MFA – Multi-Factor Authentication

Konfiguracja wieloskładnikowego logowania w Aplikacjach Microsoft PW

Centrum Informatyzacji

Sekcja Zarządzania Usługami Microsoft

Wersja 1.01 2024

W razie trudności lub uwag prosimy o kontakt:

tel. +48 (22) 234 5999, e-mail: 5999@pw.edu.pl

Spis treści

Wprowadzenie

Uwierzytelnianie wieloskładnikowe (MFA - Multi-Factor Authentication) zostało zaimplementowane w celu zabezpieczenia konta przed dostępem przez niepowołane osoby oraz informowania czy takie próby nastąpiły, np.: z powodu wycieku hasła, kiedy konieczna jest aktywacja uwierzytelniania wieloskładnikowego.

Aplikacje chmurowe Microsoft 365 umożliwiają logowanie dwuskładnikowe, tj.: oprócz loginu i hasła można zastosować :

- aplikacja Microsoft Authenticator - aplikacja zainstalowana na telefonie pozwala zatwierdzić logowanie lub wyświetlić aktualny kod do wpisania przy logowaniu,
- telefon komórkowy - możliwość wysyłania SMSów lub połączeń z informacją o kodzie potrzebnym do logowania,
- telefon biurowy - możliwość wysyłania połączeń głosowych z informacją o kodzie potrzebnym do logowania,
- token TOTP – urządzenie przenośne generujące co 30 sekund unikalny, jednorazowy kod, który umożliwia wpisanie 6 cyfr jako drugiego etapu logowania,
- klucz sprzętowy zabezpieczeń U2F/FIDO2 - posiadający specjalne oprogramowanie, które może przechowywać certyfikat z kluczem - aby aktywować tą opcję wcześniej należy aktywować uwierzytelnianie aplikacją lub telefonem. Klucz sprzętowy należy posiadać we własnym zakresie.

W razie potrzeby zmiany hasła lub resetu MFA prosimy o kontakt użytkownika z zespołem ServiceDesk telefonicznie lub osobiście. W celu weryfikacji tożsamości prosimy przygotować:

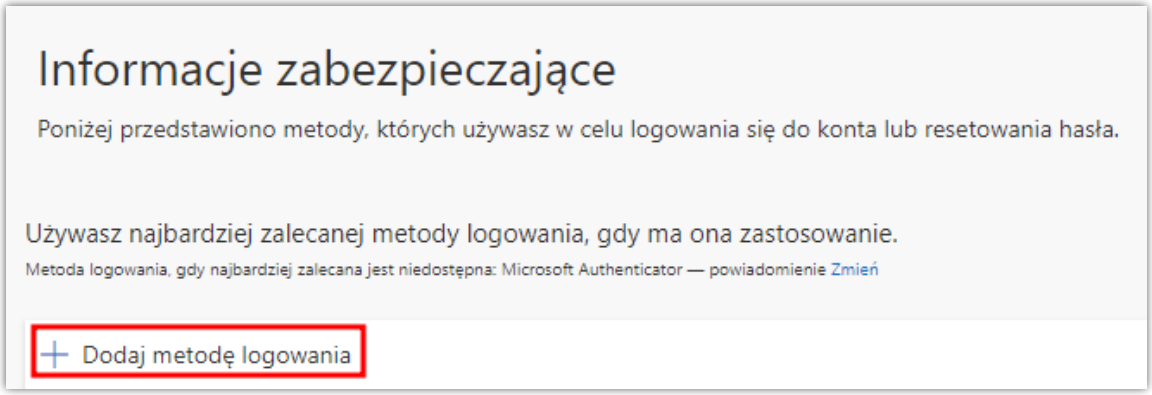
- numer SAP,
- cztery ostatnie cyfry numeru PESEL,
- numer telefonu komórkowego.

Konfiguracja aplikacji Microsoft Authenticator

Aby włączyć / dodać uwierzytelnianie dwuskładnikowe należy zalogować się na stronie przy użyciu konta PW:

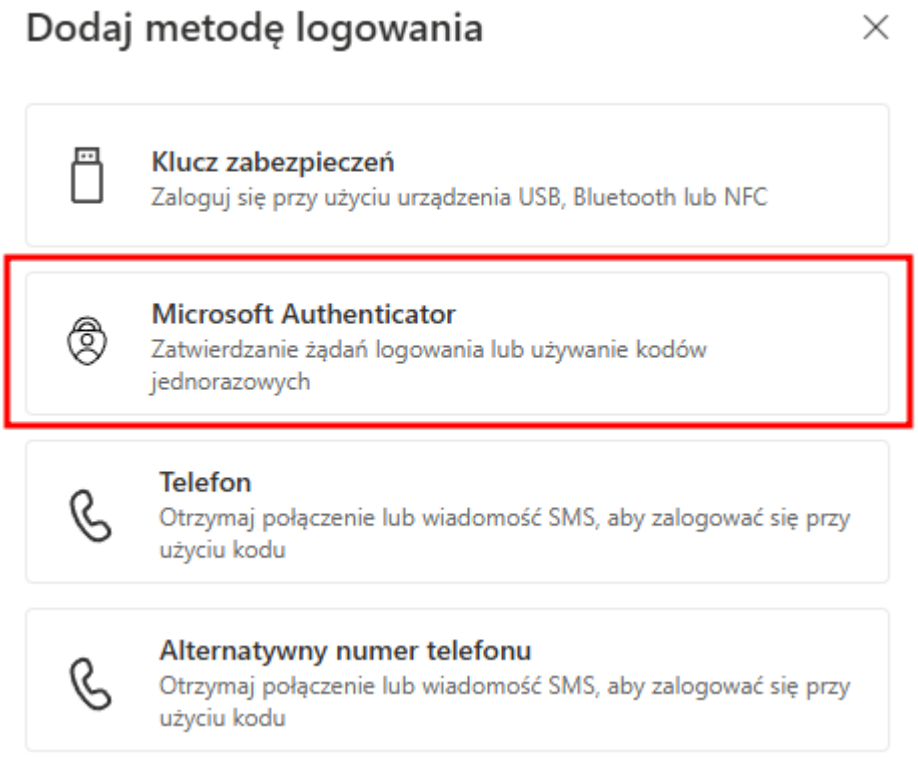
https://mysignins.microsoft.com/security-info

Po zalogowaniu wybrać "+ Dodaj metodę logowania", wybrać metodę uwierzytelniania i postępować dalej zgodnie z instrukcjami dla danej metody:



W tym przypadku przedstawimy domyślną dodatkową metodę weryfikacji jaką jest aplikacja Microsoft Authenticator. Inne metody, które są dostępne pod przyciskiem “Chcę skonfigurować inną metodę” zostaną omówione w części kolejnej.

Aby kontynuować należy wybrać „Microsoft Authenticator” i klikamy „Dodaj”:



Pobieramy aplikację odpowiednio z sklepu z aplikacjami (Google Play lub Apple AppStore):

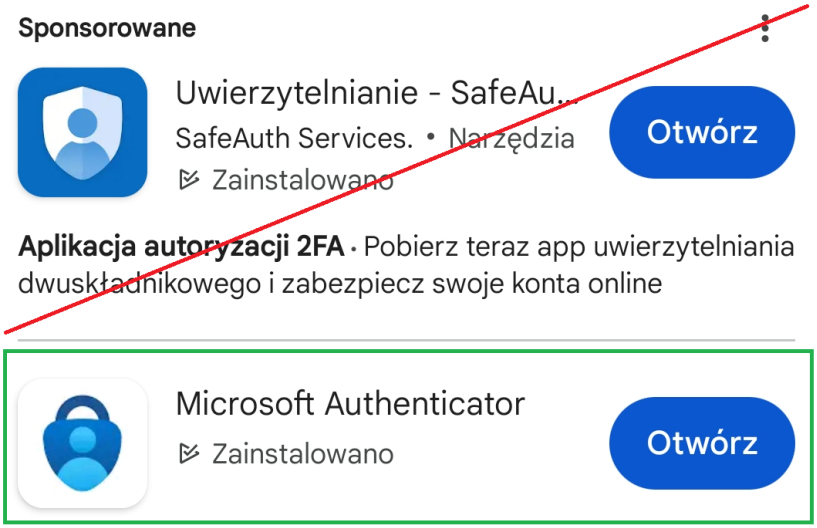
Google Android:

