



eRepozytorium w Chmurze

Instrukcja użytkownika

Spis treści

1. eRepozytorium w Chmurze.....	3
1.1 Rozpoczęcie pracy z Modułem Integracji eRepozytorium w Chmurze.....	3
1.1.1 Konfiguracja modułu.	3
1.1.2 Konfiguracja modułu od wersji 9.10.0 aplikacji mMedica.	5
1.1.3 Aktualizacja certyfikatów dla konta tenanta od wersji 8.2.1 aplikacji mMedica.	8
1.1.4 Przekazanie danych o „Strukturze Organizacyjnej” podmiotu.	8
1.1.5 Rodzaje archiwizowanych dokumentów.	8
1.1.6 Zapis certyfikatów komunikacyjnych TLS/WSSE na dysk.	10
1.2. Przegląd dokumentów.	11
1.3. Rejestracja „eRepozytorium w Chmurze” w domenie krajowej (System P1).	12
1.4. Rejestr zgód.	14
1.5. Migracja dokumentów z repozytorium zewnętrznego.	15
2. Rozwiązania częstych problemów.	17
2.1 Nie udało się pobrać id repozytorium z domeny krajowej.	17
2.2 Limit czasu operacji został przekroczony.....	18
2.3 Wystąpił błąd „Bad Request (400)”.	19
2.4 Wystąpił błąd: „Forbidden (403)”.....	20
2.5 Wystąpił błąd: „Wystąpił błąd w obsłudze bezpiecznego kanału”.....	21
2.6 Wystąpił błąd: „Nie można przekazać CSR do BOK z powodu błędów podczas próby wysyłki e-mail”.	21
2.7 Przerwa serwisowa/techniczna dla usługi „eRepozytorium w Chmurze”.	22

1. eRepozytorium w Chmurze.

System „**eRepozytorium w Chmurze**” to rozwiązanie funkcjonalne służące do gromadzenia dokumentacji medycznej w formie dokumentów HL7 CDA PIK w dedykowanej bazie danych znajdującej się w zewnętrznej chmurze. Składa się z dwóch elementów:

1. licencji „Moduł Integracji eRepozytorium w Chmurze”, kupowanej w sklepie Centrum Zarządzania Licencjami mMedica (mmmedica-licencje.asseco.pl),
2. usługi „eRepozytorium mMedica w chmurze”, kupowanej w sklepie „chmuradlzdrowia.pl”.

Rozwiązanie umożliwia składowanie dokumentów medycznych, ich wyszukiwanie, pobieranie oraz usuwanie. Scentralizowany magazyn dokumentów pozwala na wygodne i bezpieczne zarządzanie danymi.

UWAGA! Moduł eArchiwum i Moduł Integracji eRepozytorium w Chmurze nie mogą być uruchomione jednocześnie dla tej samej instalacji.

Ilustracje i „zrzuty” ekranowe zamieszczone w niniejszej publikacji mają charakter instruktażowy i mogą odbiegać od rzeczywistego wyglądu ekranów. Rzeczywisty wygląd ekranów zależy od posiadanej wersji aplikacji, aktywnych modułów dodatkowych oraz numeru wydania. Większość zrzutów ekranowych zamieszczonych w niniejszej instrukcji została wykonana przy pomocy wersji Standard+ z aktywnymi wszystkimi modułami dodatkowymi.

1.1 Rozpoczęcie pracy z Modułem Integracji eRepozytorium w Chmurze.

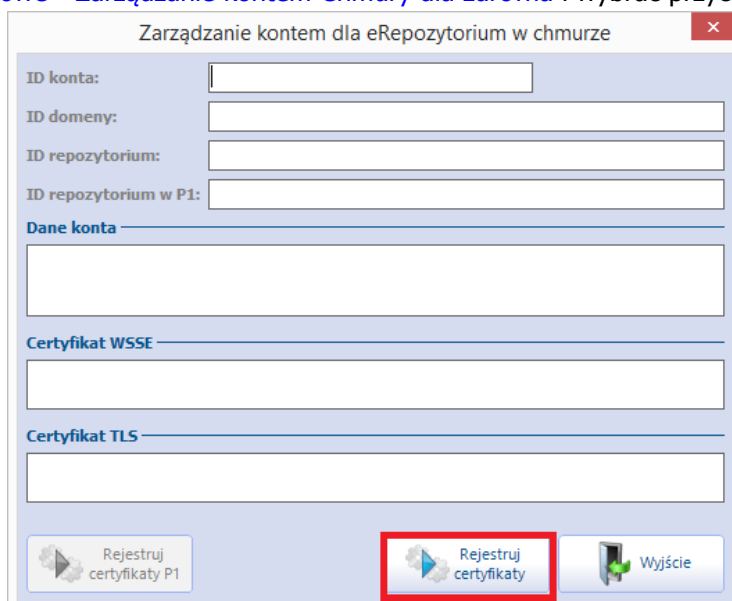
Należy dokonać konfiguracji modułu w programie mMedica, poprzez:

- a) wprowadzenie identyfikatora konta oraz zaczytanie kluczy służących do komunikacji z zasobem chmurowym
- b) określenie, jakie rodzaje dokumentów i w jakim interwale czasowym mają być zapisywane w archiwum.

1.1.1 Konfiguracja modułu.

Ścieżka: [Zarządzanie > Konfiguracja > Konfigurator](#), obszar: [Funkcje dodatkowe > Zarządzanie kontem Chmury dla zdrowia](#).

Pierwszym etapem konfiguracji jest wprowadzenie identyfikatora konta oraz zaczytanie certyfikatów służących do komunikacji z zasobem chmurowym. W tym celu należy przejść do ścieżki: [Zarządzanie > Konfiguracja > Konfigurator](#), obszar [Funkcje dodatkowe > Zarządzanie kontem Chmury dla zdrowia](#) i wybrać przycisk „Rejestruj certyfikaty”.



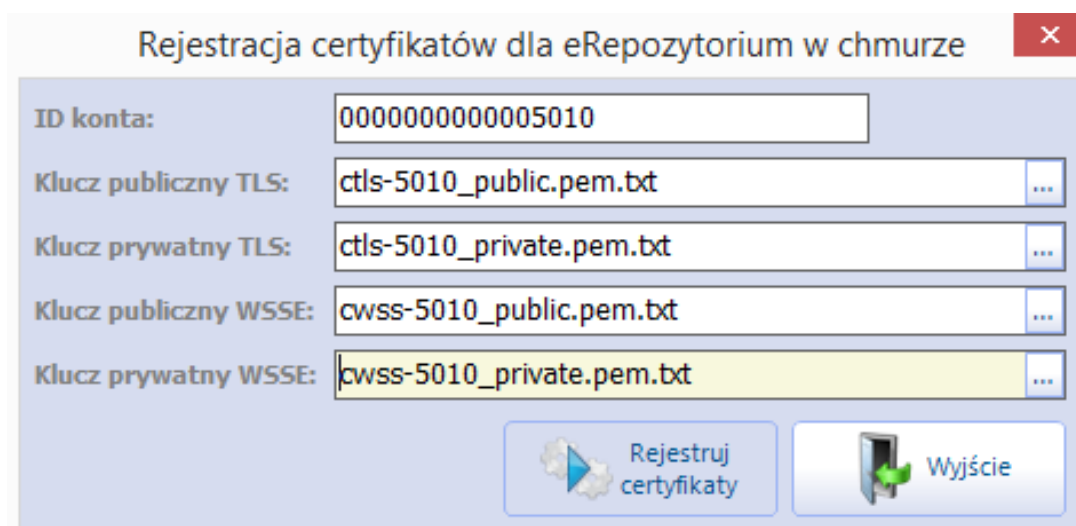
W polu „ID Konta” należy wprowadzić identyfikator konta w chmurze otrzymany w procesie zamawiania produktu w „chmuradlazdrowia.pl”.

Z kolei w polach:

- a) Klucz publiczny TLS
- b) Klucz prywatny TLS
- c) Klucz publiczny WSSE
- d) Klucz prywatny WSSE

należy wskazać pliki wygenerowane w procesie składania zamówienia (klucz prywatny TLS, WSSE) oraz klucze publiczne przekazane przez Biuro Obsługi Klienta sklepu „chmuradlazdrowia.pl”.

UWAGA! Nie należy udostępniać kluczy prywatnych osobom trzecim, są to pliki poufne.



