



Instrukcja instalacji

mSzyfr

1 Spis treści

1	Spis treści	2
2	Rejestracja nowego konta	3
2.1	Aplikacja mSzyfr – konfiguracja OTP	3
2.2	Microsoft Authenticator - konfiguracja.....	4
2.3	Aplikacja mSzyfr – logowanie się	5
3	Pytania i odpowiedzi.....	8
3.1	Dane do logowania się	8
3.2	Konfiguracja OTP/MFA	8
3.3	Logowanie się	9
3.4	Konfiguracja mSzyfr	9
3.5	Użytkowanie mSzyfr	12
3.6	Migracja z Threema	12
3.7	Ogólne informacje o aplikacji mSzyfr	13

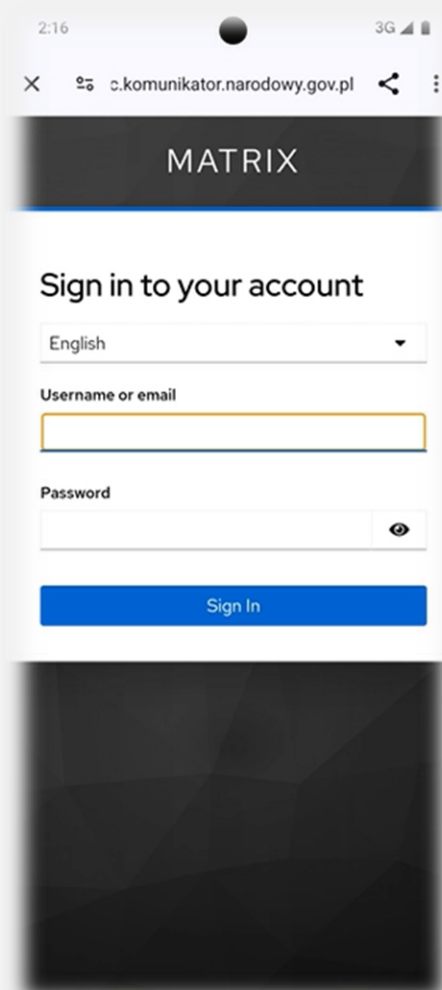
2 Rejestracja nowego konta

2.1 Aplikacja mSzyfr – konfiguracja OTP

1. Zainstaluj i uruchom aplikację mSzyfr
2. Zaloguj się do aplikacji przyciskiem „sign in”



3. Zaloguj się przy wykorzystaniu danych, które otrzymałeś mailem, albo od swojego Administratora.



4. Po zalogowaniu wyświetli Ci się ekran:



5. Zainstaluj aplikację ze sklepu Google Play. Proponujemy instalację Microsoft Authenticator. Jeśli korzystasz z telefonu służbowego, może być wymagana instalacja aplikacji przez administratora
6. Przejdź do aplikacji Microsoft Authenticator.

