eRepozytorium w Chmurze

Instrukcja użytkownika

Wersja: 1.9

2022-10-10

Spis treści

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 (mmedica-licencje.asseco.pl),
2. usługi „eRepozytorium mMedica w chmurze", kupowanej w sklepie „chmuradlazdrowia.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.

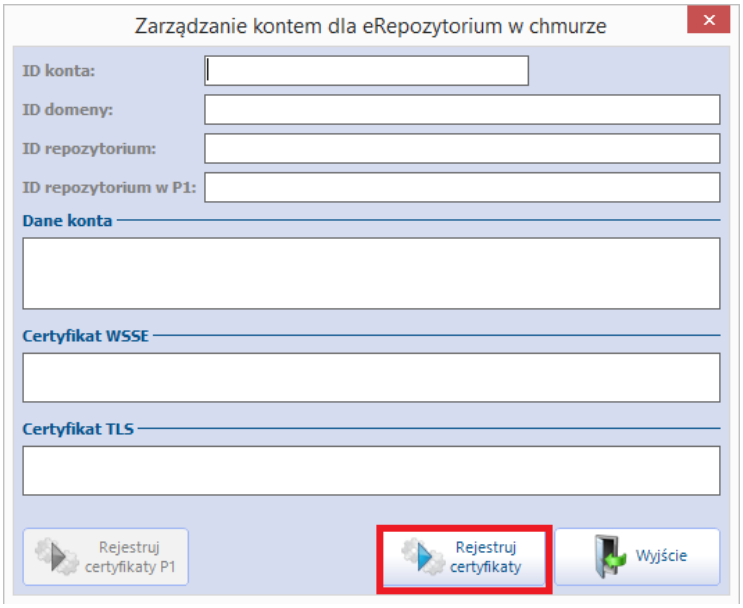
1.1 Rozpoczęcie pracy z Modułami eRepozytorium w Chmurze, eAnkiety w Chmurze.

Należy dokonać konfiguracji modułów 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 modułów

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".

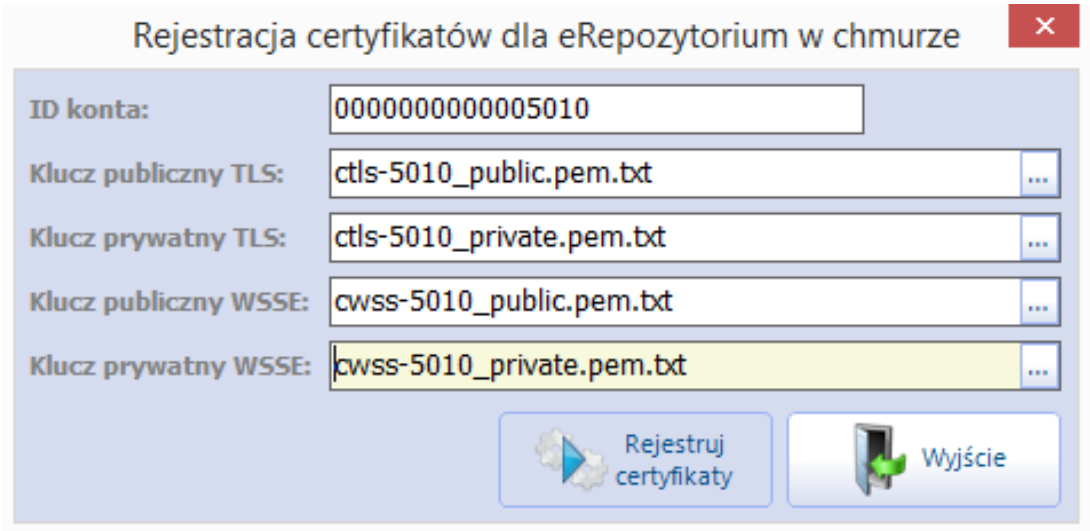


W polu „ID Konta" należy wprowadzić identyfikator konta w chmurze otrzymany w procesie zamawiania produktu w „chmuradlazdrowia.pl".
Z kolei w polach:

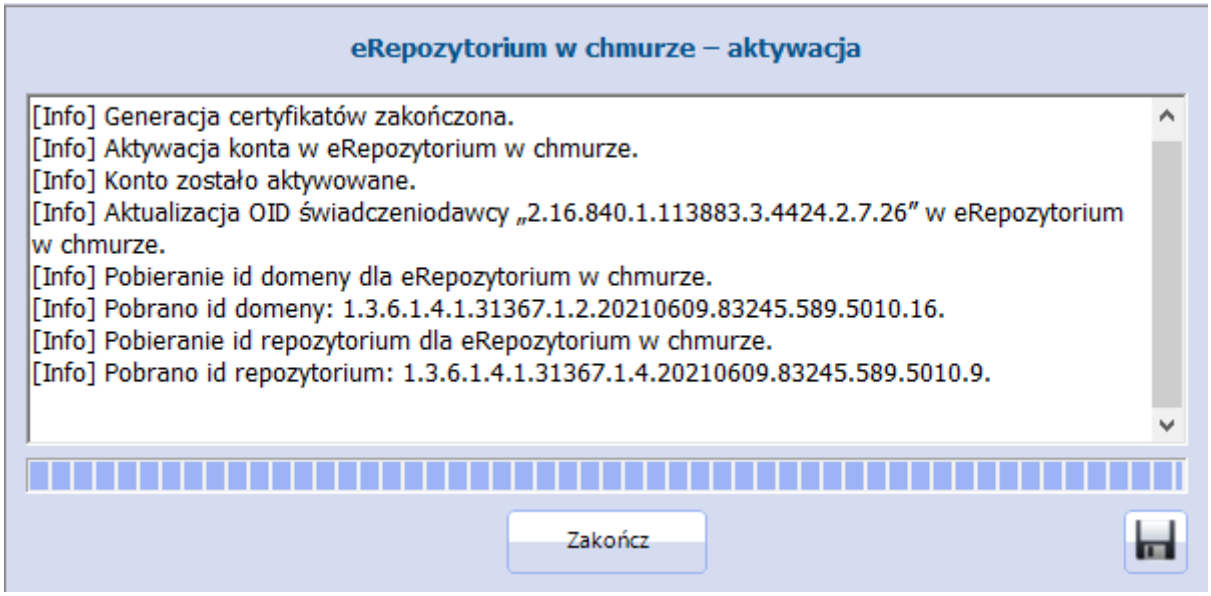
a) Klucz publiczny TLS
b) Klucz prywatny TLS
c) Klucz publiczny WSSE
d) Klucz prywatny WSSE

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.

