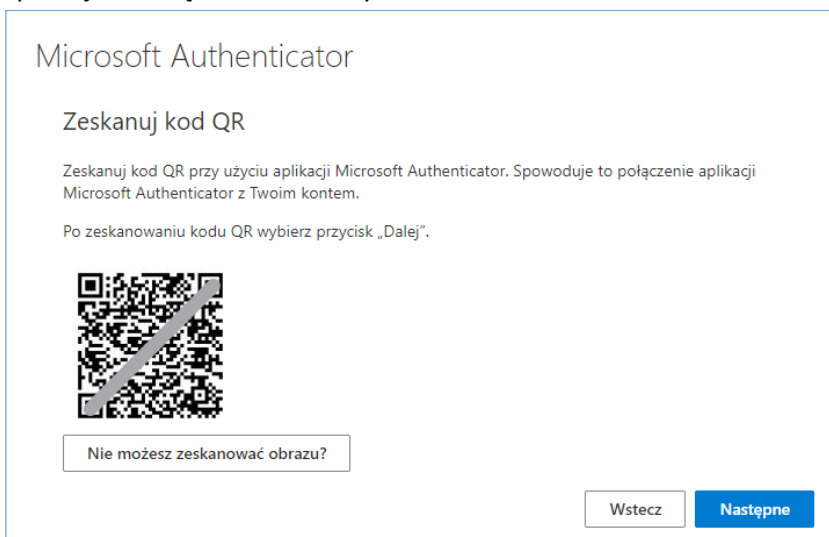
wybraniu „Pobierz teraz” pojawi się strona, na której dostępne będą do pobrania aplikacje na Androida lub iOS.

2. Po instalacji aplikacji można przejść do następnego okna:



Ważne: Pamiętaj, żeby zezwolić aplikacji na wysyłanie powiadomień.

3. Po wybraniu „Następne” wyświetli się kod QR*, który niezbędny będzie do konfiguracji aplikacji na urządzeniu mobilnym:

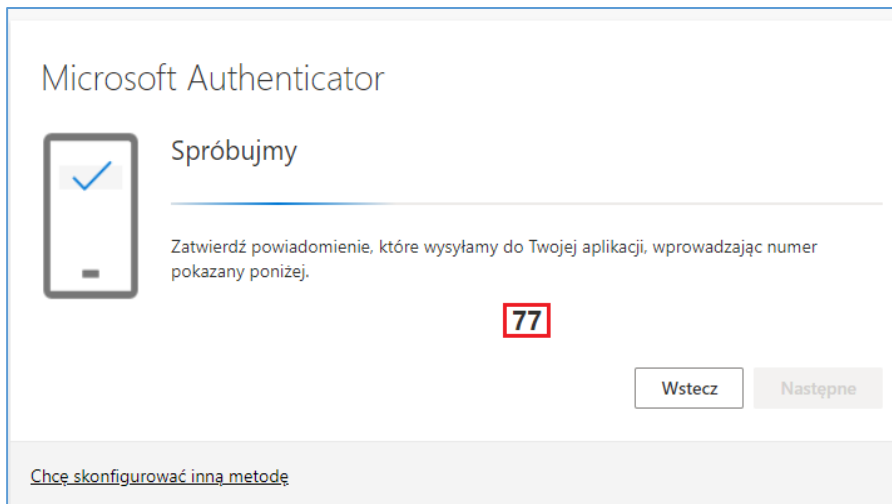


4. Po zeskanowaniu kodu w aplikacji pojawi się informacja „Pomyślnie dodano konto”.

* Gdy nie ma możliwości zeskanowania kodu QR należy wpisać kod liczbowy ukryty pod opcją „Nie możesz zeskanować obrazu?”.

