Uwierzytelnianie dwuetapowe dla konta Microsoft 365

Instrukcja dla studentów

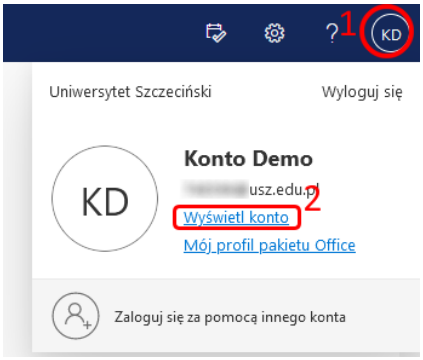
Uwierzytelnianie wieloskładnikowe, określane często skrótem MFA (od ang. *Multi-Factor Authentication*), to metoda zabezpieczania kont użytkownika. Opiera się o wykorzystanie więcej niż jednego elementu weryfikacji tożsamości użytkownika. W dobie coraz skuteczniejszych narzędzi do przechwytywania haseł to coraz popularniejszy sposób zabezpieczania usług cyfrowych przed nieuprawnionym dostępem. Aby w leszy sposób chronić dostęp do systemu Microsoft 365, a także innych systemów uczelnianych, korzystających z logowania za pośrednictwem konta w Microsoft 365, dla studentów została uruchomiona obowiązkowa autoryzacja dwuetapowa. W celu jej uruchomienia, konieczne jest skonfigurowanie metody potwierdzania tożsamości.

W poniższej instrukcji przedstawione zostaną dwie z nich - użycie aplikacji Microsoft Authenticator oraz uwierzytelnianie za pomocą kodów przesyłanych sms-ami.

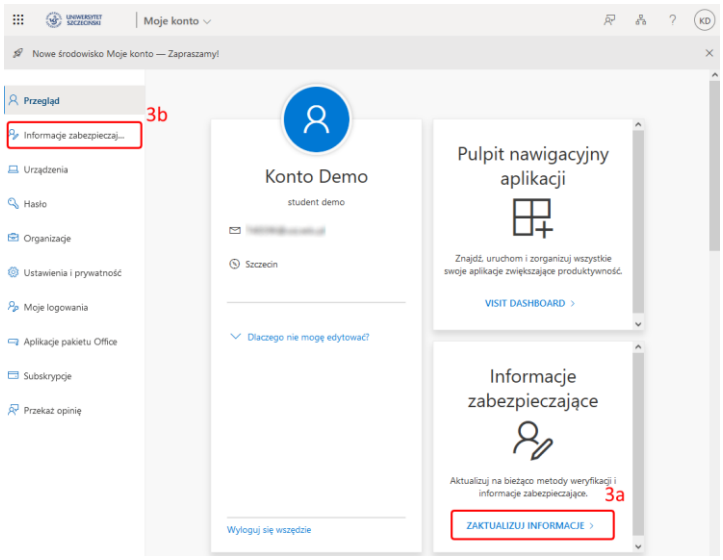
Uwaga: Uwaga. W przypadku studentów którzy logują się do swojego konta Microsotf 365 po raz pierwszy, lub NIE MAJĄ SKONFIGUROWANEJ ŻADNEJ METODY AUTORYZACJI DWUETAPOWEJ procedura konfiguracji konta jest WYMUSZANA po pierwszym zalogowaniu. Po wprowadzeniu loginu i hasła w oknie logowania Office 365 użytkownik jest automatycznie przekierowywany do konfiguracji logowania dwuetapowego za pomocą aplikacji Microsoft Authenticator. DO CZASU SKONFIGUROWANIA AUTORYZACJI DWUETAPOWEJ NIE BĘDZIE MOŻLIWE KORZYSTANIE Z KONTA!

Uwaga: instrukcja przedstawia proces uruchamiania autoryzacji dwuetapowej wykonywany w przeglądarce na komputerze stacjonarnym/laptopie. W przypadku korzystania z przeglądarki internetowej niektóre operacje mogą być realizowane w inny sposób.

Niezależnie od wybranej metody, aby skonfigurować usługę, należy zalogować się do swojego konta Microsoft 365, a następnie kliknąć znajdujący się w prawym górnym rogu okna przeglądarki ***przycisk menadżera konta*** **(1)**. W menu należy wybrać polecenie , a następnie, z menu wybrać polecenie ***Wyświetl konto*** **(2)**.



Następnie należy wybrać polecenie ***Informacje zabezpieczające***, bądź z kafelków na pulpicie **(3a)**, bądź z menu po lewej stronie **(3b)**.