2.2 Microsoft Authenticator konfiguracja

1. Uruchom aplikację Microsoft Authenticator:

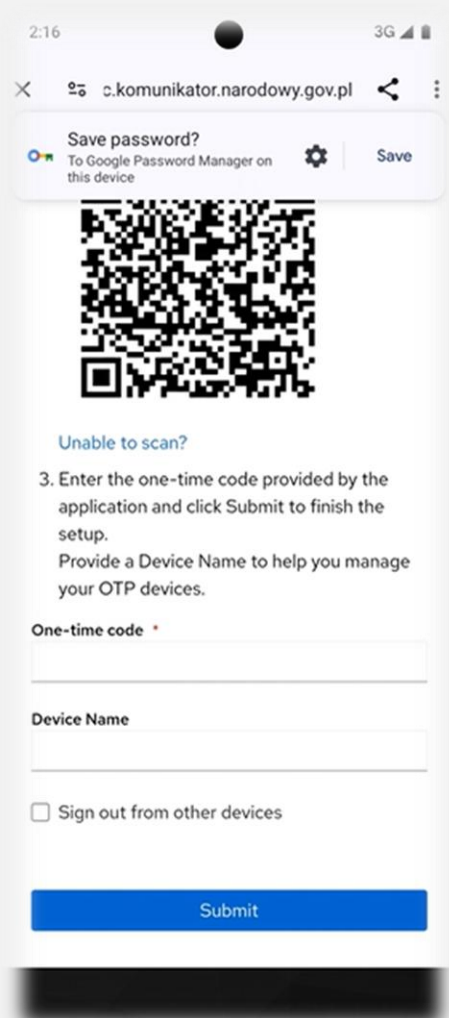


2. W aplikacji Microsoft Authenticator
- Wybierz ikonę „+”, wskaż rodzaj konta (inne),
 - Zeskanuj kod QR z aplikacji mszyfr
 - jeśli nie możesz zeskanować kodu naciśnij w aplikacji mSzyfr *unable to scan* – wyświetli Ci się kod do wprowadzenia.
 - Przepisz do aplikacji Microsoft Authenticator (odpowiednia opcja pokazuje się po wybraniu opcji *enter code manually*).
 - Nadaj nowej pozycji nazwę mSzyfr (to może pomóc nam w przypadku konieczności diagnostyki)
 - postępuj zgodnie z komunikatami na ekranie.
 - Ostatecznie, pojawi się w authenticatorze pozycja o nazwie mSzyfr.

- f. Kliknij na tę pozycję:
zostanie wyświetlony 6-
cio cyfrowy kod
jednorazowy
3. Wróć do aplikacji mSzyfr.

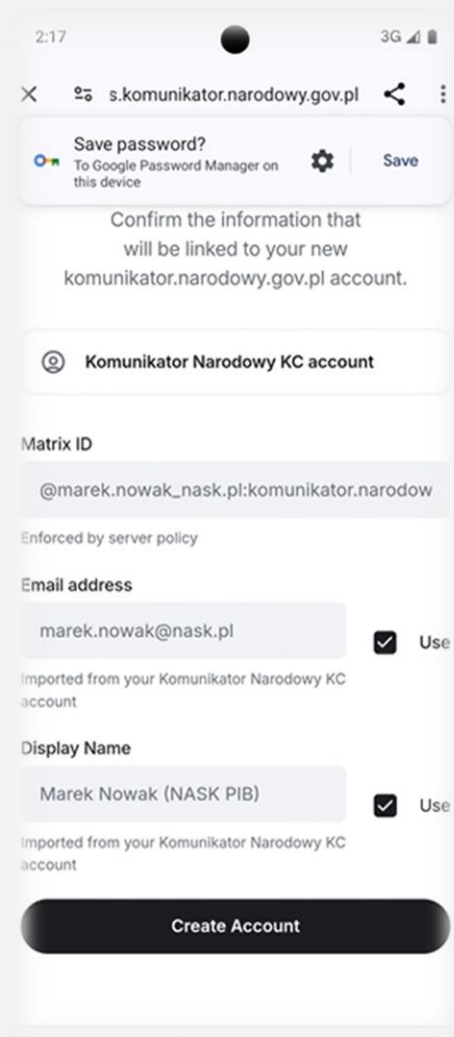
2.3 Aplikacja mSzyfr – logowanie się

1. Przewiń ekran na dół strony:



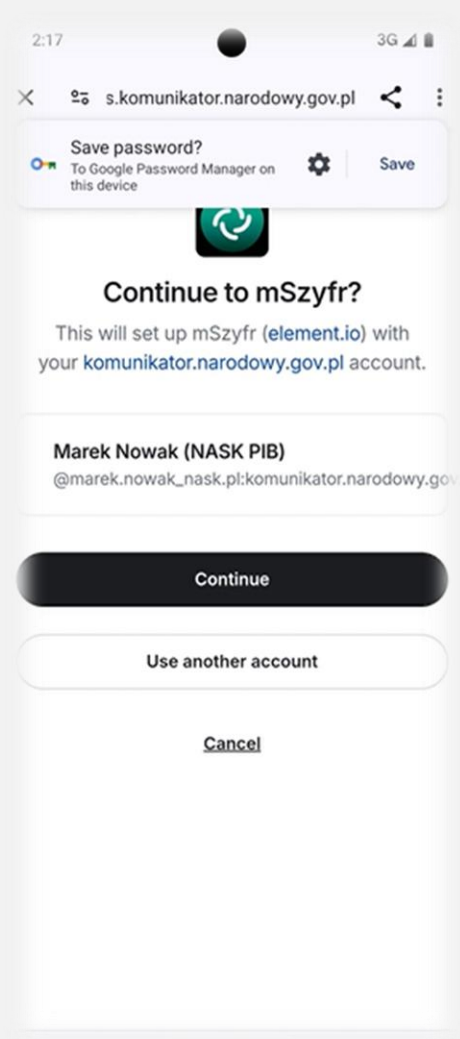
2. Wprowadź kod jednorazowy i nazwę urządzenia (podaj dowolną wybraną przez siebie nazwę)
3. Wciśnij przycisk *submit*