Rejestracja certyfikatów dla eRepozytorium w chmurze

ID konta: 0000000000005010

Klucz publiczny TLS: ctls-5010_public.pem.txt

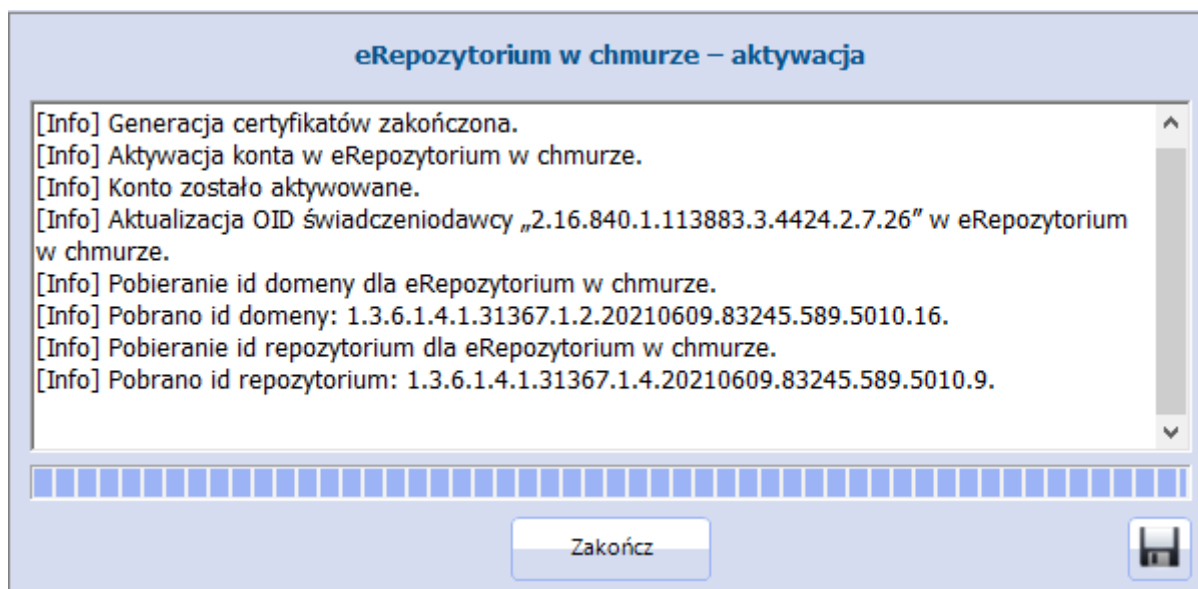
Klucz prywatny TLS: ctls-5010_private.pem.txt

Klucz publiczny WSSE: cwss-5010_public.pem.txt

Klucz prywatny WSSE: cwss-5010_private.pem.txt

Rejestruj certyfikaty Wyjście

Wybranie przycisku „Rejestruj certyfikaty” uruchamia proces aktywacji konta w chmurze, w wyniku którego zostaną przekazane identyfikatory techniczne konta. Przykładowe komunikaty zwrócone w procesie rejestracji przedstawiono poniżej:



eRepozytorium w chmurze – aktywacja

[Info] Generacja certyfikatów zakończona.
[Info] Aktywacja konta w eRepozytorium w chmurze.
[Info] Konto zostało aktywowane.
[Info] Aktualizacja OID świadczeniodawcy „2.16.840.1.113883.3.4424.2.7.26” w eRepozytorium w chmurze.
[Info] Pobieranie id domeny dla eRepozytorium w chmurze.
[Info] Pobrano id domeny: 1.3.6.1.4.1.31367.1.2.20210609.83245.589.5010.16.
[Info] Pobieranie id repozytorium dla eRepozytorium w chmurze.
[Info] Pobrano id repozytorium: 1.3.6.1.4.1.31367.1.4.20210609.83245.589.5010.9.

Zakończ

Wybranie przycisku „Zakończ” przekierowuje użytkownika do głównego panelu zarządzającego kontem i wyświetlana informacja o stanie konta. Po poprawnej aktywacji konta użytkownik otrzymuje możliwość rejestracji certyfikatów systemu P1, których przekazanie jest wymagane w przypadku chęci skorzystania z funkcjonalności indeksowania

dokumentów. W przypadku otrzymania nowych certyfikatów dla wykorzystywanego konta, gdy np. poprzednie straciły ważność lub zostały odwołane użytkownik musi przeprowadzić ich aktualizację po stronie aplikacji mMedica. Wykorzystać w tym celu należy funkcjonalność umieszczoną pod przyciskiem „Aktualizuj certyfikaty”.

Zarządzanie kontem dla eRepozytorium w chmurze

ID konta: 0000000000005010 Aktywowane

ID domeny: 1.3.6.1.4.1.31367.1.2.20210609.83245.589.5010.16

ID repozytorium: 1.3.6.1.4.1.31367.1.4.20210609.83245.589.5010.9

ID repozytorium w P1:

Dane konta

Aktywne od 2021-06-08 do 2022-06-08
Wielkość konta 20010 MB, wykorzystano 22 MB
Maksymalna liczba plików 10000, zdeponowano 20 dokumentów

Certyfikat WSSE

Numer seryjny: 2E79A132A405EBA40EE3D94AF829F81940DA5B2A
Okres ważności: 2021-06-09 08:07:21 - 2022-06-08 15:00:00

Certyfikat TLS

Numer seryjny: 3B331BE44A2162BC61BF722119924B1FE159BD9A
Okres ważności: 2021-06-09 08:07:15 - 2022-06-08 15:00:00

Rejestruj certyfikaty P1 Aktualizuj certyfikaty Wyjście

1.1.2 Konfiguracja modułu od wersji 9.10.0 aplikacji mMedica.

Pierwszym etapem konfiguracji jest wprowadzenie identyfikatora konta oraz wygenerowanie kluczy prywatnych służących do komunikacji z zasobem chmurowym. W tym celu należy przejść do ścieżki: [Zarządzanie > Konfiguracja > Konfigurator](#), obszar [Funkcje dodatkowe > Zarządzanie kontem Chmury dla zdrowia](#) i wybrać przycisk „Generuj CSR”.

Generacja certyfikatów Chmury dla zdrowia

ID konta (CN): 0000000000001003

Organizacja (O): Asseco Poland S.A.
Jednostka organizacyjna (OU): Przychodnia
Kraj (C): Polska

Generuj Wyjście

W polu „ID Konta (CN) ” należy wprowadzić identyfikator konta w chmurze otrzymany w procesie zamawiania produktu w „chmuradlazdrowia.pl”. Wartości dla obszarów:

- Organizacja (O)
- Jednostka organizacyjna (OU)
- Kraj (C)

zostaną pobrane automatycznie ze „Struktury Organizacyjnej” podmiotu. Wybranie przycisku „Generuj”, uruchamia proces wytworzenia plików „csr” i przekazania ich na adres „biuro@chmuradlzdrowia.pl”. Na wymieniony adres mailowy zostaje wysłana wiadomość o treści:

(...)

Witam,

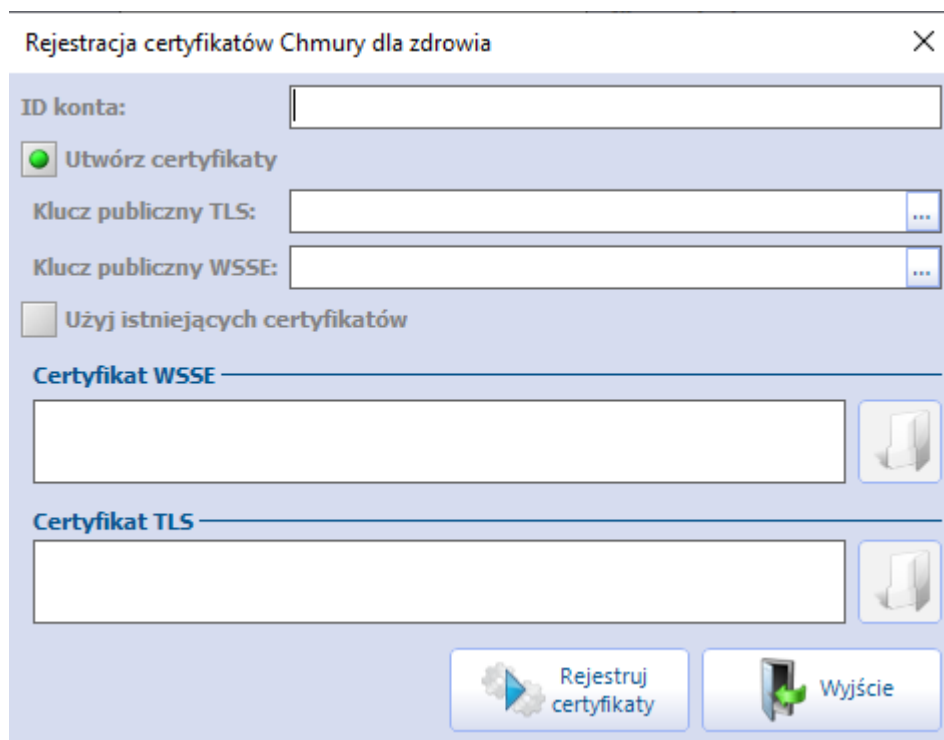
przekazano żądanie wydania certyfikatu (CSR) dla konta tenanta 0000000000001003.

Wiadomości ta została wygenerowana automatycznie.

Pozdrawiamy zespół mMedica.

(...)

W odpowiedzi na powyższego maila zwrotnie zostaną Państwu przekazane klucze publiczne, które posłużą Państwu do aktywacji konta. Aktywację konta w innej lokalizacji w ramach tego samego konta należy przeprowadzić z wykorzystaniem certyfikatów *.p12. W celu aktywacji konta należy przejść do ścieżki: [Zarządzanie > Konfiguracja > Konfigurator](#), obszar [Funkcje dodatkowe> Zarządzanie kontem Chmury dla zdrowia](#) i wybrać przycisk „Rejestruj certyfikaty”.



W polu „ID Konta” należy wprowadzić identyfikator konta w chmurze otrzymany w procesie zamawiania produktu w „chmuradlzdrowia.pl”.