- https://play.google.com/store/apps/details?id=com.azure.authenticator

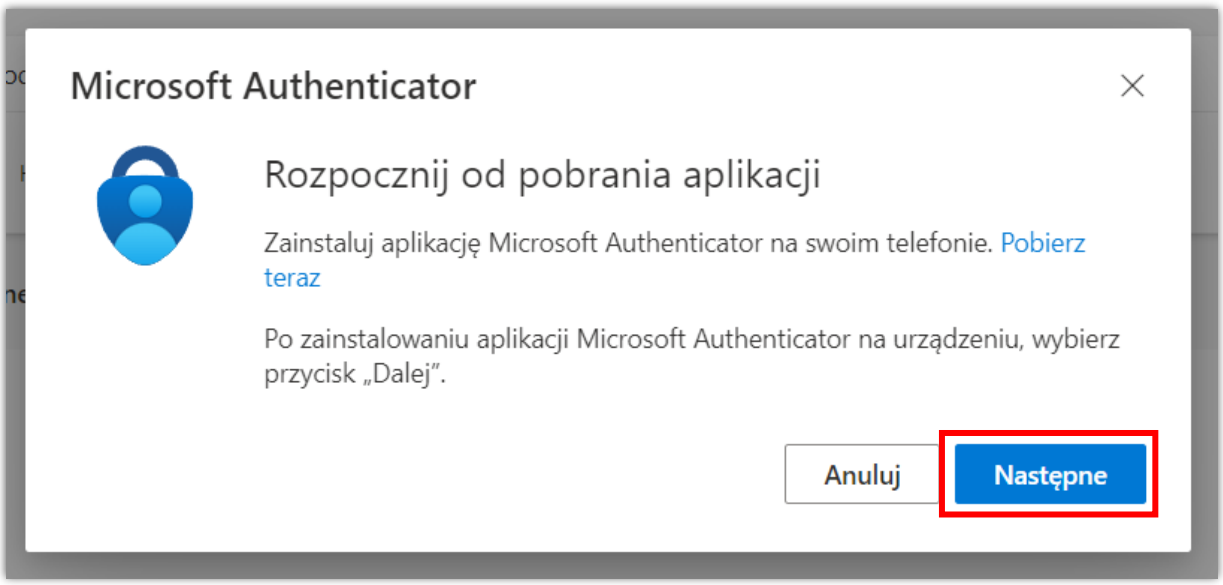
Apple AppStore:

- https://apps.apple.com/us/app/microsoft-authenticator/id983156458

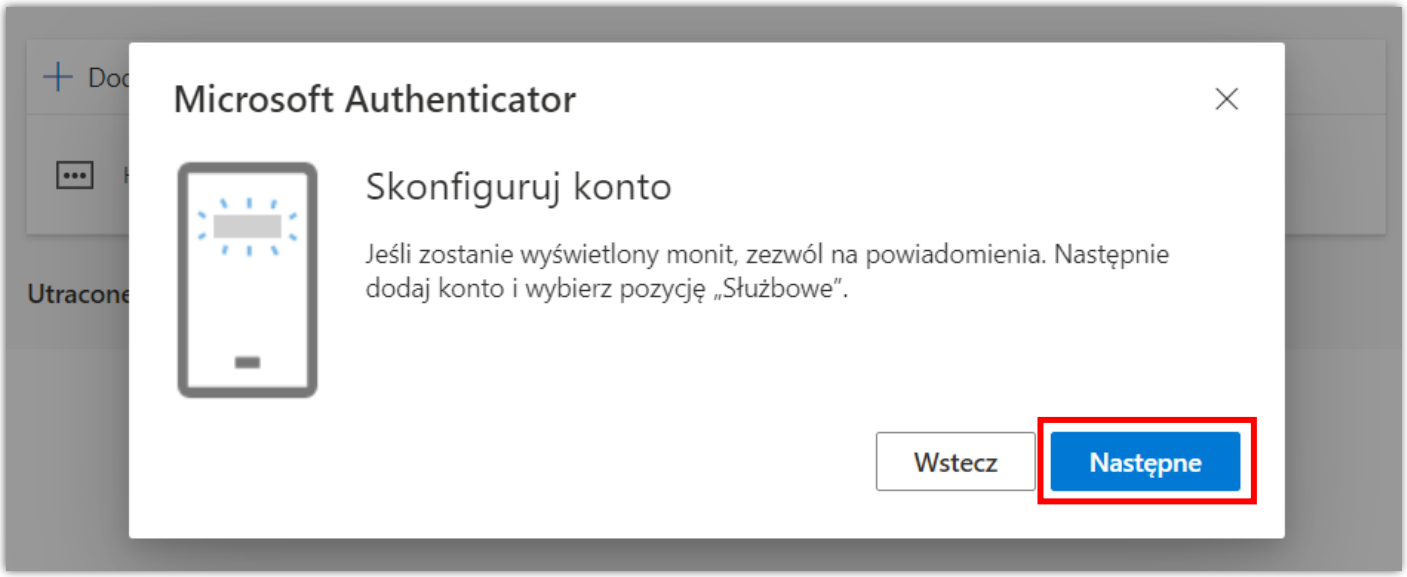
Przy wyszukiwaniu aplikacji w sklepie Google Play, należy uważać na inne podszywające się aplikację pod Microsoft Authenticator, gdyż mogą one wyłudzać dane!



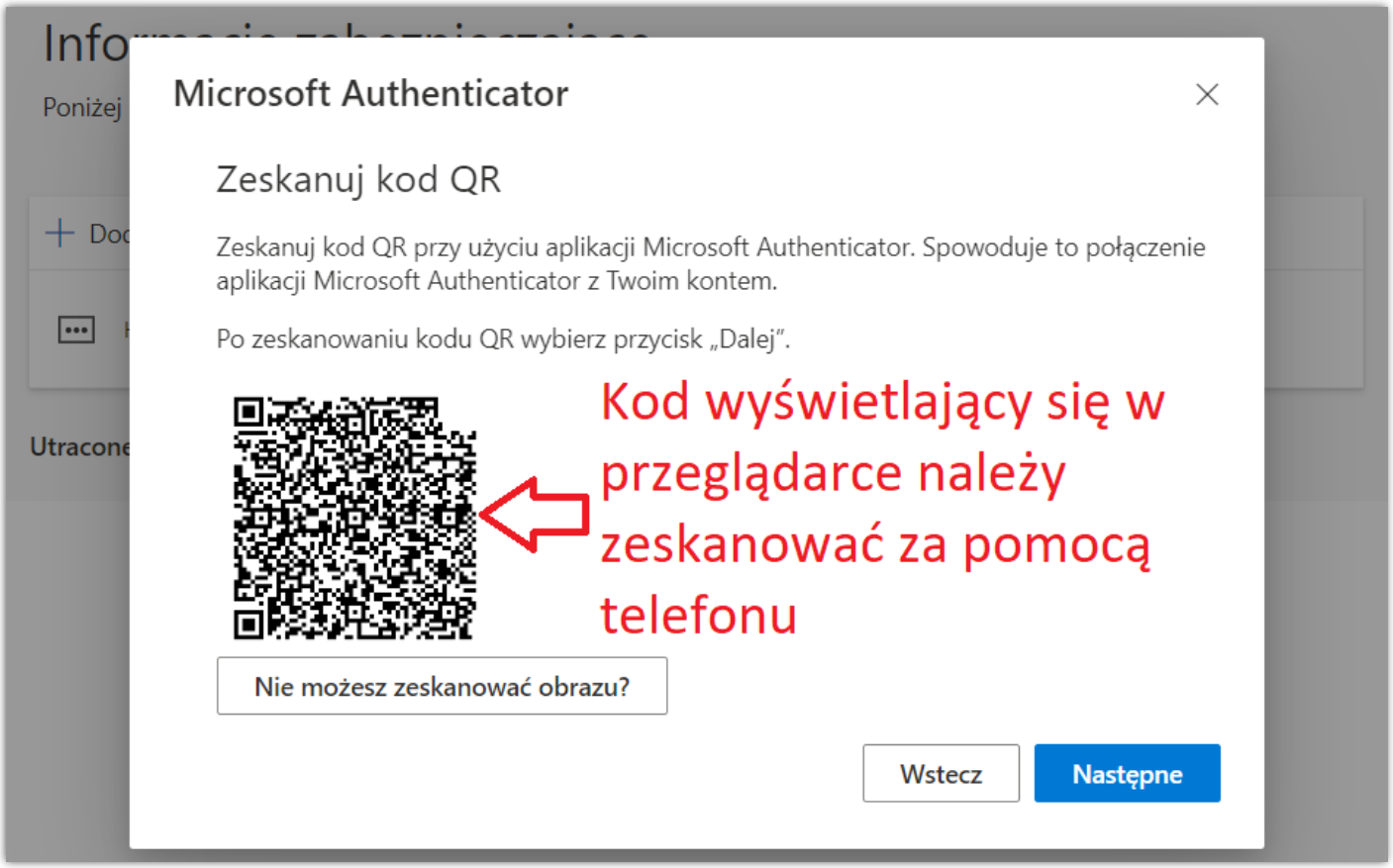
- Po pobraniu aplikacji i uruchomieniu jej na telefonie wybieramy przycisk “Następne”:



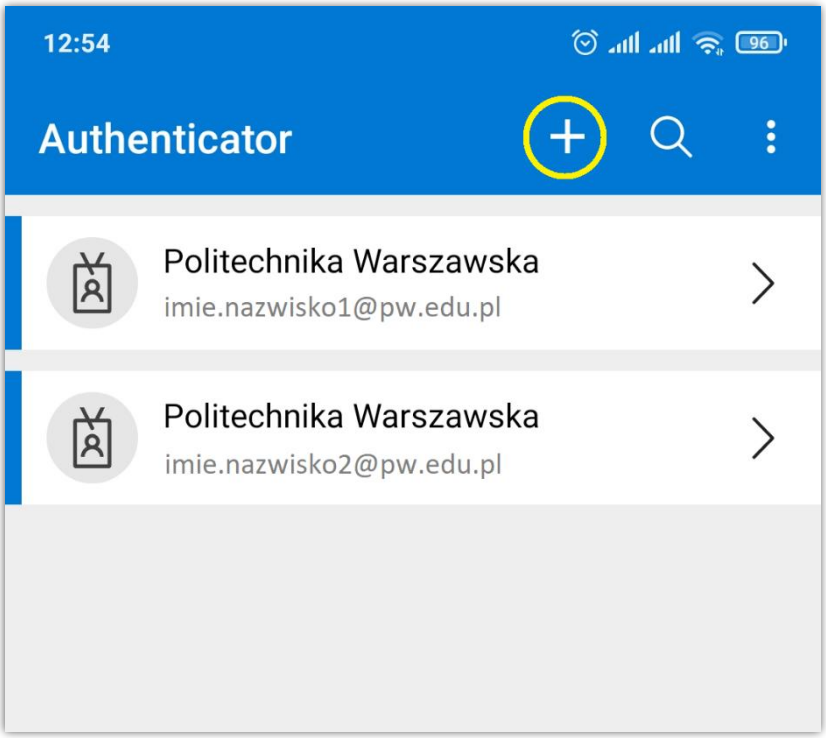
Otwieramy aplikację Microsoft Authenticator w telefonie i ponownie wybieramy przycisk “Następne” w przeglądarce.



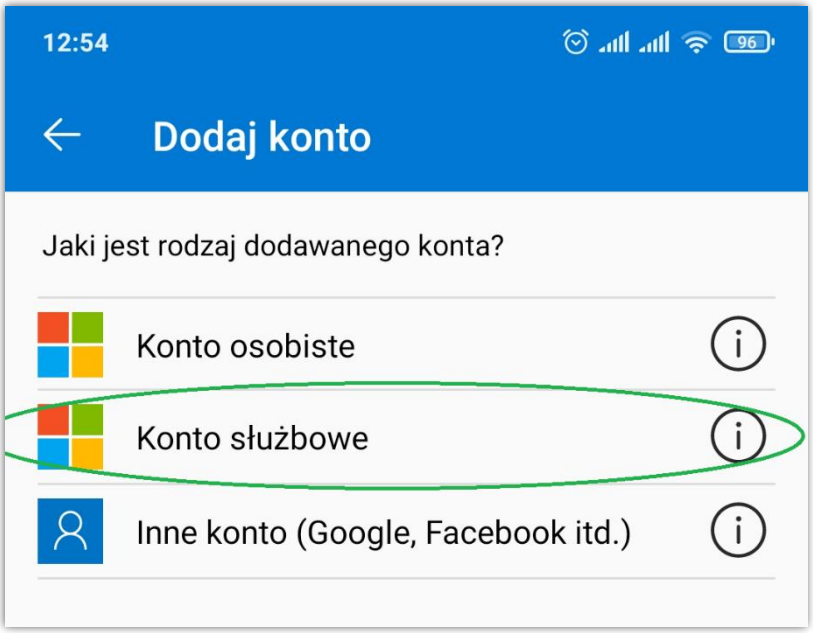
Zostanie wyświetlony QR kod, który należy zeskanować aplikacją Microsoft Authenticator.



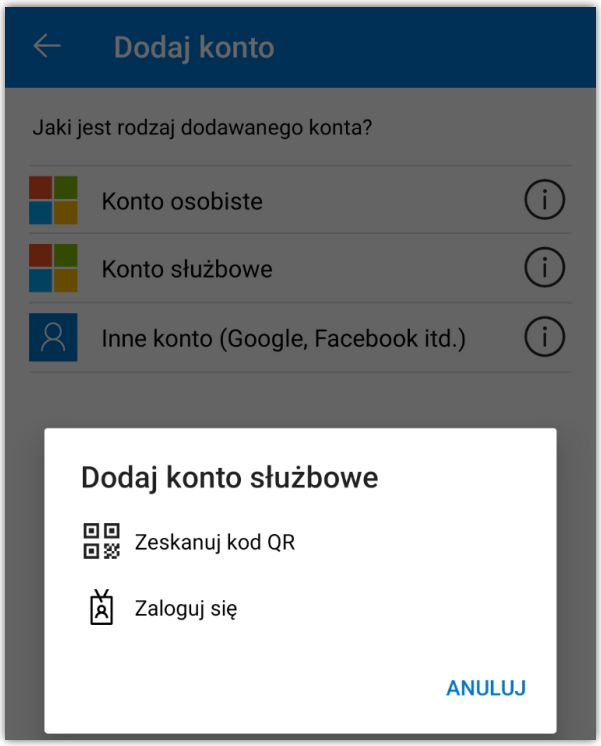
Aby to wykonać należy po zainstalowaniu aplikacji na telefonie mobilnym wybrać znak plusa w górnej części. Posiadanie innych wcześniej skonfigurowanych kont nie koliduje z aktywacją nowego konta, gdyż różne konta będą działały niezależnie od siebie.



Wybieramy opcję “Konto służbowe”.