4. Pojawi się okno podsumowania i potwierdzenia dołączenia aplikacji do konta:

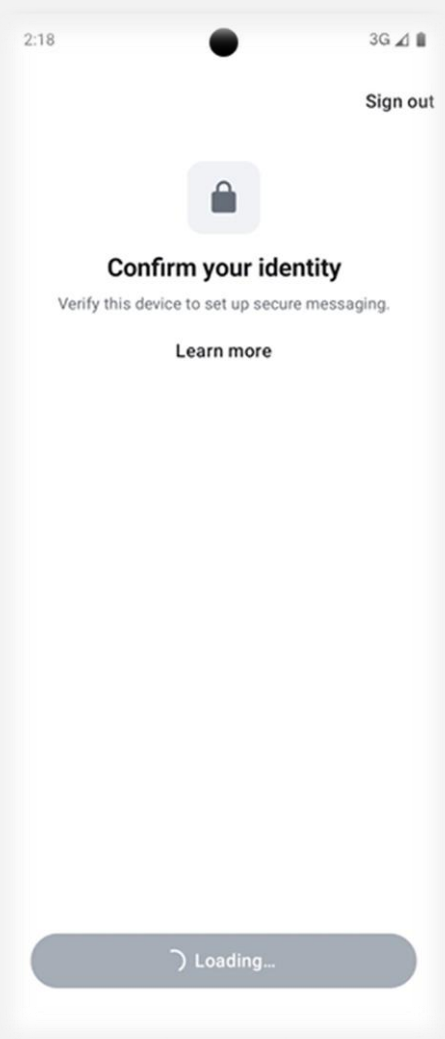


5. Wybierz *create account*

6. Zostaniesz poproszony o jeszcze jedno potwierdzenie:

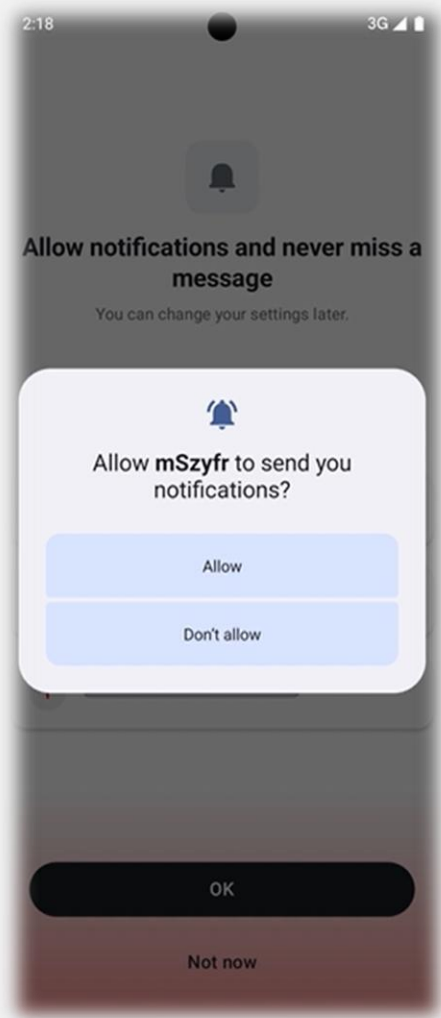


8. Pojawi się okno confirm your identity

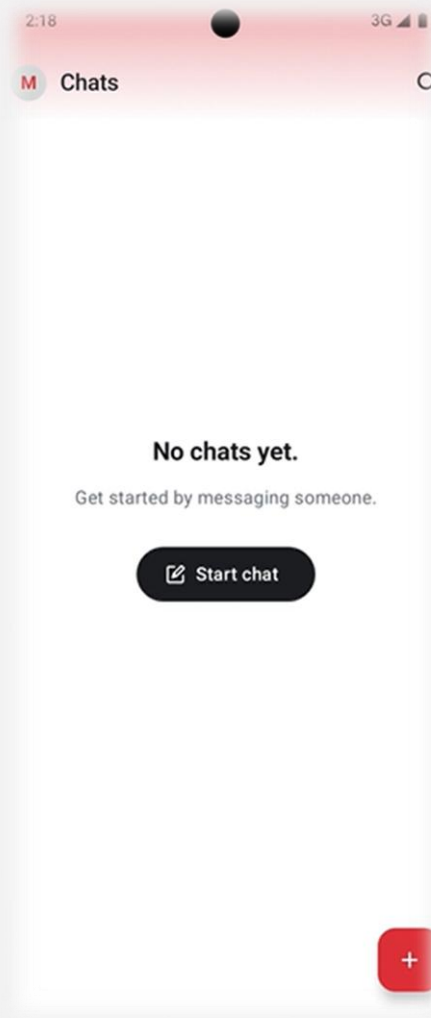


7. Wybierz opcję kontynuacji.

9. Po zalogowaniu się zostaniesz poproszony o zgodę na zezwolenie na wysyłanie notyfikacji. Rekomendujemy wyrażenie zgody.