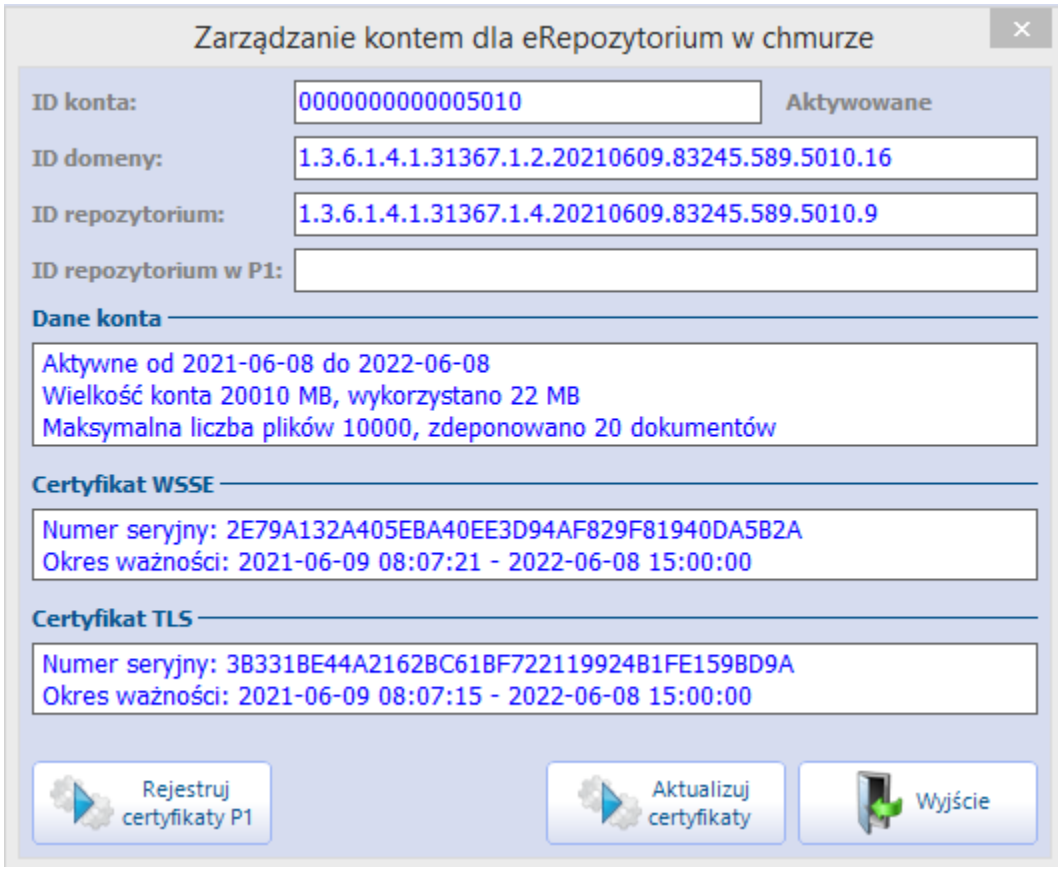


Wybranie przycisku „Rejestruj certyfikaty" uruchamia proces aktywacji konta w chmurze, w wyniku którego zostaną przekazane identyfikatory techniczne konta. Przykładowe komunikaty zwrócone w procesie rejestracji przedstawiono poniżej:



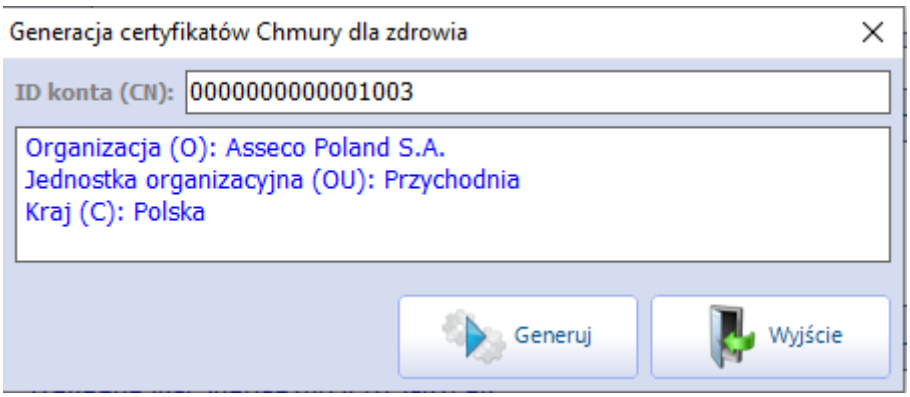
Wybranie przycisku „Zakończ" przekierowuje użytkownika do głównego panelu zarządzającego kontem i wyświetlana informacje o stanie konta. Po poprawnej aktywacji konta użytkownik otrzymuje możliwość rejestracji certyfikatów systemu P1, których przekazanie jest wymagane w przypadku chęci skorzystanie z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



1.1.2 Konfiguracja modułów od wersji 8.2.1 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”.



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

a) Organizacja (O)
b) Jednostka organizacyjna (OU)
c) Kraj (C)

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

(…)

Witam,

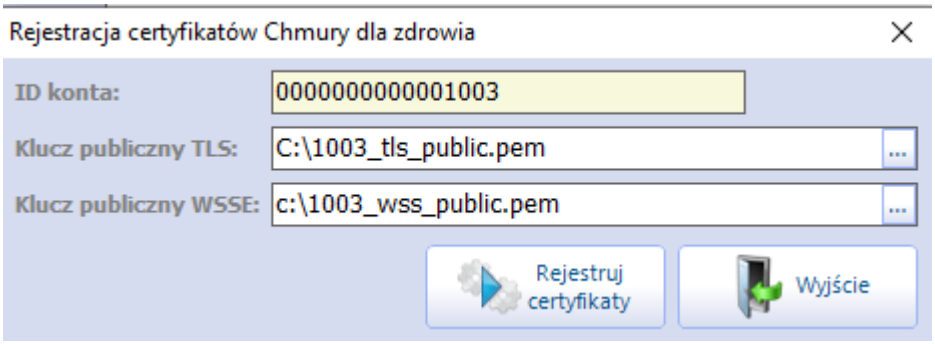
przekazano żądanie wydania certyfikatu (CSR) dla konta tenanta 0000000000001003.

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. W celu aktywacji konta należy przejść do ścieżki: Zarządzanie > Konfiguracja > Konfigurator, obszar Funkcje dodatkowe> Zarządzanie kontem Chmury dla zdrowia i wybrać przycisk „Rejestruj certyfikaty".