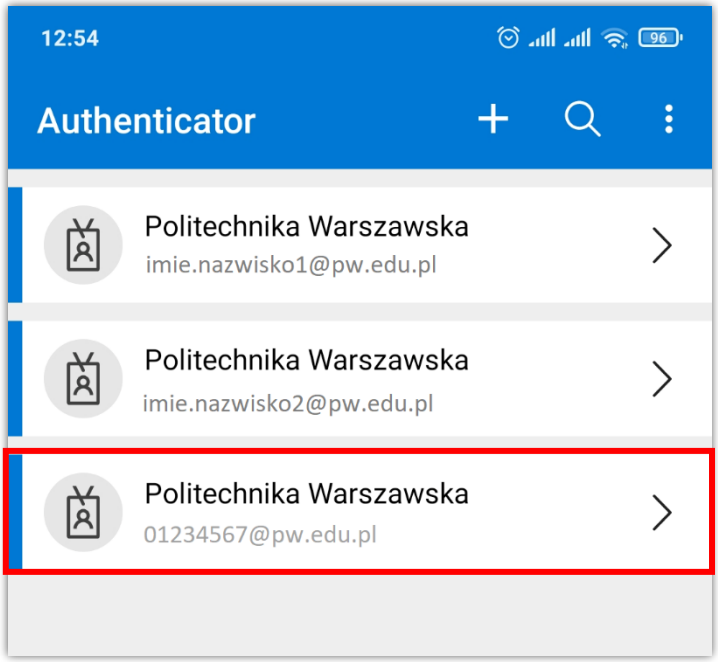


Wybieramy pierwszą opcję “Zeskanuj kod QR” i skanujemy kod dostępny na stronie. Alternatywnie możemy przeprowadzić całą procedurę wybierając opcję “Zaloguj się”.

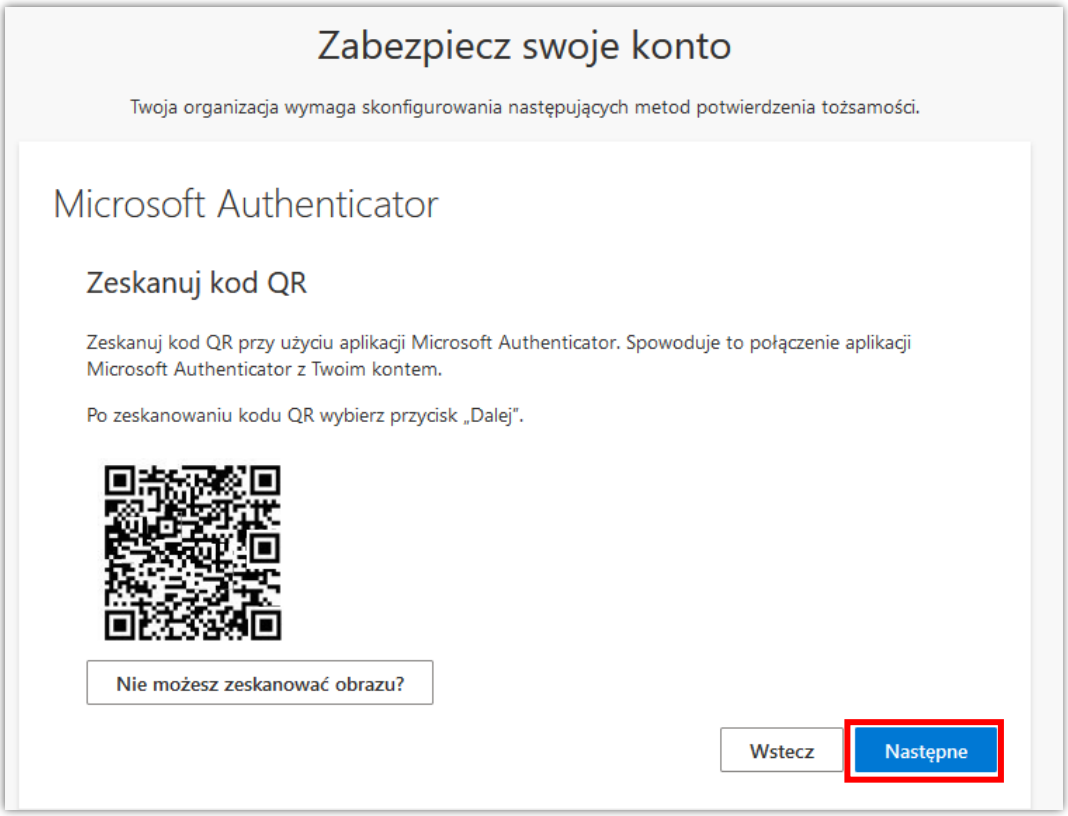


Po zeskanowaniu kodu QR, nowe konto powinno pojawić się na liście dostępnych. Jeśli nie udało się zeskanować kodu QR, należy w poprzednim kroku wybrać przycisk „Zaloguj się” i na wyświetlonej stronie zalogować się na stronie danymi do skrzynki pw.edu.pl.

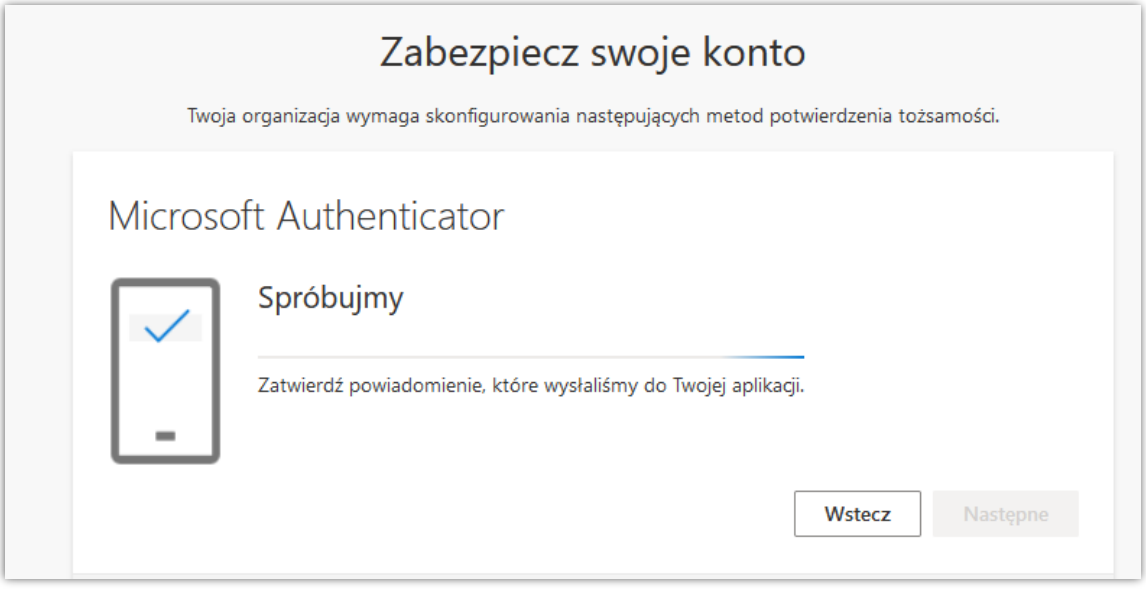
Gdy zauważymy, że na liście w aplikacji Microsoft Authenticator pojawiło się nowe konto oznacza to, że krok został wykonany pomyślnie i można wrócić do przeglądarki internetowej komputera.



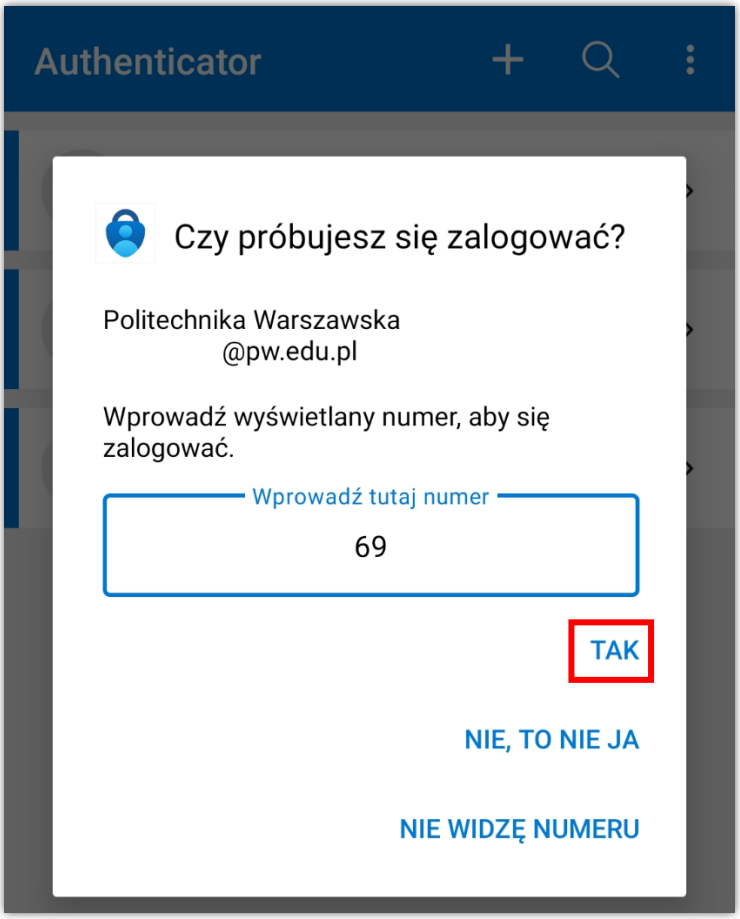
W przeglądarce internetowej wybieramy przycisk “Następne”:



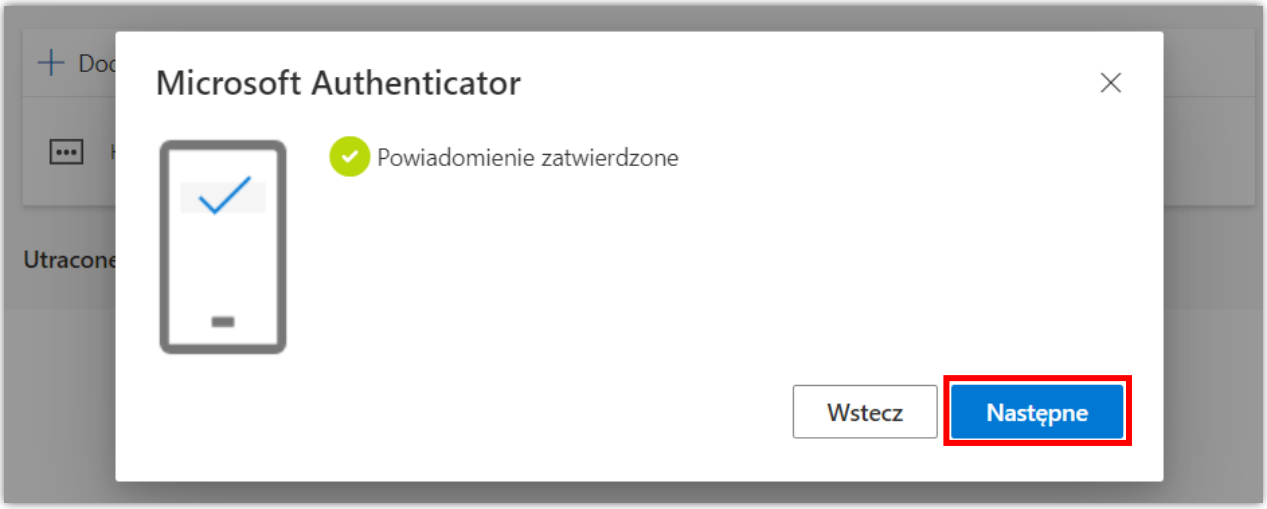
W tym momencie zostanie wysłany monit do aplikacji o potwierdzenie, który należy zaakceptować.



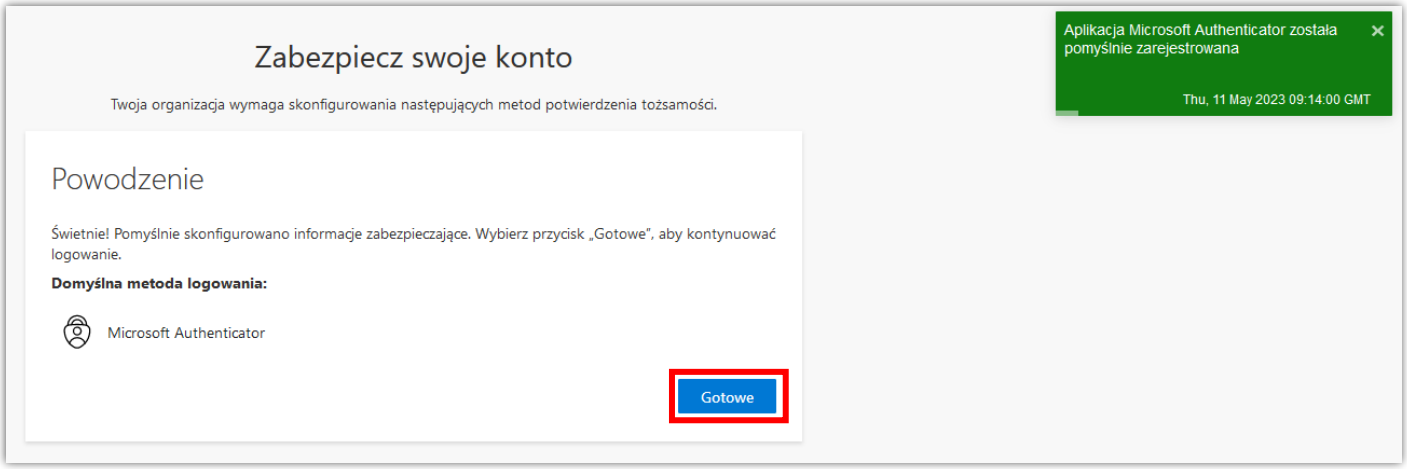
Wracamy do telefonu i w aplikacji wybieramy opcję “ZATWIERDŹ”. Jeśli monit wpisaniu kodu się nie pojawił należy sprawdzić czy komunikat o uwierzytelnianiu nie pojawia się w pasku powiadomień. Sprawdzamy jaka liczba pojawia się w przeglądarce internetowej i przepisujemy ją do aplikacji w telefonie następnie klikając przycisk „TAK”:



Po tej operacji, w przeglądarce pojawi się informacja, że powiadomienie zostało zatwierdzone i możemy wybrać przycisk “Następne”:



To kończy proces rejestracji aplikacji do autentyfikacji dwuskładnikowej, który możemy zakończyć wybierając przycisk “Gotowe”:



Konfiguracja numeru telefonu do autoryzacji SMS

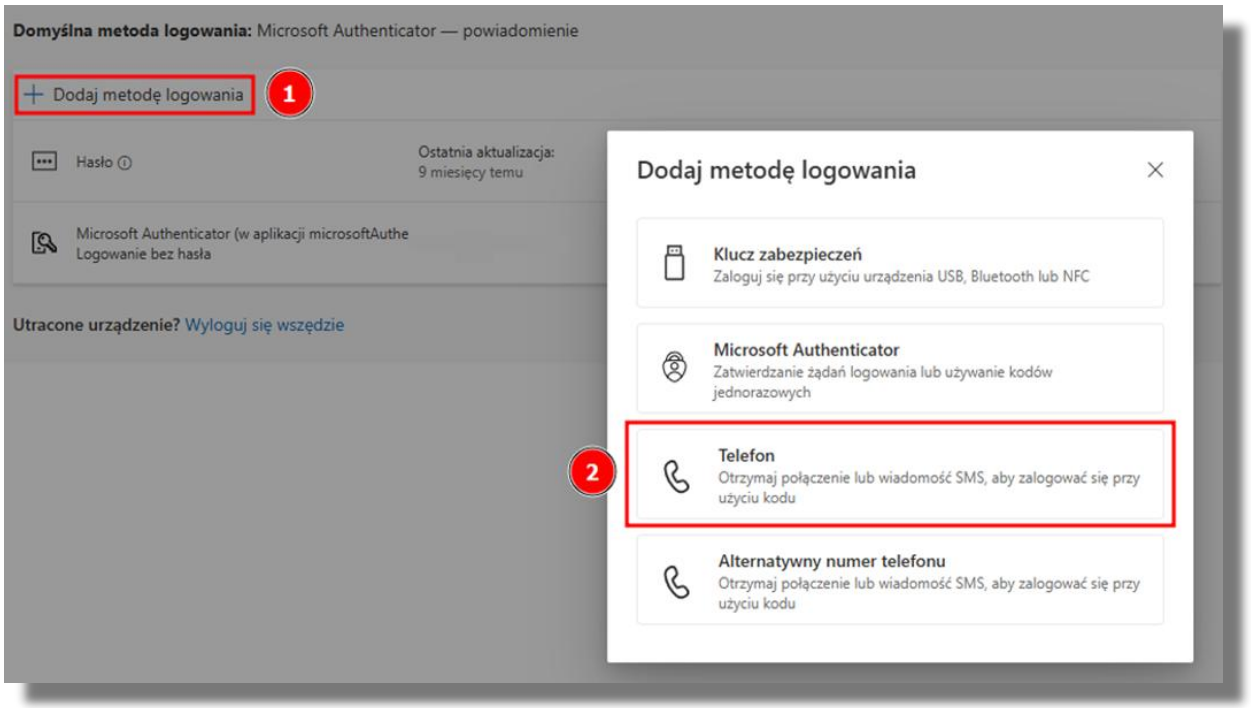
Poza metodą autoryzacji za pomocą aplikacji, kluczowe jest również skonfigurowanie metody numeru telefonu aby móc zalogować się do konta PW, w razie utraty lub zmiany urządzenia.