10. Po wyrażeniu zgody powinien pojawić się ekran powitalny aplikacji



Gratulujemy! Uzyskałeś dostęp do aplikacji mSzyfr i możesz zacząć z niej korzystać.

3 Pytania i odpowiedzi

3.1 Dane do logowania się

Nie wiem czy moja instytucja korzysta z mSzyfr. Co robić?

Spróbuj ustalić w ramach normalnej drogi służbowej, czy Twoja instytucja jest w mSzyfr. Jeśli nie udało się potwierdzić w Twojej instytucji: wyślij maila z zapytaniem na adres mszyfr@nask.pl.

Nie dostałem maila z danymi uwierzytelniającymi – co zrobić?

Skontaktuj się z administratorem mSzyfr w swojej instytucji. Administrator będzie w stanie wygenerować i przekazać Ci dane uwierzytelniające.

Kto przesyła maila z danymi uwierzytelniającymi?

Mail z danymi uwierzytelniającymi jest generowany bezpośrednio po utworzeniu konta w systemie. Jest wysyłany automatycznie z adresu mszyfr@nask.pl.

3.2 Konfiguracja OTP/MFA

Czy można to samo konto stosować dla aplikacji mobilnej i portalu web?

Tak, każdy z użytkowników aplikacji mobilnej może wykorzystywać to samo konto do logowania się na portalu: <https://komunikator.narodowy.gov.pl>

Czy można skorzystać z innej aplikacji niż Microsoft Authenticator?

Tak. Podczas logowania pojawia się lista wspieranych aplikacji. Preferujemy aplikację Microsoft, ze względu na to, że dużo instytucji korzysta ze środowisk Microsoft. W przypadku innych aplikacji authenticatora niż te, wymienione na ekranie z kodem QR, nie gwarantujemy poprawnej współpracy.

Czy mogę nazwać wpis OTP inaczej niż mSzyfr?

Tak. Nazwa jest dowolna. Proponujemy jednak zachowanie mSzyfr, tak żeby uniknąć omyłek.

Mam aplikację authenticatora na tym samym telefonie, na którym jest zainstalowany mSzyfr i nie mogę odczytać kodu QR. Co mam robić?

Zazwyczaj aplikacja authenticatora przewiduje możliwość odczytania zawartości kodu i przepisania go do aplikacji. Szukaj opcji takich jak: *unable to scan*, *nie mogę zeskanować kodu*, *odczytaj kod* itp. W przypadku aplikacji mSzyfr możliwe jest ręczne wprowadzenie kodu (opcja: *unable to scan*).

Czy jest możliwość podłączenia innego składnika uwierzytelnienia np. klucza Yubikey?

Aktualnie nie wspieramy uwierzytelnienia, w którym stosuje się inne metody niż aplikacja authenticatora. Docelowo nie wykluczamy umożliwienia tego rodzaju funkcji.

3.3 Logowanie się

Nie wyświetla się strona logowania – co robić?

Upewnij się, że uruchomiłeś właściwą aplikację i podłączyłeś aplikację z niniejszą instrukcją. Jeśli pojawia się błąd, otwórz przeglądarkę i spróbuj otworzyć stronę: <https://komunikator.narodowy.gov.pl>

Jeśli strona się nie otwiera: skontaktuj się z administratorem mSzyfr w swojej instytucji, żeby zweryfikować, czy ruch nie jest blokowany. Sugerujemy, żeby administrator instytucji kontynuował kontakt z naszym helpdeskiem, tak żeby można było zweryfikować, co jest przyczyną problemu i czy ma on charakter globalny w obrębie instytucji.

Aplikacja informuje o błędnym kodzie OTP

Upewnij się, że przepisyujesz właściwy kod. Kod powinien być 6-cio cyfrowy. Upewnij się, że okres ważności kodu nie upłynął (kod wygaśnięty może zostać odrzucony). Jeśli w dalszym ciągu otrzymujesz błąd, skontaktuj się z administratorem mSzyfr w swojej instytucji.