5. Ostatnim krokiem jest wpisanie do aplikacji na urządzeniu mobilnym 2-cyfrowego kodu, który wyświetli się na ekranie:

Ekran



Microsoft Authenticator

Spróbujmy

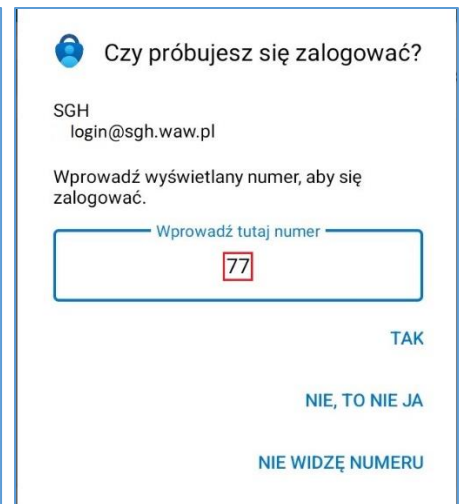
Zatwierdź powiadomienie, które wysyłamy do Twojej aplikacji, wprowadzając numer pokazany poniżej.

77

Wstecz Następne

[Chcę skonfigurować inną metodę](#)

Aplikacja



Czy próbujesz się zalogować?

SGH
login@sgh.waw.pl

Wprowadź wyświetlany numer, aby się zalogować.