W celu dodania numeru telefonu jako metody logowania przechodzimy do strony:

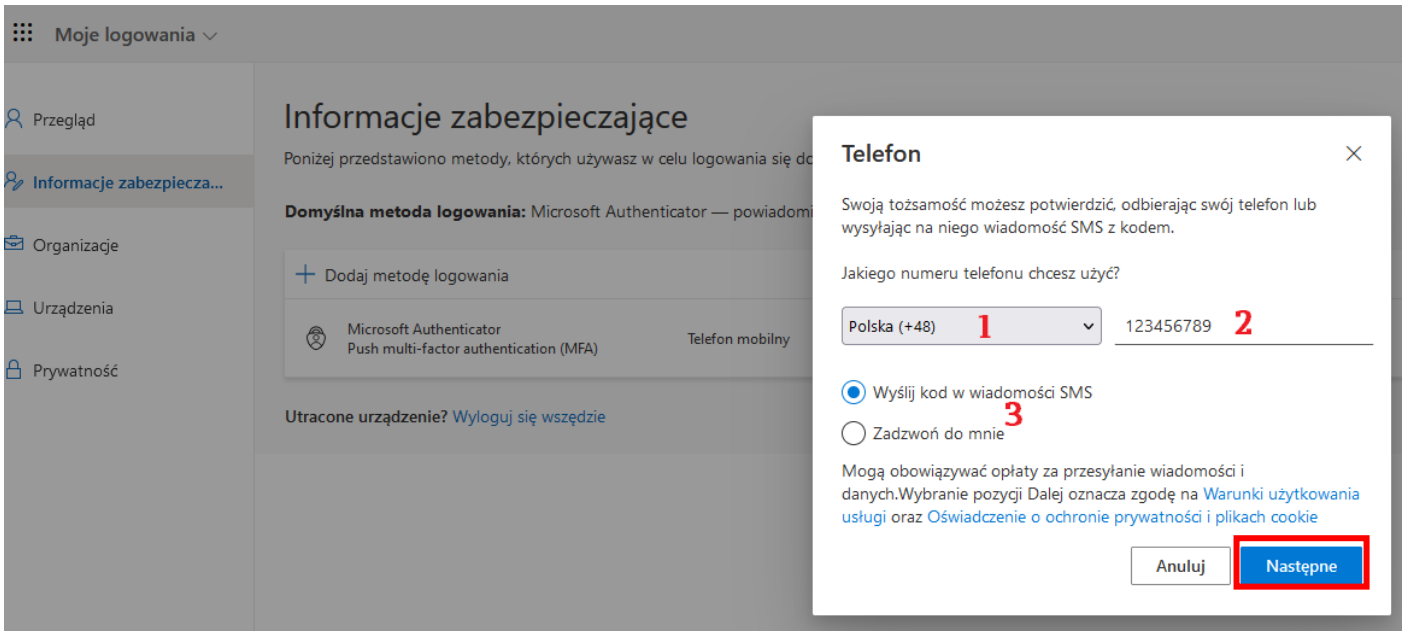
https://mysignins.microsoft.com/security-info

Następnie należy wykonać kroki dodania nowej metody w kolejności:

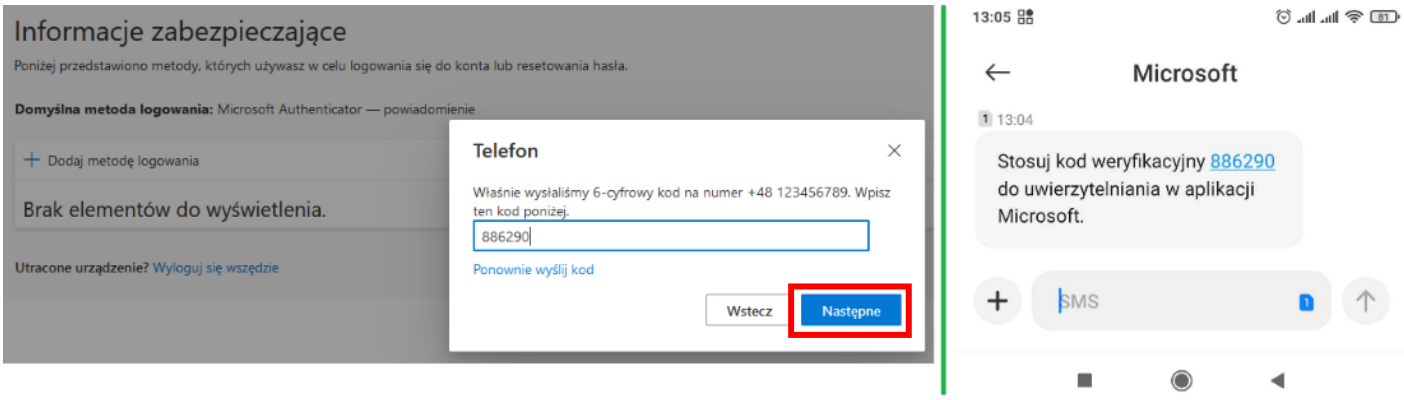
1. Wybieramy opcję “Dodaj metodę logowania”.
2. Z listy rozwijanej wybieramy “Telefon”.



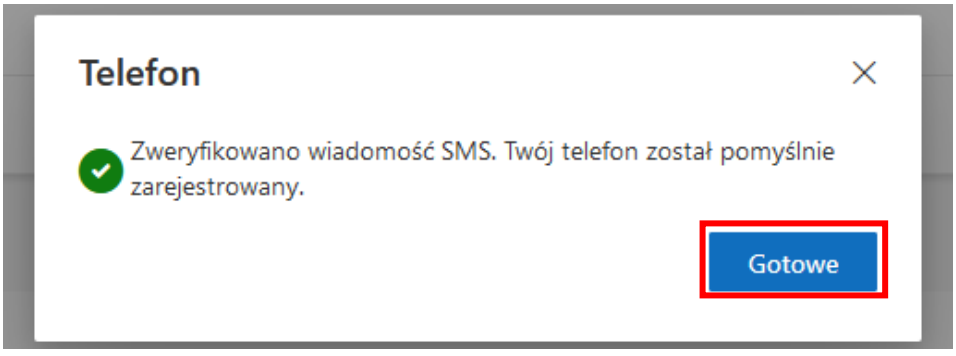
3. Należy pamiętać o wybraniu kraju w jakim jest zarejestrowany numer telefonu. Aby szybko wybrać polski region należy po rozwinięciu listy nacisnąć 8 razy klawisz „P” na klawiaturze.
4. Wpisujemy numer telefonu już bez prefixa.
5. Możemy wybrać, aby automat zadzwonił na ten numer telefonu (co jest wyjaśnione w następnym rozdziale), w tym przykładzie wybierzemy opcję SMS.



Przepisujemy kod, który dostaniemy SMSem z telefonu do aplikacji i wybieramy przycisk “Następne”.