Pojawia się informacja o błędnym użytkowniku lub hasle

Zweryfikuj czy poprawnie wprowadzasz nazwę użytkownika i hasło. W przypadku dalszego występowania błędów, skontaktuj się z administratorem mSzyfr w swojej instytucji.

Czy konto mSzyfr można zablokować?

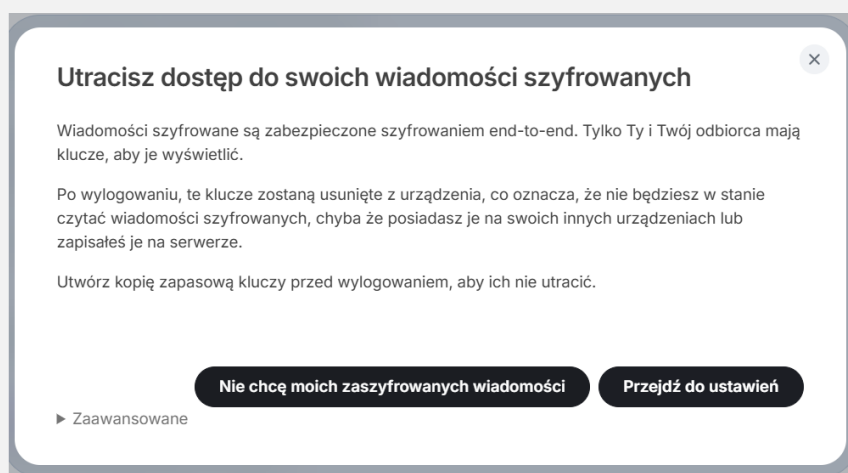
Tak, konto mSzyfr po trzech nieudanych próbach logowania blokuje się na określony przez administratora przedział czasu. W celu podjęcia kolejnych prób logowania należy odczekać maksymalnie 15 minut.

3.4 Konfiguracja mSzyfr

Aplikacja prosi o wygenerowanie kluczy zabezpieczających do szyfrowania end-to-end – jak to zrobić?

Aplikacja mSzyfr może wyświetlić ostrzeżenie o możliwości utraty dostępu do danych i poprosić o wygenerowanie klucza przywracania.

Uwaga! Domyślnie, bez kluczy przywracania, po wylogowaniu się, użytkownik traci dostęp do szyfrowanych wiadomości!



Rysunek 3.1 Ostrzeżenie na w wersji przeglądarkowej



Rysunek 3.2 Ostrzeżenie w wersji mobilnej

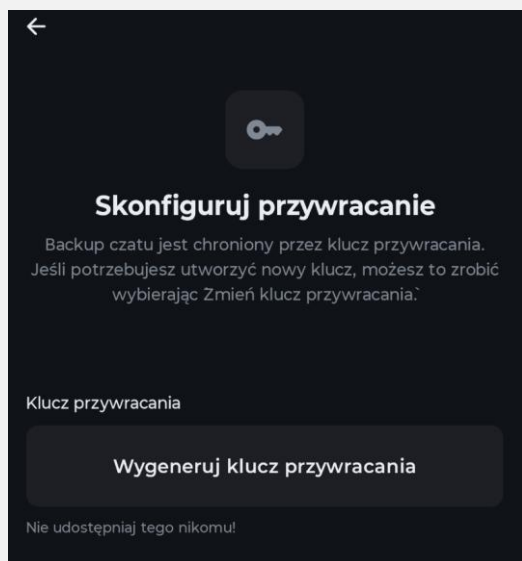
Konfiguracja przywracania wiąże się z przechowywaniem kluczy do szyfrowania na serwerze, który znajduje się w postaci zaszyfrowanej u Operatora mSzyfr. Użytkownik uzyskuje hasło, po wpisaniu którego możliwe jest odszyfrowanie tych danych i odszyfrowanie konwersacji.

W celu wygenerowania klucza przywracania należy wybrać *skonfiguruj przywracanie*. Pojawi się opcja włączenia magazynu kluczy i po włączeniu opcji pojawia się możliwość skonfigurowania.