1. Wybierając „Utwórz certyfikaty” należy w polach:

- a) Klucz publiczny TLS
- b) Klucz prywatny TLS

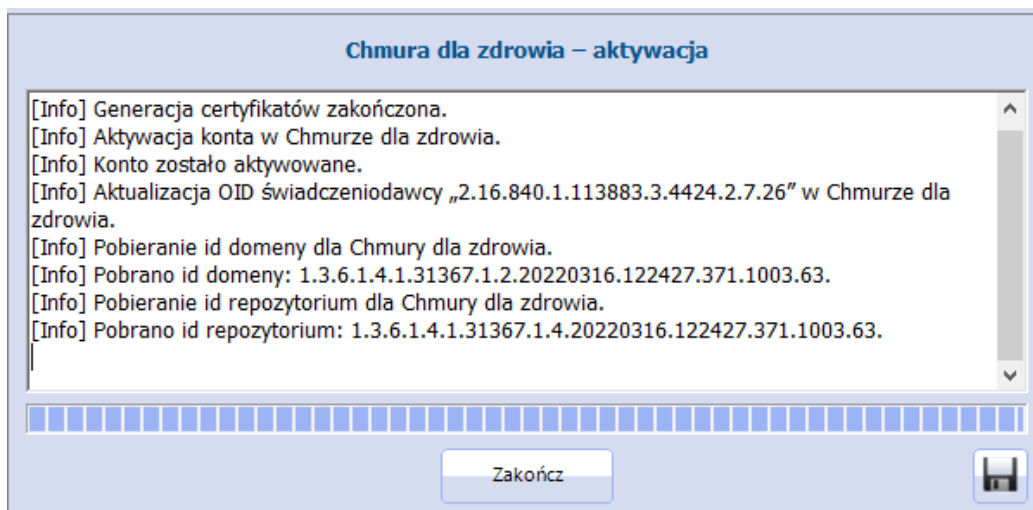
wskazać klucze publiczne przekazane przez Biuro Obsługi Klienta sklepu „chmuradlzdrowia.pl”. Pliki te posiadają rozszerzenie *.pem.

2. Wybierając „Użyj istniejących certyfikatów” należy w polach:

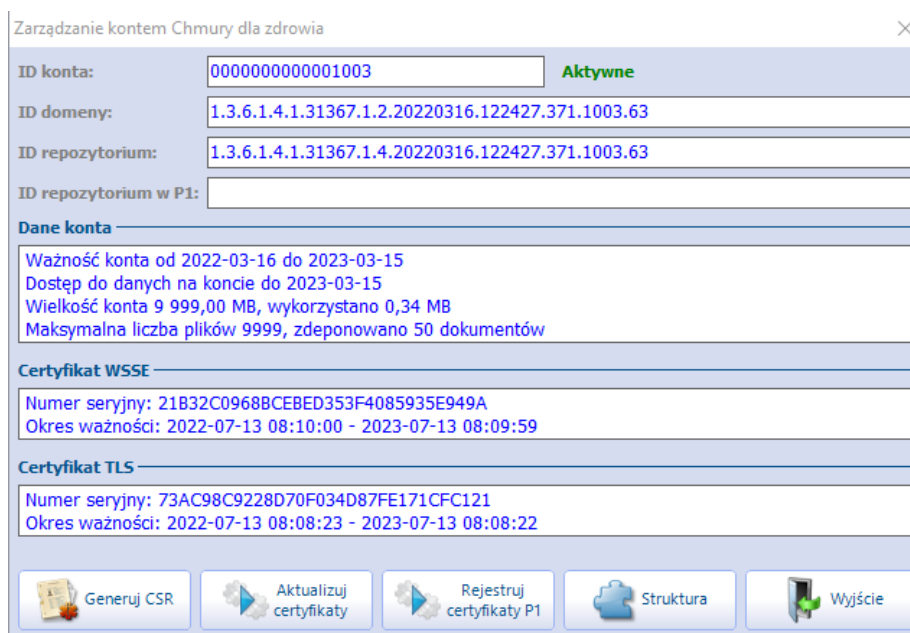
- a) Certyfikat WSSE
- b) Certyfikat TLS

wskazać certyfikaty *.p12 wygenerowane wg wytycznych w punkcie 1.1.6.

Wybranie przycisku „Rejestruj certyfikaty” uruchamia proces aktywacji konta w chmurze, w wyniku którego zostaną przekazane identyfikatory techniczne konta. Przykładowe komunikaty zwrócone w procesie rejestracji przedstawiono poniżej:



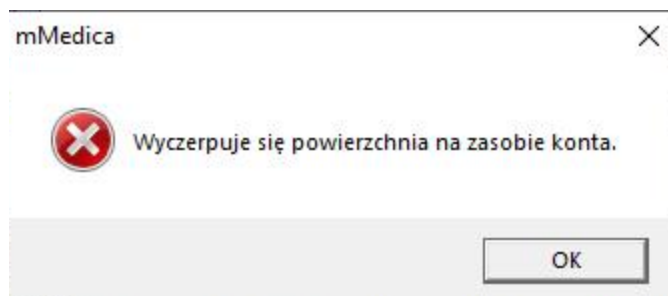
Wybranie przycisku „Zakończ” przekierowuje użytkownika do głównego panelu zarządzającego kontem i wyświetlana informacja o stanie konta. Po poprawnej aktywacji konta użytkownik otrzymuje możliwość rejestracji certyfikatów systemu P1, których przekazanie jest wymagane w przypadku chęci skorzystania z funkcjonalności indeksowania dokumentów. W przypadku otrzymania nowych certyfikatów dla wykorzystywanego konta, gdy np. poprzednie straciły ważność lub zostały odwołane użytkownik musi przeprowadzić ich aktualizację po stronie aplikacji mMedica. Wykorzystać w tym celu należy funkcjonalność umieszczoną pod przyciskiem „Aktualizuj certyfikaty”.



Poprawna aktywacja konta umożliwia jego monitorowanie z poziomu aplikacji mMedica. W obszarze „Dane konta” zostały umieszczone kluczowe dla klienta informacje, do których należą:

- ważność konta
- wielkość konta oraz stan jego wykorzystania
- maksymalna ilość dokumentów możliwych do zdeponowania oraz aktualna ilość dokumentów zdeponowanych

W przypadku, gdy dostępny dla konta limit osiągnie granicę 90% zasobu, użytkownikowi końcowemu zostanie wyświetlony komunikat ostrzegawczy. Treść komunikatu została przedstawiona poniżej.



1.1.3 Aktualizacja certyfikatów dla konta tenanta od wersji 8.2.1 aplikacji mMedica.

W celu aktualizacji certyfikatów dla konta tenanta należy ponownie przejść ścieżkę generacji plików CSR. Po otrzymaniu kluczy publicznych należy zaczytać je w obszarze: [Zarządzanie > Konfiguracja > Konfigurator](#), obszar [Funkcje dodatkowe > Zarządzanie kontem Chmury dla zdrowia](#) i wybrać przycisk „Aktualizuj certyfikaty”.

1.1.4 Przekazanie danych o „Strukturze Organizacyjnej” podmiotu.

Aplikacja mMedica posiada możliwość przekazania informacji o „Strukturze Organizacyjnej” podmiotu do zasobu w chmurze. W celu przekazania danych o strukturze należy w obszarze: [Zarządzanie > Konfiguracja > Konfigurator](#), obszar [Funkcje dodatkowe > Zarządzanie kontem Chmury dla zdrowia](#) i wybrać przycisk „Struktura”, a następnie przycisk „Wyslij”

Struktura organizacyjna przekazana do Chmury dla zdrowia

Świadczeniodawca

Asseco Poland S.A.
08-110 Siedlce, ul. ul. Jana Kilińskiego 29
tel.: 178885550
REGON: 010334578, NIP: 5220003782
Kod res. cz. I: 000000025677

Zakład leczniczy

Przychodnia (Asseco Poland S.A.)
00-184 Warszawa, ul. ul. Dubois 5A
tel.: 178885550
REGON: 01033457800005
NIP: 5220003782

Komórki organizacyjne

Kod	Nazwa	Kod. res. V	Kod. res. VII	Kod. res. VIII	Kod. res. IX	Kod. res. X	Telefon	E-mail
01	Przychodnia	01	001	1810	HC.1.1	115	178885550	

Wyślij Wyjście

1.1.5 Rodzaje archiwizowanych dokumentów.

Ścieżka: [Moduły dodatkowe > Archiwum dokumentów > Rodzaje dokumentów](#)

Kolejnym krokiem jest określenie rodzajów dokumentów, które będą przekazywane z bazy mMedica do zewnętrznego „eRepozytorium mMedica w chmurze”.