Wprowadź tutaj numer

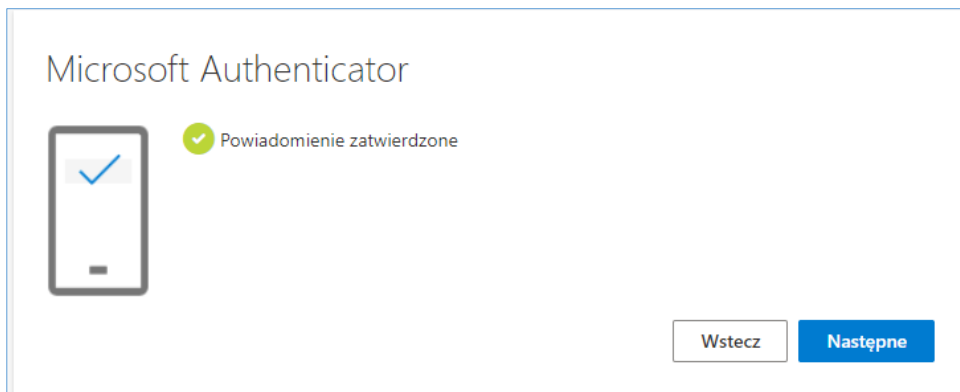
77

TAK

NIE, TO NIE JA

NIE WIDZĘ NUMERU

6. Poprawnie wpisany kod spowoduje ukończenie konfiguracji aplikacji uwierzytelniania.

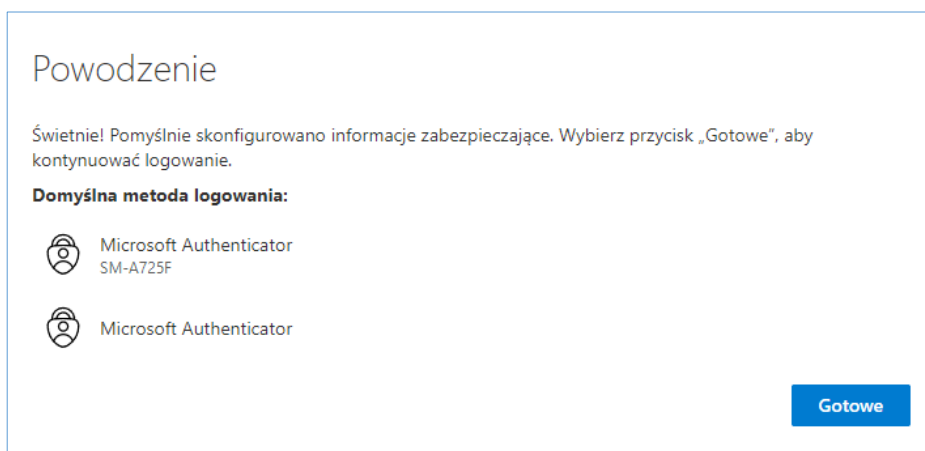


Microsoft Authenticator

Powiadomienie zatwierdzone

Wstecz Następne

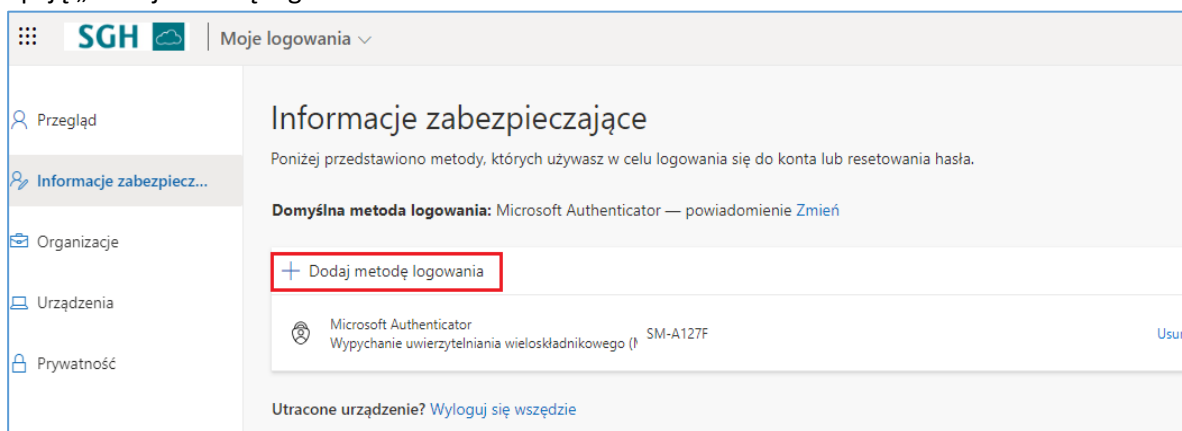
7. Po wybraniu „Następne” wyświetli się informacja o skonfigurowaniu metody, a po wybraniu „Gotowe” odbędzie się logowanie za pomocą ustawionego drugiego składnika:



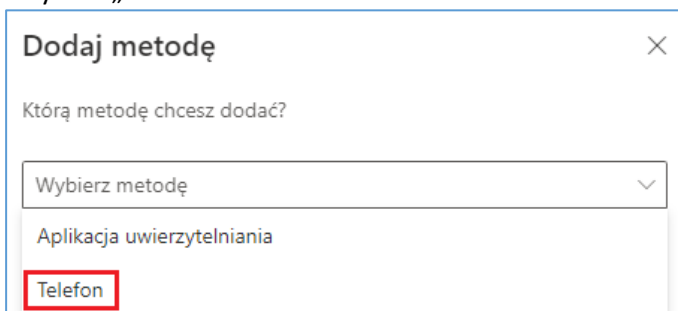
b. Konfiguracja numeru telefonu – MFA

W przeciwieństwie do aplikacji uwierzytelniania – numer telefonu do uwierzytelniania może być tylko jeden. Można wybrać opcję „oddzwonienia” przez automat w celu potwierdzenia logowania lub otrzymać SMSem kod weryfikujący do wpisania podczas logowania.

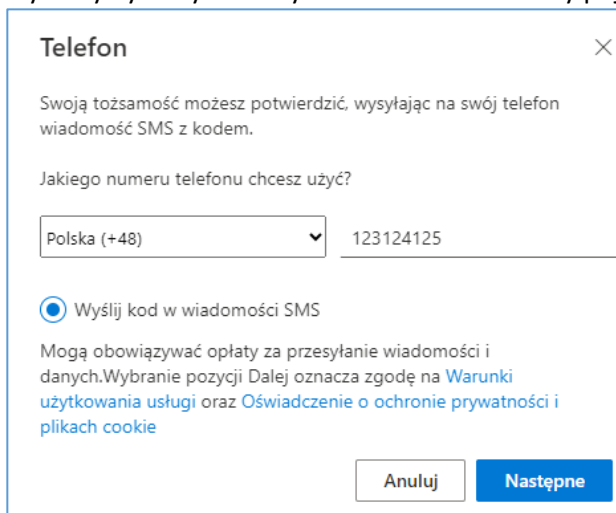
1. Aby dodać drugą metodę uwierzytelniania, na stronie <https://mfa.sgh.waw.pl> należy wybrać opcję „Dodaj metodę logowania”



i wybrać „Telefon”:

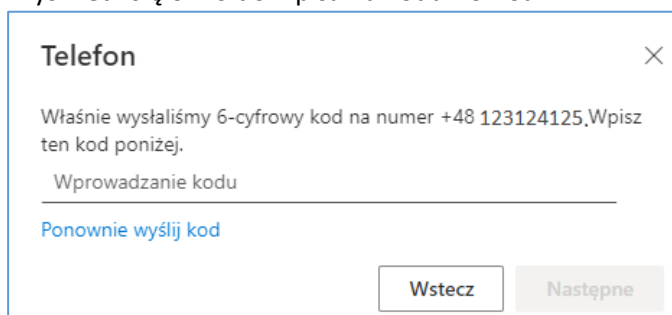


2. Po zatwierdzeniu wyświetli się miejsce na wpisanie nr telefonu (chyba że wcześniej był już wykorzystywany do odzyskiwania hasła – wtedy pojawi się domyślnie)



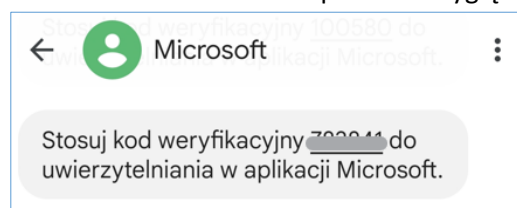
The screenshot shows a dialog box titled "Telefon" with a close button (X) in the top right corner. The text inside reads: "Swoją tożsamość możesz potwierdzić, wysyłając na swój telefon wiadomość SMS z kodem." Below this is the question "Jakiego numeru telefonu chcesz użyć?". There is a dropdown menu showing "Polska (+48)" and a text input field containing "123124125". A radio button is selected next to the text "Wyślij kod w wiadomości SMS". Below that, there is a warning: "Mogą obowiązywać opłaty za przesyłanie wiadomości i danych. Wybranie pozycji Dalej oznacza zgodę na [Warunki użytkowania usługi](#) oraz [Oświadczenie o ochronie prywatności i plikach cookie](#)". At the bottom, there are two buttons: "Anuluj" and "Następne".

3. Należy zatwierdzić, aby otrzymać wiadomość SMS.
4. Wyświetli się okno do wpisania kodu z SMSa:

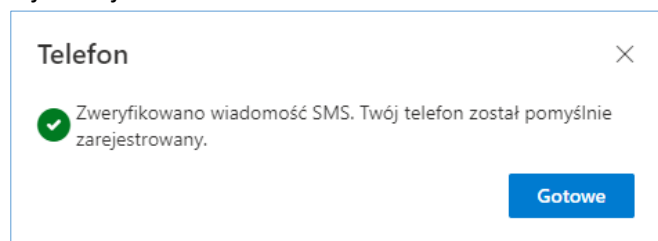


The screenshot shows a dialog box titled "Telefon" with a close button (X) in the top right corner. The text inside reads: "Właśnie wysłaliśmy 6-cyfrowy kod na numer +48 123124125. Wpisz ten kod poniżej." Below this is a text input field with the placeholder "Wprowadzanie kodu". A link "Ponownie wyślij kod" is visible below the input field. At the bottom, there are two buttons: "Wstecz" and "Następne".

5. Wiadomość SMS z kodem powinna wyglądać jak na załączonym zrzucie ekranu:



6. Po przepisaniu kodu z SMSa i zatwierdzeniu wyświetli się potwierdzenie weryfikacji i rejestracji numeru telefonu:



The screenshot shows a dialog box titled "Telefon" with a close button (X) in the top right corner. The text inside reads: "Zweryfikowano wiadomość SMS. Twój telefon został pomyślnie zarejestrowany." There is a green checkmark icon to the left of the text. At the bottom, there is a blue button labeled "Gotowe".