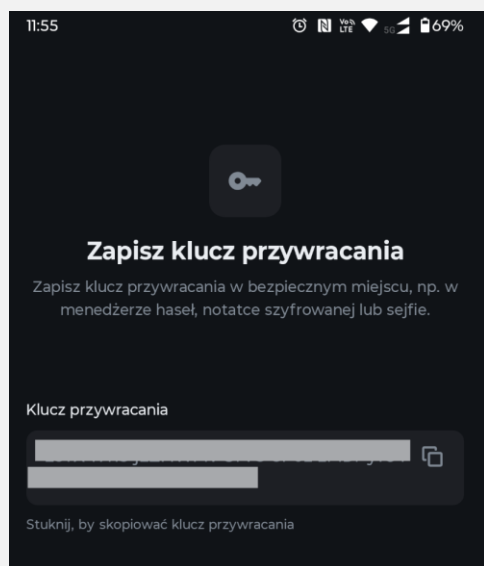


Rysunek 3.3 konfiguracja przywracania

Po wybraniu opcji pojawia się ekran umożliwiający generowanie klucza przywracania:



Rysunek 3.4 Generowanie przywracania



Rysunek 3.5 Wygenerowany klucz przywracania

Wygenerowany klucz należy zapisać i przechowywać w bezpiecznym miejscu. W przypadku nowego logowania się, lub konfiguracji nowego urządzenia użytkownik zostanie poproszony o wprowadzenie tego klucza. Alternatywą jest potwierdzenia logowania się na innym urządzeniu, na którym użytkownik jest zalogowany.

3.5 Użytkowanie mSzyfr

Jak wyszukać użytkownika po nazwisku?

Żeby wyszukać użytkownika, z którym jeszcze się nie kontaktowałeś wybierz przycisk „+”. Pojawi się okno wyszukiwania nowych użytkowników. Wprowadź pierwsze trzy litery nazwiska. Jeśli nazwisko składa się z dwóch liter – po dwóch literach podaj spację. Aplikacja zwróci Ci listę użytkowników spełniających kryteria.

Jak wyszukać użytkowników w danej instytucji?

Żeby wyszukać użytkowników z instytucji, wybierz przycisk „+”. Pojawi się okno wyszukiwania nowych użytkowników. Wprowadź pierwsze trzy litery nazwy instytucji. Jeśli nazwa składa się z dwóch liter, po dwóch literach podaj spację. Aplikacja zwróci Ci listę użytkowników spełniających kryteria (w tym wypadku przynależących do danej instytucji).

3.6 Migracja z Threema

Czy moje dane historyczne zostaną przeniesione z komunikatora Threema?

Nie. Twoje dane nie zostaną przeniesione z komunikatora Threema. Dane są szyfrowane i nie jest możliwa ich migracja.

Czy moje grupy zostaną przeniesione z komunikatora Threema?

Nie. Nie przewidujemy migracji grup, ani danych z komunikatora Threema. Rekomendujemy utworzenie w komunikatorze mSzyfr wyłącznie grup, które są aktywnie wykorzystywane.

Czy wszyscy użytkownicy Threema będą dostępni w aplikacji mSzyfr?

Tak. Zakładamy migrację wszystkich aktywnych użytkowników do nowej aplikacji.

Czy po migracji będę mógł od razu logować się do aplikacji mSzyfr?

Nie. Konieczne jest wcześniejsze wykonanie niniejszej procedury konfiguracji konta.

3.7 Ogólne informacje o aplikacji mSzyfr

Czy mogę zadzwonić z aplikacji mSzyfr do innych aplikacji rządowych?

Nie. Aktualnie mSzyfr nie jest sfederowany z innymi aplikacjami komunikatora.

Czy mogę zadzwonić z aplikacji mSzyfr na MS Teams i odwrotnie?

Nie. Aplikacja mSzyfr nie jest sfederowana z komunikatorem Microsoftu.

Jak wypada mSzyfr w porównaniu z innymi komunikatorami?

					
Nazwa	mSzyfr	Threema	Whatsapp	Signal	Telegram
Pivacy by design	☒	☒	☐	☐	☐
Szyfrowanie end-to-end	☒	☒	☒	☒	
Open Source	☒	☒	☐	☒	☒
Zgodność z RODO	☒	☒	☐	☐	☐
Dostępność rozwiązania komercyjnego	☒	☒	☐	☐	☐
Raport przejrzystości	☒	☒	(☒)	☐	☐
Finansowanie	Rząd RP	Użytkownicy (komercyjne)	Meta/ reklamy	Datki/ Briam Acton	Pavel Durov/ subskrypcje/ reklamy
Jurysdykcja	Polska	Szwajcaria	USA	USA	n/a

Jakie języki wspiera aplikacja mSzyfr?

Lista języków w aplikacji została ograniczona do polskiego i angielskiego.