Po przejściu do powyższej ścieżki, w górnym oknie *Rodzaje dokumentów* prezentowane są rodzaje dokumentów, które mogą być przekazywane z programu do zewnętrznego repozytorium. Przykładowe dokumenty wymienione poniżej:

- **Dokument własny pacjenta** - dokument udostępniony lekarzowi przez pacjenta za pomocą aplikacji mobilnej Informacje Medyczne. Wymaga posiadania Modułu Integracji Aplikacji Mobilnych.
- **Wynik badania laboratoryjnego PIK HL7 CDA** - dotyczy wyników badań przekazywanych przez zintegrowane laboratorium. Wymaga posiadania modułu eWyniki Lab.
- **Wynik badania diagnostycznego PIK HL7 CDA** - dotyczy wyników badań przekazywanych przez zintegrowaną pracownię diagnostyczną. Wymaga posiadania modułu eWyniki Diag.
- **Załącznik** - Wszelkie dokumenty umieszczone w danych pacjenta lub dołączone do wizyty w formie załączników (zdjęcia, zeskanowane pliki itd.).
- **Udostępniona dokumentacja medyczna** - dokumentacja medyczna pacjenta udostępniona z poziomu: [EDM > Udostępnianie > Zapisz dokumentację jako XML HL7 CDA](#). Wymaga posiadania modułu EDM.
- **Recepta** - dokument e-Recepty wystawionej pacjentowi.
- **Karta informacyjna leczenia szpitalnego** - dokument tworzony na etapie wypisu pacjenta z realizowanej hospitalizacji. Wymaga posiadania modułu Hospitalizacje.
- **Informacja dla lekarza kierującego** - dokument wystawiony pacjentowi na wizycie realizowanej w Gabiniecie.
- **Dokument anulujący** - dokument potwierdzający anulowanie e-Recepty. Powstaje automatycznie na skutek usunięcia wcześniej utworzonego dokumentu recepty elektronicznej.
- **Skierowanie do specjalisty** - dokument e-Skierowania wystawiony pacjentowi
- **Skierowanie do szpitala** - dokument e-Skierowania wystawiony pacjentowi
- **Skierowanie na badanie diagnostyczne** - dokument e-Skierowania wystawiony pacjentowi
- **Skierowanie na badanie diagnostyczne wysłane do P1** - dokument e-Skierowania pobrany dla pacjenta z systemu P1
- **Karta odmowy przyjęcia do szpitala** – dokument pobrany dla pacjenta z systemu P1

Dla rodzajów dokumentów:

- e-Recepta
- e-Skierowanie do specjalisty
- e-Skierowanie do szpitala
- e-Skierowanie na badanie diagnostyczne podlegające wysyłce do P1.

użytkownik definiuje, czy ma on być przekazywany do zewnętrznego repozytorium i jak długo będzie dostępny w lokalnej bazie danych. Służą do tego następujące parametry:

- **Czy zapisywać dokument automatycznie w archiwum** – określa czy dokument ma zostać przeniesionych do zewnętrznego repozytorium(domyślnie zaznaczony)
- **Dostępny lokalnie przez (dni)** - określenie okresu wyrażonego w dniach, po upływie którego dokumenty z bazy lokalnej mMedica zostaną przekazane do archiwum zewnętrznego.

ZBD	Skierowanie na badania diagnostyczne wysłane do P1
KIF	Karta informacyjna leczenia szpitalnego
ILK	Informacja dla lekarza kierującego
ZPS	Wynik weryfikacji zlecenia na zaopatrzenie w wyroby medyczne
ZPA	Anulowanie zlecenia na zaopatrzenie w wyroby medyczne
ZPO	Zlecenie na zaopatrzenie w wyroby medyczne

[KIF] Karta informacyjna leczenia szpitalnego

Rodzaj:

Nazwa:

Czy zapisywać dokument automatycznie w archiwum ☒

Dostępny lokalnie przez (dni):

Od wersji 7.2.0 dla parametru „**Czy zapisywać dokument automatycznie w archiwum**” zostało wprowadzone usprawnienie, jeśli dany rodzaj dokumentu, został wytworzony, a pole jest odznaczone (puste), to nie zostanie on przeniesiony do zewnętrznego repozytorium. W procesie aktualizacji do wersji 7.2.0 automatycznie zostaną odznaczone typy dokumentów HL7 CDA PIK:

- a) e-Recepta
- b) e-Skierowanie do specjalisty
- c) e-Skierowanie do szpitala
- d) e-Skierowanie na badanie diagnostyczne podlegające wysyłce do P1.

Pozostałe typy dokumentów, które są wytwarzane w podmiocie leczniczym jako dokumenty PIK HL7 CDA lub zostały pobrane z zewnętrznych repozytoriów innych świadczeniodawców będą przenoszone do zewnętrznego repozytorium.

Aby poprawnie zdeponować dokument w zewnętrznym repozytorium w aplikacji mMedica muszą być uzupełnione:

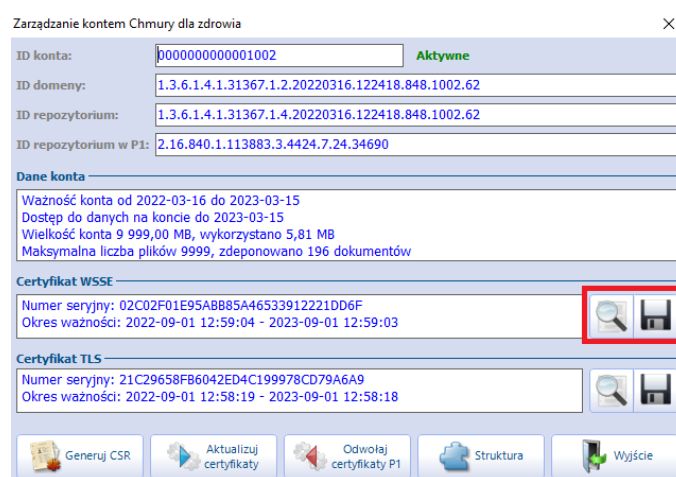
- a) Kody resortowe cz. I, V, VII, VIII oraz X w danych podmiotu i komórek organizacyjnych
- b) Domyślny użytkownik archiwizacji dokumentu dla zadania „Archiwizacja dokumentów” (Zarządzanie-> Operacje techniczne -> Harmonogram zadań)

Uwaga! Należy pamiętać, iż otwarcie dokumentów przechowywanych w archiwum może trwać dłużej, niż w przypadku dokumentów znajdujących w lokalnej bazie danych. Wpływ na to ma szybkość wykorzystywanego łącza oraz serwera, na którym zainstalowano archiwum.

1.1.6 Zapis certyfikatów komunikacyjnych TLS/WSSE na dysk.

Od wersji 8.3.1 w obszarze „Zarządzenie kontem Chmury dla zdrowia” dodano możliwość:

- a) Zapisu certyfikatu w formie pliku *.p12 na dysk
- b) Skopiowania hasła certyfikatu do schowka systemowego



Certyfikaty TLS/WSS służą do połączenia się z panelami zarządzającymi takimi zasobami jak:

- a) Panel administracyjny konta tenanta
- b) Portal eAnkiety

Powyższe zasoby dostępne są pod adresami:

- a) Panel administracyjny konta tenanta

https://konto.chmuradlazdrowia.pl/services/id_konta/app

b) Portal eAnkiety

https://konto.chmuradlzdrowia.pl/services/id_konta/e-survey-gui/#/login

Aby poprawnie uruchomić ekrany logowania należy:

1. Zacytować certyfikat TLS w przeglądarce wykorzystywanej do połączenia z powyższymi paneli.
2. **Zmodyfikować powyższy link** i w miejsce „id konta” **wpisać właściwy numer tenanta**, otrzymany po zakupie usługi w BOK
3. Pierwsze logowanie do powyższych aplikacji należy przeprowadzić za pomocą konta administracyjnego, utworzonego w systemie mMedica.

1.2. Przegląd dokumentów.

Ścieżka: [Moduły dodatkowe](#) > [Archiwum dokumentów](#) > [Przegląd archiwum](#)

Na formatce *Przegląd archiwum dokumentów* prezentowana jest lista wszystkich dokumentów, które zostały przekazane z bazy mMedica do „eRepozytorium mMedica w chmurze”. Z tego poziomu można wyszukać wszystkie dokumenty, jakie zostały wystawione wybranemu pacjentowi w określonym czasie, do czego służą filtry w panelu *Wyszukiwanie zaawansowane*. Można również wykonywać pozostałe operacje na dokumentach - podglądać je, zapisywać w formie dokumentów XML HL7 CDA lub zapisywać załączniki.

Opis przycisków znajdujących się w górnej części okna:

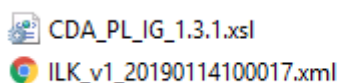
- **Udostępnij** - przekazuje wybrany dokument do „eRepozytorium mMedica w chmurze” wraz ze zgodą na jego udostępnienie poprzez Portal eRejestracji podmiotu medycznego. Poprawnie przekazany dokument zostanie

oznaczony w kolumnach „eRepozytorium”, Wystawiono zgodę: nast. znacznikiem . Z kolei pacjent w celu odebrania dokumentu powinien zalogować się do Portalu eRejestracji podmiotu na swoje konto.

- **Zapisz XML HL7 CDA** - zapisuje na dysku komputera wybrany dokument w formacie XML HL7 CDA.
- **Pokaż w przeglądarce** - otwiera w przeglądarce wybrany dokument w celu jego podglądu. W zależności od rodzaju dokumentu, podgląd zostanie otwarty w domyślnej przeglądarce internetowej lub programie do wyświetlania plików graficznych.
- **Zapisz załącznik** - zapisuje wybrany załącznik na dysku komputera. Przycisk aktywny wyłącznie dla rodzaju dokumentu „Udostępniona dokumentacja medyczna”.
- **Indeksuj dokument** – przekazuje indeks dokumentu do systemu P1.

Utworzone dokumenty elektroniczne w formacie HL7 CDA można zapisać i udostępnić pacjentowi. W tym celu należy zaznaczyć na liście właściwy dokument i wybrać przycisk **Zapisz XML HL7CDA**. We wskazanym przez użytkownika miejscu zapisu dokumentu, zostaną zapisane co najmniej dwa pliki:

- plik z rozszerzeniem .XSL - transformata generująca warstwę prezentacyjną dokumentów medycznych,
- plik z rozszerzeniem .XML - dokument medyczny w formie elektronicznej.