Otrzymujemy komunikat o powodzeniu operacji, co oznacza koniec pełnej konfiguracji:



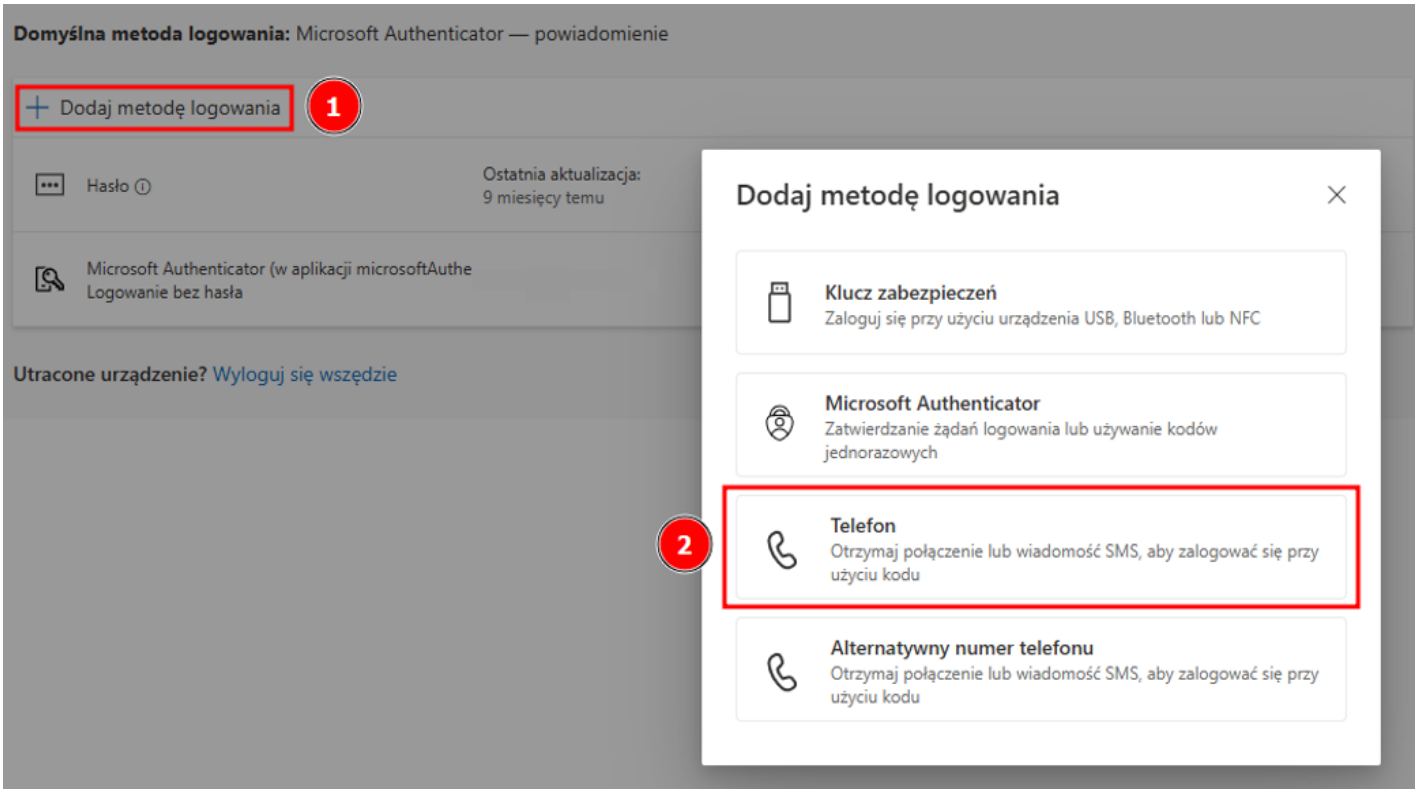
Konfiguracja numeru biurowego do autoryzacji głosowej

Poza metodą autoryzacji za pomocą numeru komórkowego jest opcja alternatywna w postaci autoryzacji numeru telefonu biurowego. W celu dodania numeru biurowego jako metody logowania przechodzimy do strony:

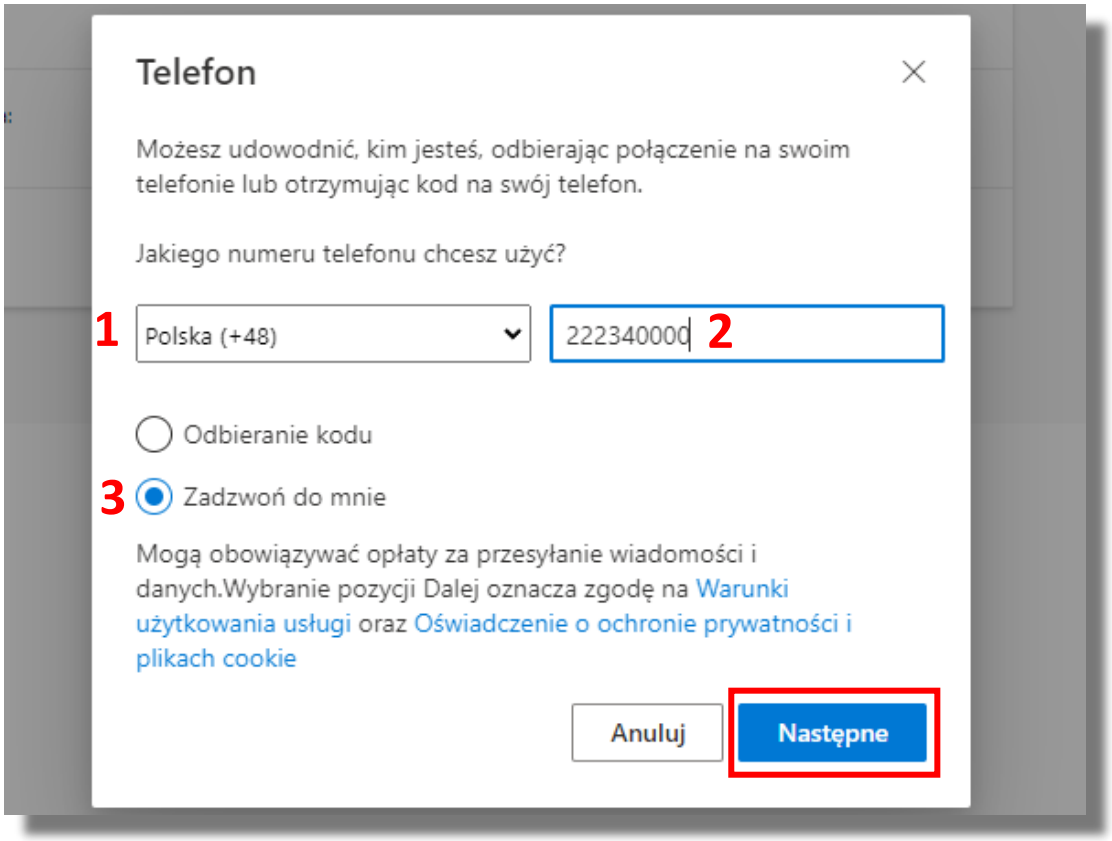
https://mysignins.microsoft.com/security-info

Następnie należy wykonać kroki dodania nowej metody w kolejności:

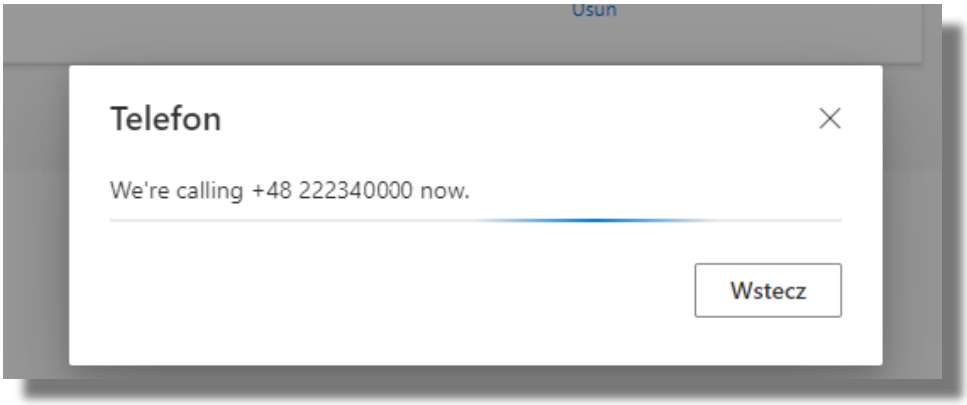
1. Wybieramy opcję “Dodaj metodę logowania”.
2. Z listy rozwijanej wybieramy “Telefon”.