3. Konfiguracja wielu metod dwuskładnikowego uwierzytelniania

Każdy użytkownik ma ustawiony drugi składnik uwierzytelniania. Jednakże istnieje możliwość ustawienia kilku metod uwierzytelniania (potwierdzenie w aplikacji, czy wysłanie SMSa na telefon). Domyślną metodą uwierzytelniania zazwyczaj jest pierwsza ustawiona metoda.

W celu ustawienia kilku metod uwierzytelniania należy wejść na stronę <https://mfa.sgh.waw.pl> i ustawić kolejne opcje uwierzytelniania.

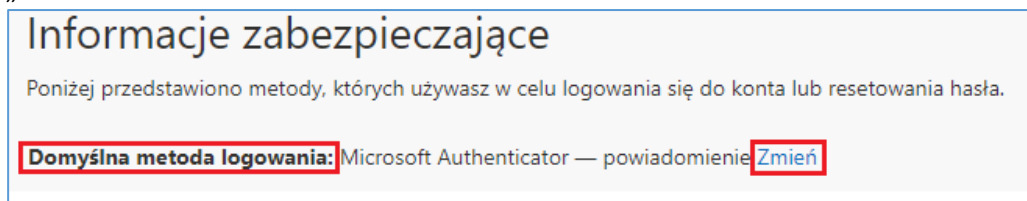
Ważne: Niezależnie od tego, ile składników uwierzytelniania dodamy, domyślny składnik uwierzytelniania może być tylko jeden. W związku z tym, podczas logowania do Chmury SGH będziemy proszeni o wykorzystanie domyślnego składnika uwierzytelniania, a nie jednego z ustawionych składników uwierzytelniania.

4. Zmiana domyślnego składnika uwierzytelniania

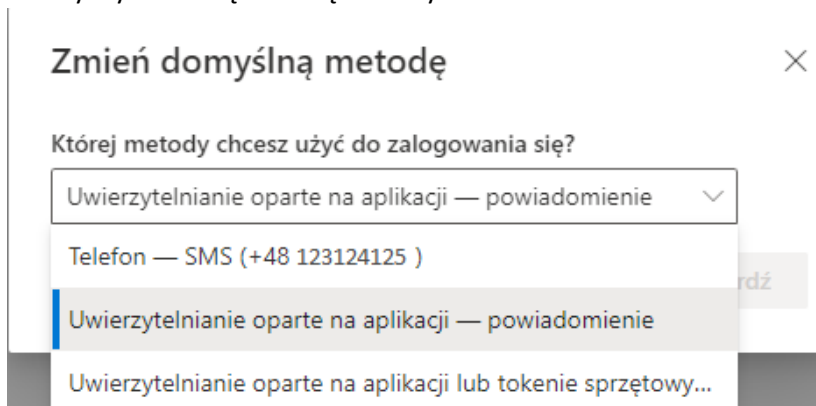
Domyślny sposób weryfikacji oznacza, że podczas logowania, po podaniu hasła do konta, będziemy proszeni o potwierdzenie swojej tożsamości poprzez właśnie ten sposób weryfikacji. Jeśli nie będziemy mogli z niego skorzystać, możliwe będzie potwierdzenie swojej tożsamości poprzez inną metodę weryfikacji skonfigurowaną wcześniej (patrz pkt. 3). W każdej chwili możemy również zmienić domyślną metodę uwierzytelniania.

Aby zmienić domyślną metodę uwierzytelniania:

1. Na stronie <https://mfa.sgh.waw.pl> przy „Domyślnej metodzie logowania” należy wybrać „Zmień”:



2. Należy wybrać inną metodą niż dotychczasowa:



i potwierdzić wybór.

3. Domyślna metoda zostanie zmieniona:

Domyślna metoda logowania została zaktualizowana 