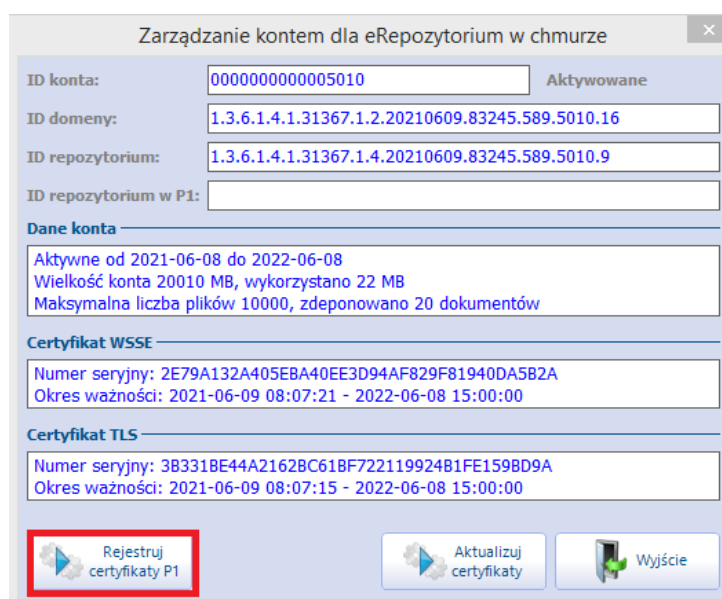


Z kolei wizualizacja elektronicznego dokumentu medycznego następuje poprzez wyświetlenie go w postaci strony HTML. Aby podejrzeć wygenerowany dokument, należy wybrać przycisk **Pokaż w przeglądarce**.

1.3. Rejestracja „eRepozytorium w Chmurze” w domenie krajowej (System P1).

Ścieżka: [Zarządzanie](#) > [Konfiguracja](#) > [Konfigurator](#), obszar: [Funkcje dodatkowe](#)> [Zarządzanie kontem dla eRepozytorium w chmurze](#)

W celu pozyskania możliwości indeksowania dokumentów w systemie P1, użytkownik musi przeprowadzić rejestrację posiadanego przez siebie repozytorium w domenie krajowej. Aby tego dokonać musi przekazać do zasobu w chmurze certyfikaty, które aktualnie są wykorzystywane przez podmiot do wystawiania takich dokumentów jak e-Recepta, czy też e-Skierowanie. Przekazanie certyfikatów realizowane jest przez przycisk „Rejestruj certyfikaty P1”. Proces instalacji certyfikatów dla obszaru P1 został zamieszczony w „[Instrukcja obsługi programu mMedica](#)” w rozdziale 7.2.1.



Poprawne przekazanie certyfikatów z zakresu P1 do zasobu chmurowego uruchomi proces rejestracji repozytorium w dokumencie krajowej.

Zarządzanie kontem dla eRepozytorium w chmurze

ID konta: 0000000000005010 Aktywowane

ID domeny: 1.3.6.1.4.1.31367.1.2.20210609.83245.589.5010.16

ID repozytorium: 1.3.6.1.4.1.31367.1.4.20210609.83245.589.5010.9

ID repozytorium w P1:

Dane konta

Aktywne od 2021-06-09 08:07:15
Wielkość konta 20010 MB, wykorzystano 22 MB
Maksymalna liczba plików 10000, zdeponowano 20 dokumentów

Certyfikat WSSE

Numer seryjny: 2E79A132A405EBA40EE3D94AF829F81940DA5B2A
Okres ważności: 2021-06-09 08:07:21 - 2022-06-08 15:00:00

Certyfikat TLS

Numer seryjny: 3B331BE44A2162BC61BF722119924B1FE159BD9A
Okres ważności: 2021-06-09 08:07:15 - 2022-06-08 15:00:00

Rejestruj certyfikaty P1 Aktualizuj certyfikaty Wyjście

Zarządzanie kontem dla eRepozytorium w chmurze

ID konta: 0000000000005010 Aktywowane

ID domeny: 1.3.6.1.4.1.31367.1.2.20210609.83245.589.5010.16

ID repozytorium: 1.3.6.1.4.1.31367.1.4.20210609.83245.589.5010.9

ID repozytorium w P1: 2.16.840.1.113883.3.4424.7.24.8879

Dane konta

Aktywne od 2021-06-08 do 2022-06-08
Wielkość konta 20010 MB, wykorzystano 22 MB
Maksymalna liczba plików 10000, zdeponowano 20 dokumentów

Certyfikat WSSE

Numer seryjny: 2E79A132A405EBA40EE3D94AF829F81940DA5B2A
Okres ważności: 2021-06-09 08:07:21 - 2022-06-08 15:00:00

Certyfikat TLS

Numer seryjny: 3B331BE44A2162BC61BF722119924B1FE159BD9A
Okres ważności: 2021-06-09 08:07:15 - 2022-06-08 15:00:00

Odwolaj certyfikaty P1 Aktualizuj certyfikaty Wyjście

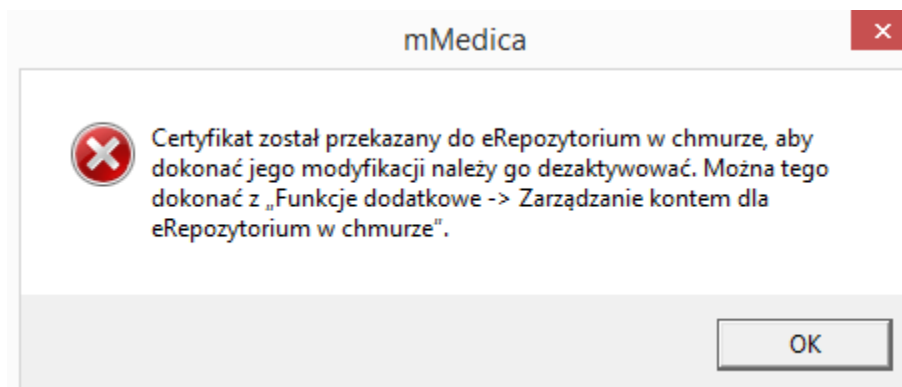
Przekazany przez system P1 identyfikator repozytorium zostanie wykorzystany w procesie indeksowania dokumentów.

W przypadku otrzymania nowych certyfikatów dla obszaru P1, gdy np. poprzednie straciły ważność lub zostały odwołane użytkownik musi przeprowadzić ich aktualizację po stronie aplikacji mMedica. W celu aktualizacji certyfikatów dla obszaru P1 należy:

1. Przejść w [Zarządzanie > Konfiguracja > Konfigurator](#), obszar: [Funkcje dodatkowe> Zarządzanie kontem dla eRepozytorium w chmurze](#)
2. Wybrać dostępny na formatce przycisk „Odwolaj Certyfikaty P1”
3. Przejść w [Zarządzanie > Konfiguracja > Konfigurator](#) obszar: [System>Autoryzacja](#)

Należy dokonać zaczytania certyfikatów WSSE oraz TLS otrzymanych z CSIOZ na potrzeby komunikacji. W sekcji Certyfikat P1 WSSE należy wybrać przycisk **Wczytaj...** i w otwartym oknie **Wybierz załącznik** wskazać certyfikat WSSE, który został zapisany na dysku komputera lub nośniku danych. Następnie zostanie otwarte okno dialogowe **Podaj hasło do certyfikatu**, w którym należy wpisać otrzymane hasło do certyfikatu i zatwierdzić zmiany. Po poprawnym zaczytaniu certyfikatu do systemu, w oknie „Certyfikat...” zostanie wyświetlony jego numer seryjny oraz okres ważności. Analogicznie należy zaczytać certyfikat TLS.

W przypadku nie odwołania certyfikatów w „eRepozytorium mMedica w chmurze” dla próby aktualizacji certyfikatów z obszaru P1 zostanie wyświetlony komunikat o treści zamieszczonej poniżej.



1.4. Rejestr zgód.

Ścieżka: [Zarządzanie](#) > [Ochrona danych osobowych](#) > [Rejestr zgód dla eRepozytorium w chmurze](#)

W celu udostępnienia za pośrednictwem portalu eRejestracja dokumentu przekazanego do „eRepozytorium mMedica w chmurze”, użytkownik mMedica musi wprowadzić do systemu „zgode”, w ramach której określa:

- Zakres czasowy w którym dokument ma być widoczny w Portalu eRejestracja. Pola „Data od”, „Data do”
- Pacjenta, dla którego został wytworzony udostępniany dokument
- Odbiorcę dokumentu
- Przyczynę potrzeby udostępnienia dokumentu. Pole „Sprawa”

A screenshot of a web form titled "Zgoda na udostępnienie dokumentów w eRepozytorium w chmurze". The form includes fields for "Data od:" (set to 2021-06-16), "Data do:", "Pacjent:" (set to Senior Sylwester), "Odbiorca:", and "Sprawa:". Below these is a section titled "Udostępnione dokumenty" containing a table with columns: "Identyfikator dokumentu", "Nazwa dokumentu", "Data wystawienia", and "Wysłano". The table is currently empty. At the bottom right are two buttons: "Wyślij" (with a green checkmark icon) and "Wyjdź" (with a green exit icon).

Poprzez  przycisk użytkownik aplikacji określa które dokumenty pacjenta mają zostać udostępnione poprzez Portal eRejestracji.