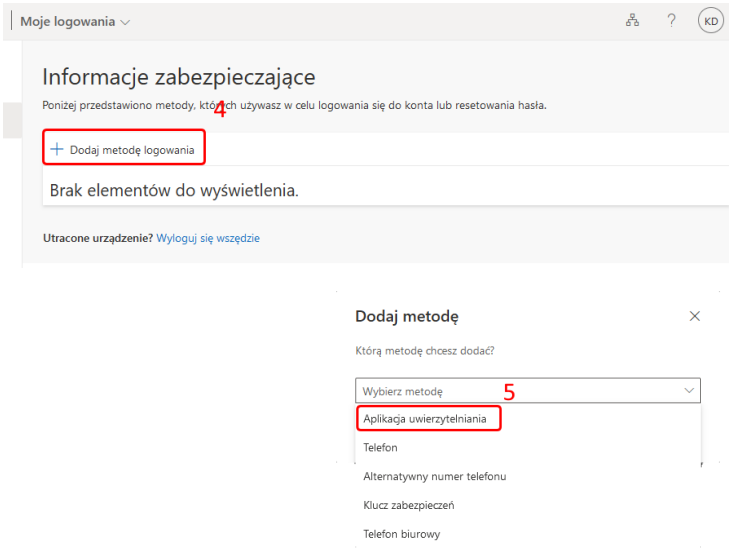


Wyświetlona zostanie konfiguracja uruchomione usługi zabezpieczeń. Dalsze postępowanie zależne jest od wybranej metody.

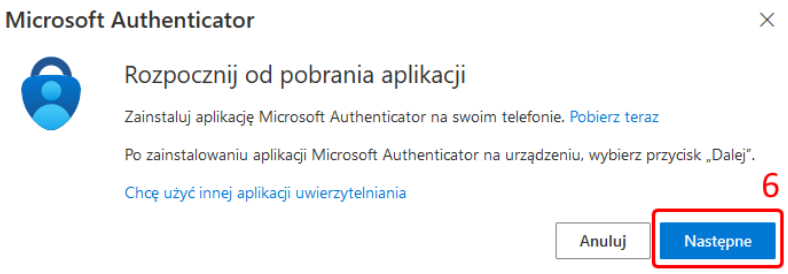
Aplikacja Microsoft Authenticator

Do użycia weryfikacji za pomocą aplikacji Microsoft authenticatro konieczne jest jej pobranie i zainstalowanie w smartphonie. Aplikacja jest bezpłatna, dostępna do pobrania, zależnie od producenta smarphonu, z Google Play lub AppStore. Procedura instalacji oprogramowania nie będzie tu omówiona, ze względu na różnorodność systemów i konfiguracji smartfonów.

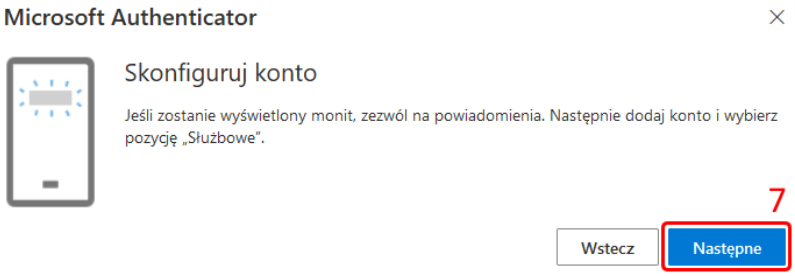
Na komputerze, na którym konfigurowana jest autoryzacja wieloetapowa oknie Informacje zabezpieczające należy kliknąć polecenie ***Dodaj metodę logowania*** **(4)**, a następnie z listy rozwijanej w oknie dialogowym wybrać metodę dodatkowego uwierzytelniania – ***Aplikacja uwierzytelniania*** **(5)**.