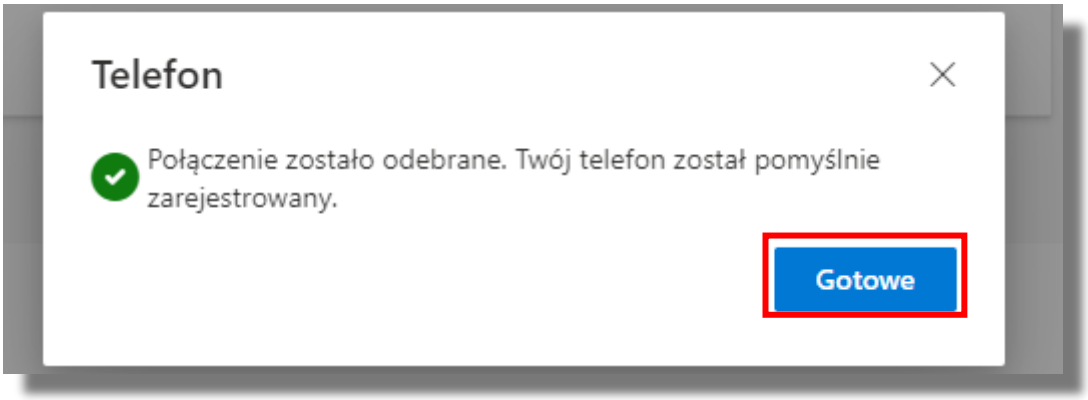
3. W celu wpisania wyboru kraju (Polska +48) a następnie wpisania numeru kierunkowego a następnie numeru biurowego np. 22 234 0000 (bez przerw). Jako opcję autoryzacji wybrać metodę „Zadzwoń do mnie”.



4. Po kliknięciu przycisku „Następne” nastąpi wykonanie połączenia głosowego na wpisany numer telefonu co będzie zapowiedziane komunikatem na ekranie:



5. Konsultant w języku angielsku poprosi o wciśnięcie na klawiaturze telefonu przycisku Hash (#), co należy wykonać a następnie rozłączyć się. Po wykonaniu tego kroku, wyświetli się komunikat o powodzeniu operacji i przypisaniu metody autoryzacji do konta.

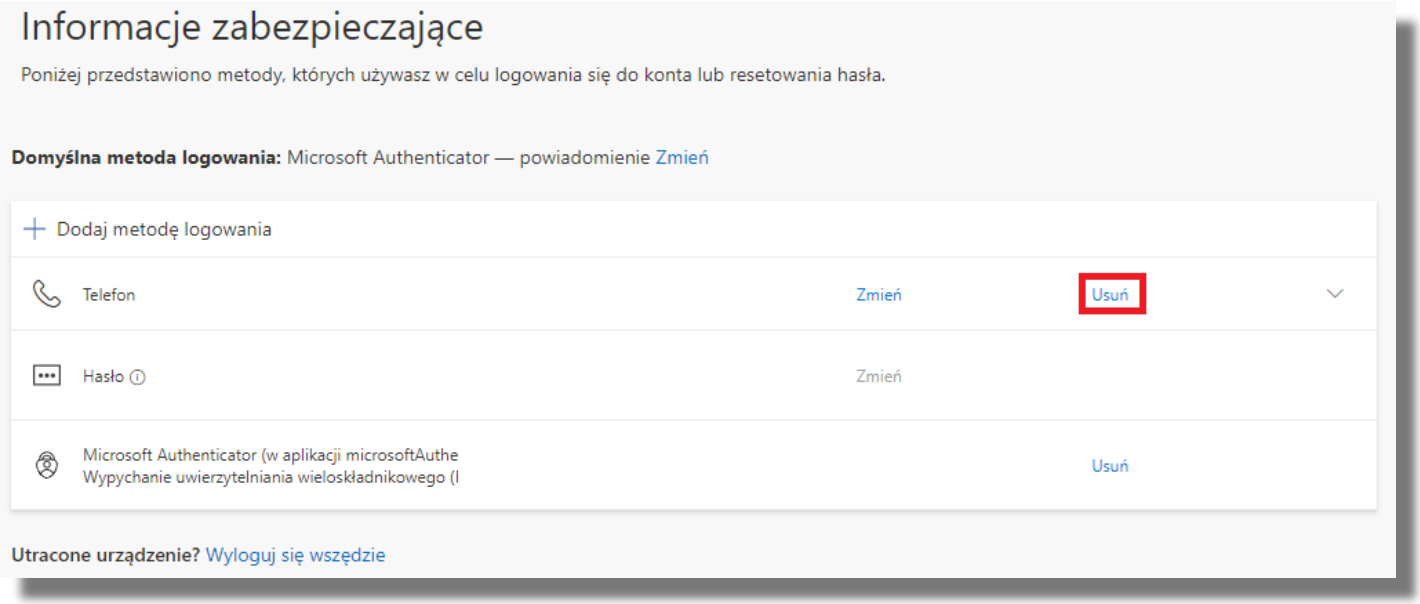


Usunięcie metody autoryzacji

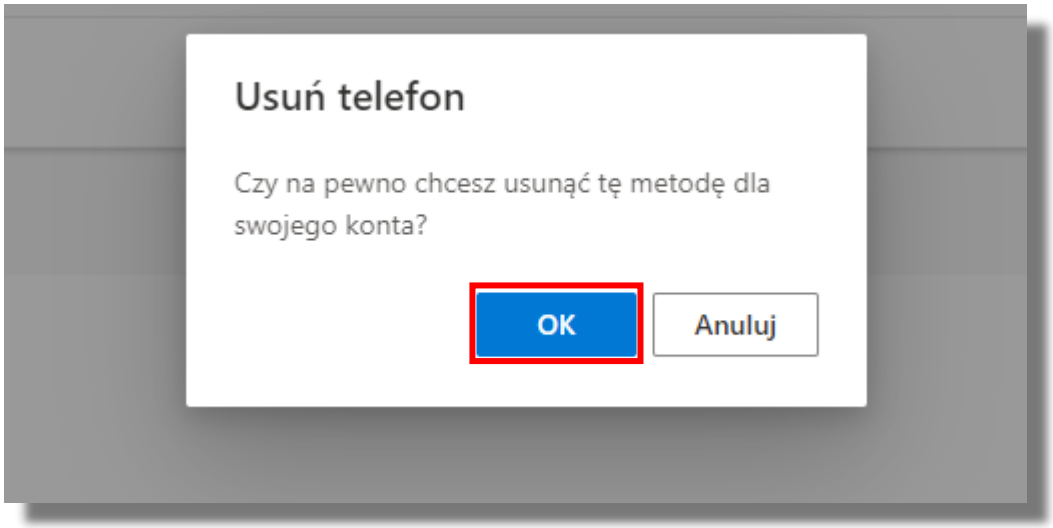
W przypadku zmiany modelu telefonu lub jego utraceniu należy usunąć go z metody uwierzytelniania wieloskładnikowego aby nie zablokować dostępu do konta.

W tym celu należy wejść na stronę https://mysignins.microsoft.com/security-info i dokonać przeglądu wykorzystywanych metod logowania.

W przypadku konieczności zmiany jednej z metod wystarczy przy wybranej metodzie nacisnąć przycisk „Usuń”:



A następnie potwierdzić przyciskiem „OK”:



W przypadku, gdy utracimy urządzenie i nie wiemy gdzie się ono znajduje warto nacisnąć przycisk „Wyloguj się wszędzie”, które spowoduje wymuszenie zalogowania się na nowo na wszystkich dotychczasowych urządzeniach.