Zgoda na udostępnienie dokumentów w eRepozytorium w chmurze

Data od: 2021-06-16 Data do:

Pacjent: Senior Sylwester Odbiorca:

Sprawa:

Udostępnione dokumenty

*	Identyfikator dokumentu	Nazwa dokumentu	Data wystawienia	Wysłano
	2.16.840.1.113883.3.4424.2.7.26.7.1^0...	Informacja dla lekarza kierując...	2021-06-15 08:41	
▶	2.16.840.1.113883.3.4424.2.7.26.7....	Informacja dla lekarza kieru...	2021-06-15 08:46	

 Wyślij  Wyjście

Wybranie przycisku „Wyślij” uruchamia proces udostępniania.

W celu odwołania zgody użytkownik musi skorzystać z przycisku „Odwołanie zgody” znajdującego się w górny menu.

 Rejestr zgód dla eRepozytorium w chmurze

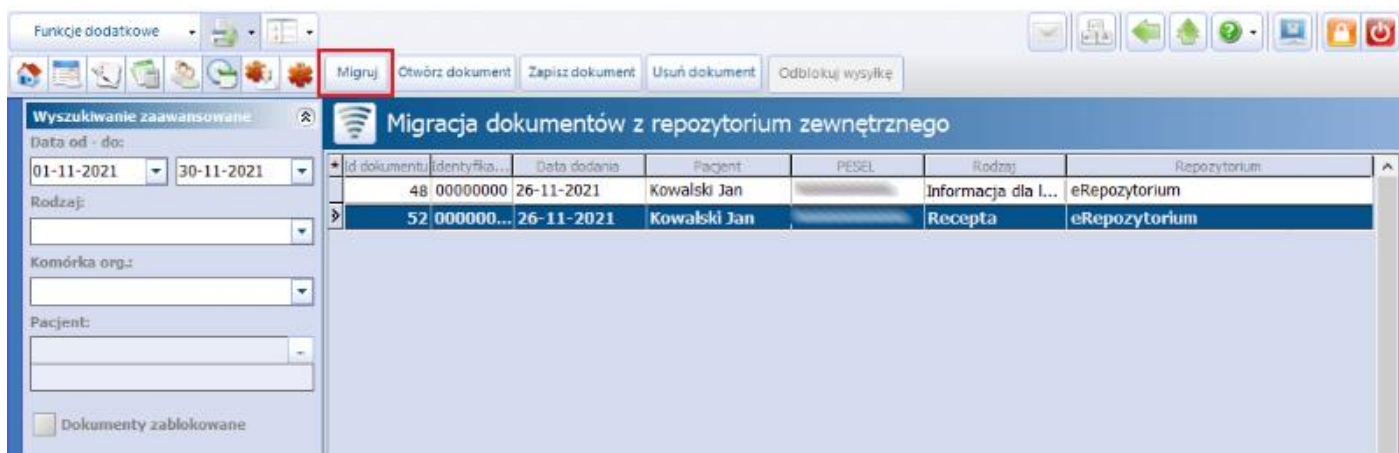
1.5. Migracja dokumentów z repozytorium zewnętrznego.

Ścieżka: Moduły dodatkowe > Archiwum dokumentów > Migracja dokumentów z repozytorium zewnętrznego

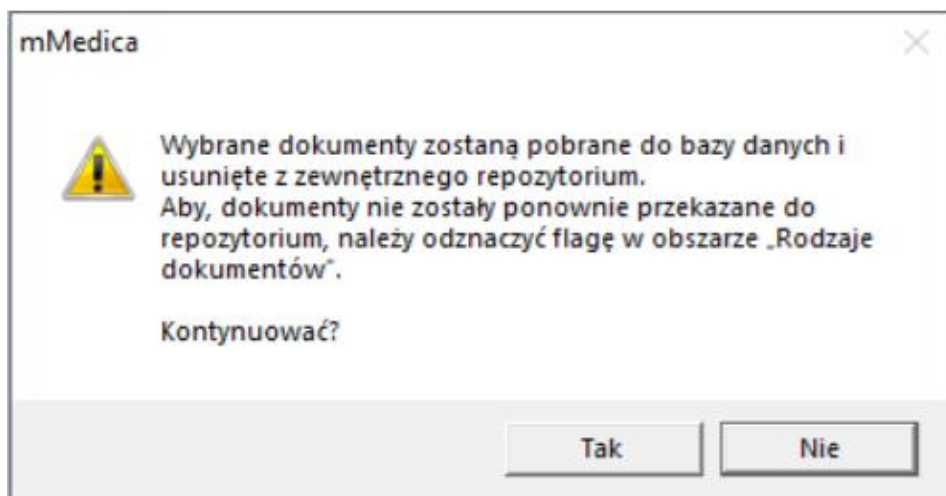
W aplikacji mMedica dostępna jest funkcjonalność migracji dokumentów z posiadanego przez świadczeniodawcę repozytorium zewnętrznego (eArchiwum/eRepozytorium w Chmurze) do bazy lokalne jmMedica, z równoczesnym usunięciem ich z bazy zewnętrznego repozytorium.

Uwaga! Aby omawiana funkcjonalność była dostępna dla użytkownika, musi on w swoich danych, w ścieżce: Zarządzanie > Konfiguracja > Użytkownicy systemu, na zakładce 5. Uprawnienia funkcjonalne, w gałęzi: Administracja systemem, mieć zaznaczone uprawnienie: "Migracja dokumentów z repozytoriów zewnętrznych".

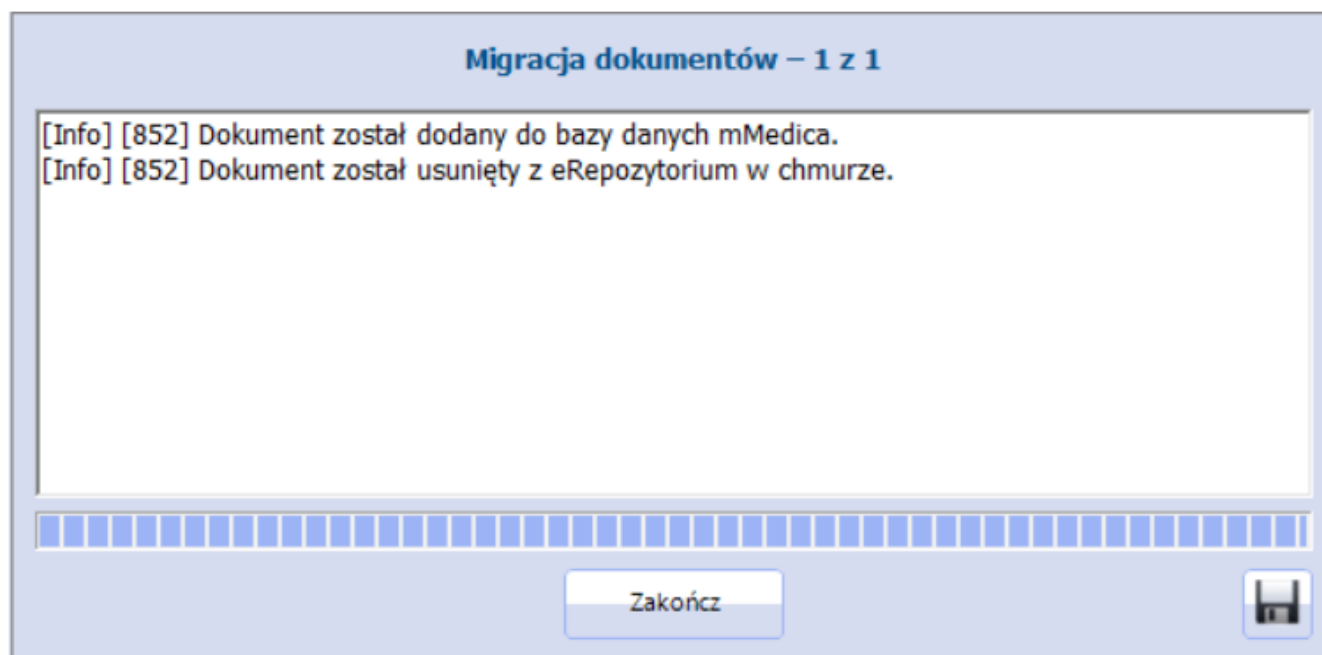
W oknie Migracja dokumentów z repozytorium zewnętrznego, dostępnym w ścieżce: Moduły dodatkowe > Archiwum dokumentów > Migracja dokumentów z repozytorium zewnętrznego, wyświetlana jest lista dokumentów przesłanych do eArchiwum lub eRepozytorium w Chmurze (w zależności od rodzaju repozytorium, z którego świadczeniodawca korzysta).



W celu migracji dokumentów należy je zaznaczyć na liście, a następnie wybrać przycisk Migruj, znajdujący się u góry ekranu. Po tej czynności pojawi się komunikat:



Po wyborze przycisku **Tak** rozpocznie się operacja przeniesienia wskazanych dokumentów do bazy mMedica i ich usunięcia z bazy repozytorium zewnętrznego. Wyświetli się także okno z komunikatami informującymi o jej przebiegu (patrz przykład poniżej).



Uwaga! Aby dokumenty danego rodzaju nie były przekazywane do eArchiwum/eRepozytorium w Chmurze, należy dla tego rodzaju wyłączyć parametr **"Przenieś dokument automatycznie do repozytorium zewnętrznego"**. Dokładne informacje na ten temat zawiera rozdział [Rodzaje archiwizowanych dokumentów](#).