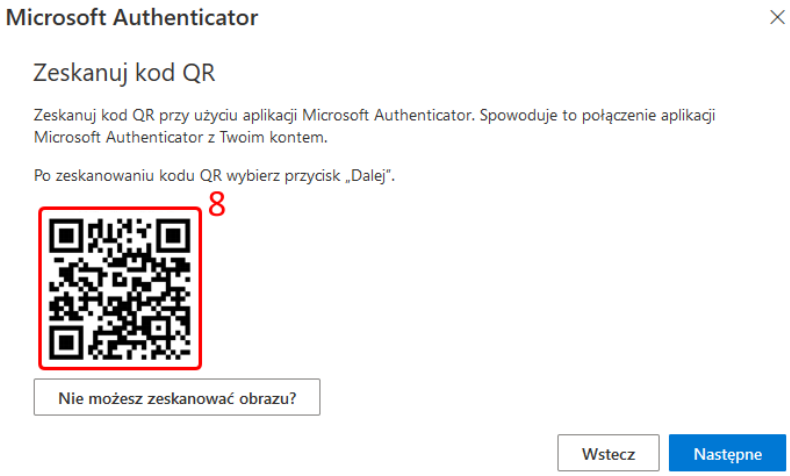
Wyświetlony zostanie monit o zainstalowanie aplikacji Microsoft Authenticator w telefonie, który będzie wykorzystywany do potwierdzania tożsamości. Aby kontynuować, po zainstalowani aplikacji należy kliknąć ***Następne*** **(6)**.



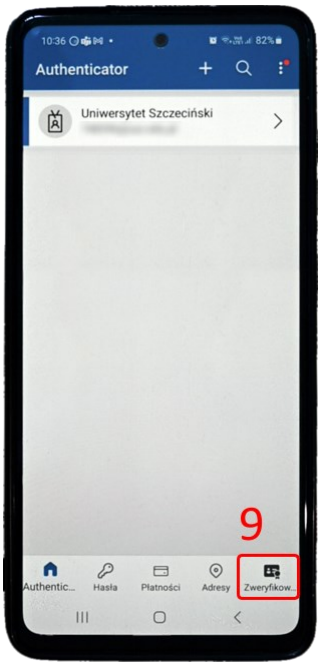
W kolejny oknie, informującym o możliwych monitach konfiguracyjnych, po zapoznaniu się z komunikatem należy kliknąć ***Następne*** **(7)**. Jeżeli w trakcie konfiguracji w smartfonie zostanie wyświetlone pytanie o zgodę na powiadomienia z aplikacji „Authenticator, należy jej udzielić.



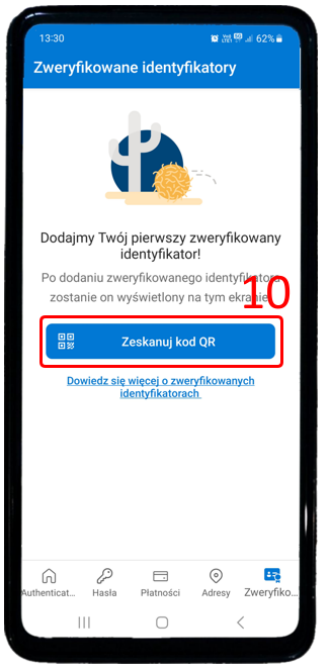
Na ekranie komputera wyświetlony zostanie kod QR **(8)**.



‚W tym momencie należy uruchomić aplikację Athenticator w telefonie, a następnie z głównego menu aplikacji wybrać polecenie ***Zweryfikowane identyfikatory*** **(9)**.

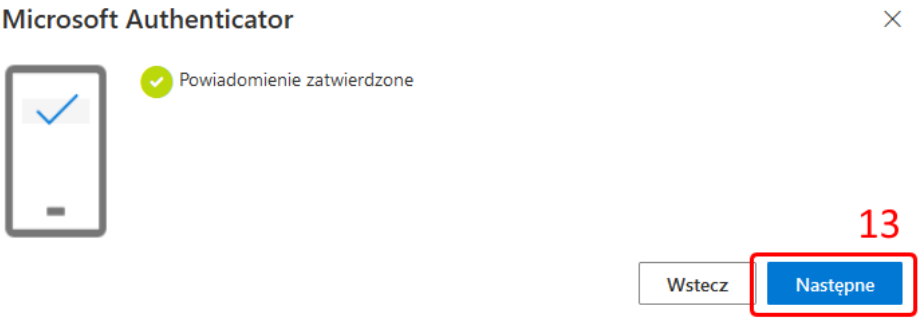


Na kolejnym ekranie należy wybrać polecenie ***Zeskanuj kod QR*** **(9)**.



Po uruchomieniu aparatu, należy zeskanować kod QR z monitora komputera. Konto Microsoft 365 zostanie automatycznie dodane do aplikacji i wyświetlone na liście w głównym oknie aplikacji. W celu potwierdzenia prawidłowości parowania urządzenia i konta, wyświetlony zostanie monit o wprowadzenie w aplikacji dwucyfrowego ***kodu weryfikacyjnego*** **(11)**. Kod należy wpisać w ***pole aplikacji*** **(12)** i zatwierdzić.