Uwaga! Domyślnie [zadanie automatycznego przesyłania dokumentów do repozytorium zewnętrznego](#) pomija wszystkie dokumenty, które z tego repozytorium zostały zmigrowane. Aby przywrócić automatyczne przesyłanie takich dokumentów, należy je wyświetlić na liście, poprzez zaznaczenie w panelu Wyszukiwanie zaawansowane pola "Dokumenty zablokowane" (powoduje wyświetlenie tylko pozycji zmigrowanych, które są zablokowane do wysyłki przez mmService), a następnie dla odpowiednich pozycji skorzystać z przycisku **Odblokuj wysyłkę**. [Wspomniana funkcjonalność została udostępniona w wersji 8.3.0 aplikacji mMedica](#). W wersji tej został dodany przycisk **Odblokuj wysyłkę** oraz pole "Dokumenty zablokowane".

W oknie Migracja dokumentów z repozytorium zewnętrznego istnieje dodatkowo możliwość podglądu oraz zapisu na dysku komputera zaznaczonych dokumentów. Służą do tego przyciski **Otwórz dokument** i **Zapisz dokument**, zamieszczone obok przycisku migracji.

Przycisk **Usuń dokument** służy do usuwania dokumentów z repozytorium zewnętrznego. Funkcjonalność działa tylko dla dokumentów w rodzaju:

- Recepta
- Skierowanie do specjalisty
- Skierowanie do szpitala
- Skierowanie na badania diagnostyczne wysłane do P1
- Skierowanie na rehabilitację

W celu usunięcia dokumentów, należących do powyższego zakresu, należy zaznaczyć odpowiednie pozycje na liście, a następnie skorzystać ze wspomnianego przycisku.

[W wersji 8.2.0 aplikacji mMedica](#) umożliwiono korzystanie z funkcjonalności migracji dokumentów z repozytorium zewnętrznego również w przypadku braku aktywnej licencji na "Moduł eArchiwum" lub "Moduł Integracji eRepozytorium w Chmurze".

2. Rozwiązania częstych problemów.

2.1 Nie udało się pobrać id repozytorium z domeny krajowej.

Należy przeprowadzić operację ponownego przekazania do usługi „eRepozytorium mMedica w chmurze” certyfikaty TLS i WSSE dla systemu P1. W tym celu należy wykonać następujące operacje:

1. Przejść do obszaru: [Zarządzanie > Konfiguracja > Konfigurator](#),
2. Wybrać [Funkcje dodatkowe > Zarządzanie kontem dla eRepozytorium w chmurze](#),

3. W oknie „Zarządzanie kontem dla eRepozytorium w chmurze” wybrać przycisk „Odwołaj certyfikaty P1”,

The screenshot shows a web application window titled "Zarządzanie kontem dla eRepozytorium w chmurze". It contains several input fields for account and repository information, including ID konta, ID domeny, ID repozytorium, and ID repozytorium w P1. Below these are sections for "Dane konta" (account details), "Certyfikat WSSE" (WSSE certificate), and "Certyfikat TLS" (TLS certificate), each displaying a serial number and validity period. At the bottom, there are three buttons: "Odwołaj certyfikaty P1" (highlighted with a red rectangle), "Aktualizuj certyfikaty", and "Wyjście".

4. W oknie „Zarządzanie kontem dla eRepozytorium w chmurze” wybrać przycisk „Rejestruj certyfikaty P1”

This screenshot shows the same web application window as the previous one, but with different data values. The "Odwołaj certyfikaty P1" button is no longer highlighted. Instead, the "Rejestruj certyfikaty P1" button at the bottom left is highlighted with a red rectangle. The other fields and sections remain the same.

2.2 Limit czasu operacji został przekroczony.

Należy przeprowadzić operację zwiększenia czasu oczekiwania na odpowiedź z systemu zewnętrznego. W tym celu należy wykonać następujące operacje:

1. Przejść do obszaru: [Zarządzanie](#) > [Konfiguracja](#) > [Konfigurator](#),

2. Wybrać **Komunikacja > Inne**,

3. W polu Timeout wpisać wartość określającą czas oczekiwania na odpowiedź z systemu zewnętrznego np. 15000

2.3 Wystąpił błąd „Bad Request (400)”.

Należy przeprowadzić weryfikację poprawności przekazanych certyfikatów w kontekście konta tenanta w ramach którego mają być wykorzystane. Weryfikację certyfikatu można przeprowadzić poprzez polecenie certutil.

Czynności jakie należy wykonać to:

1. Uruchomić wiersz poleceń "CMD" w katalogu w których znajdują się zaczytywane do bazy certyfiakty TLS i WSSE dla usługi „eRepozytorium mMedica w chmurze”
2. W wierszu poleceń wpisać polecenie: certutil "nazwa pliku certyfikatu.pem".
3. W wyświetlonym oknie należy skoncentrować się na sekcji „Subject”, która powinna zawierać pole „CN” o

składni:

CN="nr konta tenanta" „rodzaj certyfikatu” ,

gdzie:

- nr konta tenanta – identyfikator konta w chmurze, przekazany w procesie zamawiania usługi
- rodzaj certyfikatu – określa rodzaj weryfikowanego certyfikatu, może przyjmować jedną z dwóch wartości:

- a) TLS
- b) WSS

Nazwy plików certyfikatów przyjmują postać:

- a) TLSnumerseryjny.pem dla certyfikatu w rodzaju TLS
- b) WSSnumerseryjny.pem dla certyfikatu w rodzaju TLS

Przykładowe wartości po wykonaniu polecenia „certutil” zostały przedstawione na poniższych screenach:

1. Certyfikat w rodzaju TLS:

```
Issuer:
  CN=Certum Enterprise Subordinate CA
  O=Asseco Data Systems S.A.
  C=PL
  Name Hash(sha1): 6d337b9df3ee5cbe02cd3bf30e1c443158b5ca2b
  Name Hash(md5): 32a3102745c7bf572a05a09ece2bb162

NotBefore: 2021-06-18 15:29
NotAfter: 2022-06-18 15:29

Subject:
  CN=00000000000000005 TLS
  O=Asseco Poland S.A.
  OU=mMedica
  C=PL
  Name Hash(sha1): 216ab7ce90b004a61372b609fc0baa8be7cb3507
  Name Hash(md5): c75b7394e39ffcc124c116b69f581648
```

2. Certyfikat w rodzaju WSS:

```
Issuer:
  CN=Certum Enterprise Subordinate CA
  O=Asseco Data Systems S.A.
  C=PL
  Name Hash(sha1): 6d337b9df3ee5cbe02cd3bf30e1c443158b5ca2b
  Name Hash(md5): 32a3102745c7bf572a05a09ece2bb162

NotBefore: 2021-06-18 15:30
NotAfter: 2022-06-18 15:30

Subject:
  CN=00000000000000005 WSS
  O=Asseco Poland S.A.
  OU=mMedica
  C=PL
  Name Hash(sha1): 77173ce3a063378b8bd5ba16292405a0b100ea2f
  Name Hash(md5): 777b90c3bd38a4aacedc3b6230f98225
```

W przypadku kiedy wartość w polu „CN” odbiega od zaprezentowanego powyżej zalecamy kontakt z Biurem Obsługi Klienta dla usługi ‘eRepozytorium mMedica w chmurze’ w celu weryfikacji poprawności otrzymanych certyfikatów. Weryfikacji należy podać certyfikaty publiczne dla rodzaju TLS jak i WSS.

Biuro Obsługi Klienta dla usługi ‘eRepozytorium mMedica w chmurze’, czynne w dni robocze od godziny 8 do 16:

- telefonicznie z sieci stacjonarnych i komórkowych - **22 574 81 60**, koszt połączenia zgodnie z cennikiem operatora
- mailem - pomoc@chmuradlazedrowia.pl

2.4 Wystąpił błąd: „Forbidden (403)”.

Komunikat wskazuje, iż mogły nie zostać zarejestrowane na koncie tenenta klucze publiczne lub użytkownik wykonujący operacje nie został powiązany z personelem posiadającym nadany numer pesel lub NPWZ. W związku z powyższym należy sprawdzić:

- a) czy użytkownik (wykonujący operacje związane z chmurą) jest powiązany z osobą personelu posiadającą przypisany nr pesel lub NPWZ (Zarządzanie-> Konfiguracja -> Rejestr Personelu
- b) ważność certyfikatów dla usługi eRepozytorium w Chmurze. W przypadku stwierdzenia takiego braku aktualnych certyfikatów prosimy o kontakt z Biurem Obsługi Klienta dla usługi 'eRepozytorium mMedica w chmurze'.

Biuro Obsługi Klienta dla usługi 'eRepozytorium mMedica w chmurze', czynne w dni robocze od godziny 8 do 16:

- telefonicznie z sieci stacjonarnych i komórkowych - **22 574 81 60**, koszt połączenia zgodnie z cennikiem operatora
- mailem - pomoc@chmuradlazedrowia.pl

2.5 Wystąpił błąd: „Wystąpił błąd w obsłudze bezpiecznego kanału”.

Przyczyną otrzymywanego komunikatu mogą być:

1. Błędne wgranie klucza publicznego lub prywatnego TLS na formatce Zarządzania kontem w eRepozytorium w chmurze w mMedica (np. wgranie klucza prywatnego lub publicznego z WSS). Należy ponownie wykonać czynności opisane w rozdziale „1.1.1 Konfiguracja modułu”.
2. System operacyjny, który nie wspiera zabezpieczeń komunikacji TLS 1.2.

2.6 Wystąpił błąd: „Nie można przekazać CSR do BOK z powodu błędów podczas próby wysyłki e-mail”.

Komunikat związany jest z brakiem lub niepoprawną konfiguracją obszaru „Poczta inna”. W celu konfiguracji obszaru „Poczta inna” należy przejść do [Zarządzanie > Konfiguracja > Konfigurator](#) i w obszarze [Komunikacja > Poczta inna](#) wypełnić pola:

- a) Adres serwera poczty wychodzącej SMTP
- b) Adres e-mail
- c) Użytkownik
- d) Hasło

Po wypełnieniu danych należy przeprowadzić test połączenia poprzez wybranie przycisku .

Poczta do wysyłania powiadomień z aplikacji

Adres serwera poczty przychodzącej (POP3):

Port:

110

☐ SSL/TLS

☐ STARTTLS

☐ Użyj biblioteki OpenSSL dla połączeń szyfrowanych POP3

Adres serwera poczty wychodzącej (SMTP):

smtp.poczta.pl

Port:

25

☐ SSL/TLS

☐ STARTTLS

☐ Użyj biblioteki OpenSSL dla połączeń szyfrowanych SMTP

Adres e-mail:

poczta@poczta.pl

Użytkownik:

poczta

Hasło:

Test połączenia

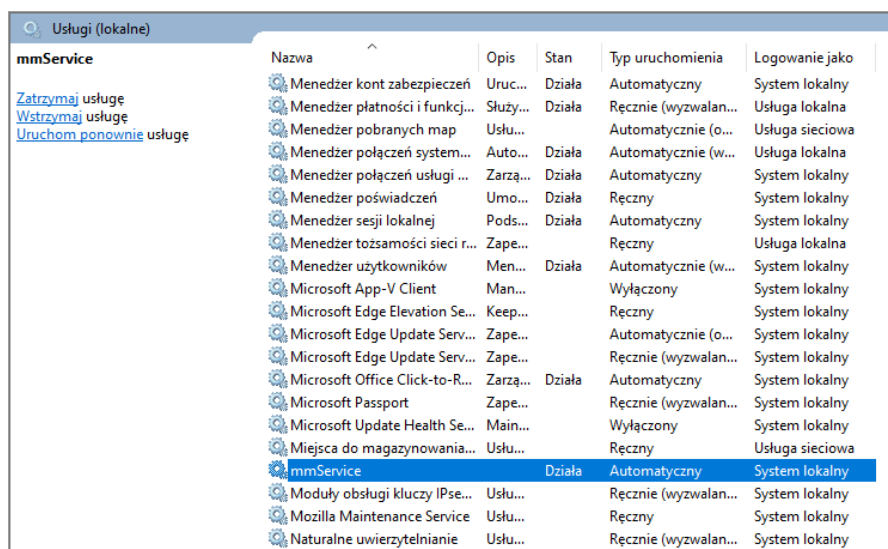


2.7 Przerwa serwisowa/techniczna dla usługi „eRepozytorium w Chmurze”.

Na czas przeprowadzania prac serwisowych/konserwacyjnych zaleca się wstrzymanie procesów mających za zadanie deponowanie dokumentów w repozytorium zewnętrznym.

Zatrzymanie procesów można osiągnąć poprzez zatrzymanie usługi wg następujących kroków na serwerze:

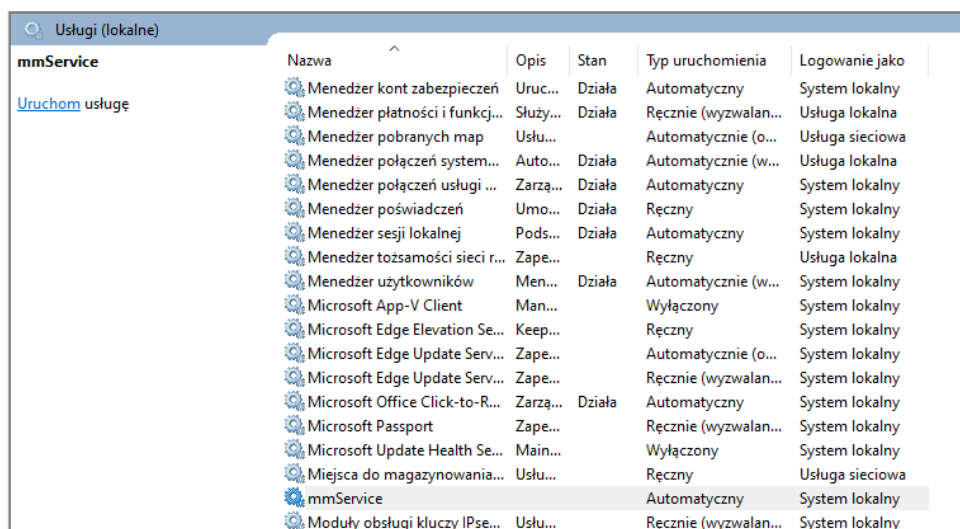
- Przejszć w Panel Sterowania -> Narzędzia Administracyjne -> Usługi
- Odszukać usługę mmService , a następnie wybrać operację „Zatrzymaj usługę”



The screenshot shows the Windows Services console with the 'Usługi (lokalne)' (Local Services) tab selected. The 'mmService' service is highlighted in blue. The left sidebar shows the 'Zatrzymaj usługę' (Stop service) button. The main table lists various services with their names, descriptions, status, start type, and logon account.

Nazwa	Opis	Stan	Typ uruchomienia	Logowanie jako
Menedżer kont zabezpieczeń	Uruc...	Działa	Automatyczny	System lokalny
Menedżer płatności i funkcj...	Służy...	Działa	Ręcznie (wyzwalan...	Usługa lokalna
Menedżer pobranych map	Uslu...		Automatycznie (o...	Usługa sieciowa
Menedżer połączeń system...	Auto...	Działa	Automatycznie (w...	Usługa lokalna
Menedżer połączeń usługi ...	Zarzą...	Działa	Automatyczny	System lokalny
Menedżer poświadczeń	Umo...	Działa	Ręczny	System lokalny
Menedżer sesji lokalnej	Pods...	Działa	Automatyczny	System lokalny
Menedżer tożsamości sieci r...	Zape...		Ręczny	Usługa lokalna
Menedżer użytkowników	Men...	Działa	Automatycznie (w...	System lokalny
Microsoft App-V Client	Man...		Wyłączony	System lokalny
Microsoft Edge Elevation Se...	Keep...		Ręczny	System lokalny
Microsoft Edge Update Serv...	Zape...		Automatycznie (o...	System lokalny
Microsoft Edge Update Serv...	Zape...		Ręcznie (wyzwalan...	System lokalny
Microsoft Office Click-to-R...	Zarzą...	Działa	Automatyczny	System lokalny
Microsoft Passport	Zape...		Ręcznie (wyzwalan...	System lokalny
Microsoft Update Health Se...	Main...		Wyłączony	System lokalny
Miejsca do magazynowania...	Uslu...		Ręczny	Usługa sieciowa
mmService		Działa	Automatyczny	System lokalny
Moduły obsługi kluczy IPse...	Uslu...		Ręcznie (wyzwalan...	System lokalny
Mozilla Maintenance Service	Uslu...		Ręczny	System lokalny
Naturalne uwierzytelnianie	Uslu...		Ręcznie (wyzwalan...	System lokalny

- Po zakończeniu przerwy usługę należy uruchomić z wykorzystaniem przycisku „Uruchom usługę”



The screenshot shows the Windows Services console with the 'Usługi (lokalne)' (Local Services) tab selected. The 'mmService' service is highlighted in blue. The left sidebar shows the 'Uruchom usługę' (Start service) button. The main table lists various services with their names, descriptions, status, start type, and logon account.

Nazwa	Opis	Stan	Typ uruchomienia	Logowanie jako
Menedżer kont zabezpieczeń	Uruc...	Działa	Automatyczny	System lokalny
Menedżer płatności i funkcj...	Służy...	Działa	Ręcznie (wyzwalan...	Usługa lokalna
Menedżer pobranych map	Uslu...		Automatycznie (o...	Usługa sieciowa
Menedżer połączeń system...	Auto...	Działa	Automatycznie (w...	Usługa lokalna
Menedżer połączeń usługi ...	Zarzą...	Działa	Automatyczny	System lokalny
Menedżer poświadczeń	Umo...	Działa	Ręczny	System lokalny
Menedżer sesji lokalnej	Pods...	Działa	Automatyczny	System lokalny
Menedżer tożsamości sieci r...	Zape...		Ręczny	Usługa lokalna
Menedżer użytkowników	Men...	Działa	Automatycznie (w...	System lokalny
Microsoft App-V Client	Man...		Wyłączony	System lokalny
Microsoft Edge Elevation Se...	Keep...		Ręczny	System lokalny
Microsoft Edge Update Serv...	Zape...		Automatycznie (o...	System lokalny
Microsoft Edge Update Serv...	Zape...		Ręcznie (wyzwalan...	System lokalny
Microsoft Office Click-to-R...	Zarzą...	Działa	Automatyczny	System lokalny
Microsoft Passport	Zape...		Ręcznie (wyzwalan...	System lokalny
Microsoft Update Health Se...	Main...		Wyłączony	System lokalny
Miejsca do magazynowania...	Uslu...		Ręczny	Usługa sieciowa
mmService			Automatyczny	System lokalny
Moduły obsługi kluczy IPse...	Uslu...		Ręcznie (wyzwalan...	System lokalny