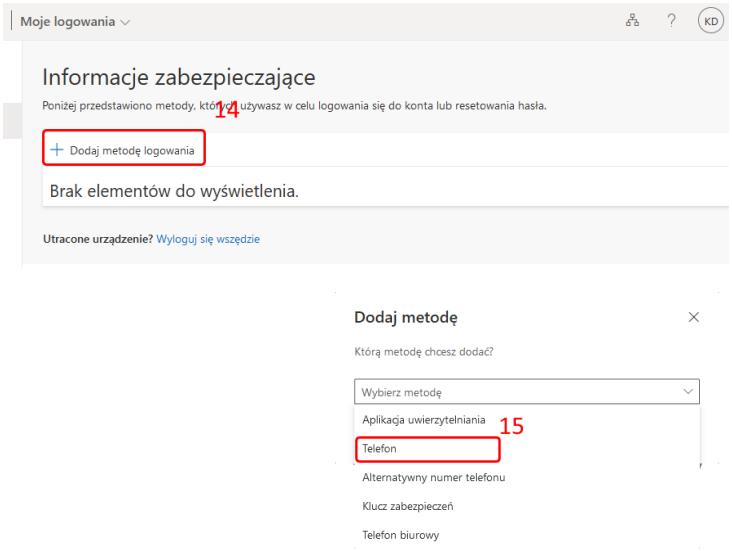
Konfiguracja konta jest zakończona, należy tylko potwierdzić jej prawidłowość o oknie dialogowym **(11)**.



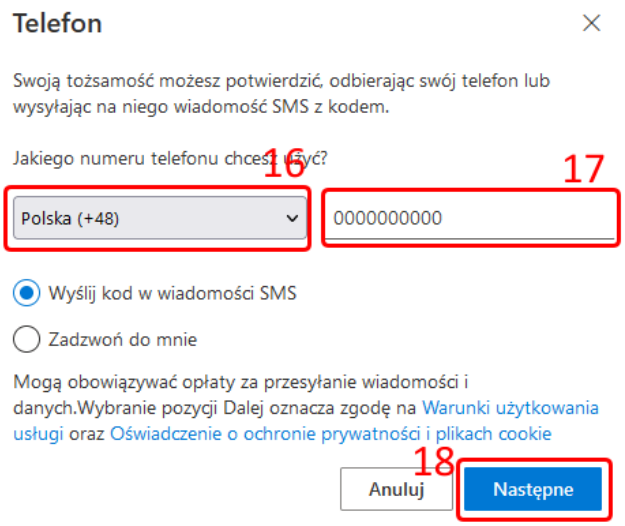
UWAGA! Usunięcie z telefonu aplikacji Authenticator, jeżeli nie została skonfigurowana żadna inna metoda uwierzytelniania, uniemożliwi korzystanie z konta!

Weryfikacja za pomocą kodów SMS

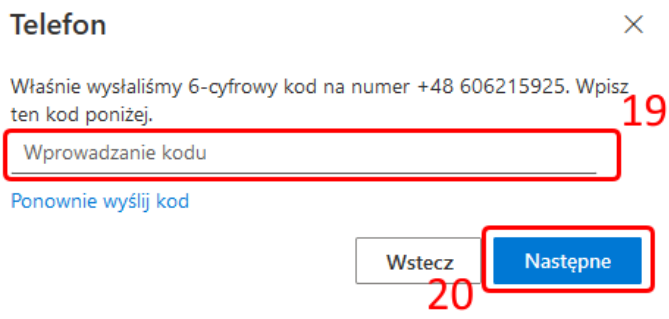
Na komputerze, na którym konfigurowana jest autoryzacja wieloetapowa oknie Informacje zabezpieczające należy kliknąć polecenie ***Dodaj metodę logowania*** **(14)**, a następnie z listy rozwijanej w oknie dialogowym wybrać metodę dodatkowego uwierzytelniania – ***Telefon*** **(15)**.



Następnie w kolejnym oknie dialogowym należy wskazać kraj w którym zarejestrowany jest telefon **(16)** oraz wpisać numer telefonu komórkowego w odpowiednie pole **(17)**. Wprowadzone dane należy zatwierdzić klikając ***Następne*** **(18)**



Otrzymany w wiadomości sześciocyfrowy kod należy wprowadzić w pole w oknie dialogowym **(18)** i zatwierdzić klikając w polecenie ***Nastepne*** **(18)**.



Konfiguracja konta jest zakończona, należy tylko potwierdzić jej prawidłowość o oknie dialogowym **(21)**.