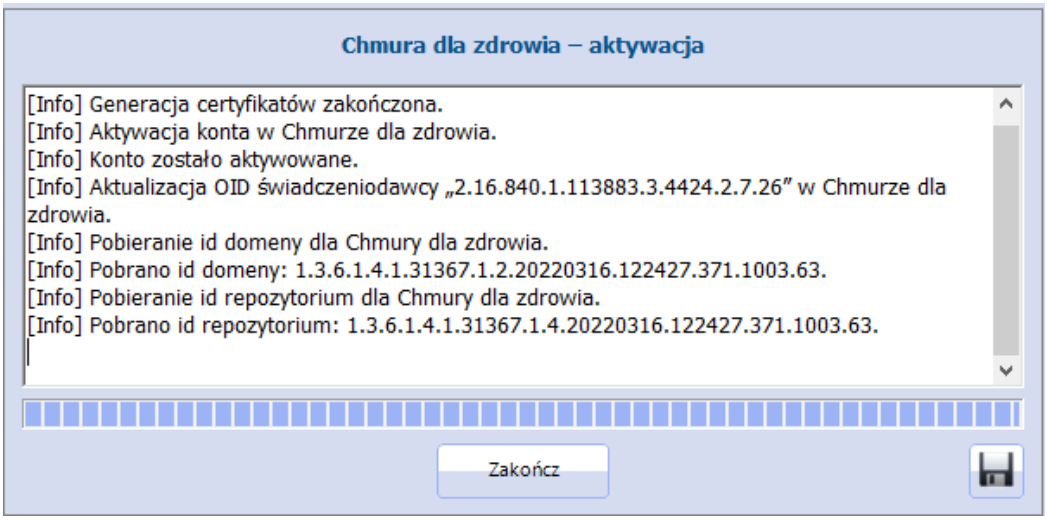


W polu „ID Konta" należy wprowadzić identyfikator konta w chmurze otrzymany w procesie zamawiania produktu w „chmuradlazdrowia.pl". Z kolei w polach:

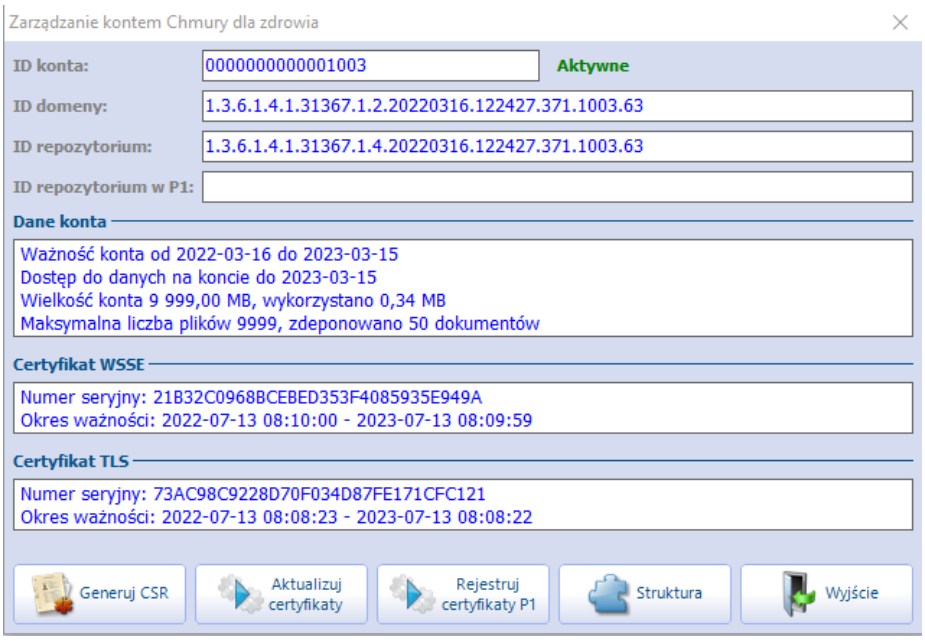
a) Klucz publiczny TLS
b) Klucz prywatny TLS

należy wskazać klucze publiczne przekazane przez Biuro Obsługi Klienta sklepu „chmuradlazdrowia.pl". Pliki te posiadają rozszerzenie *.pem.

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:



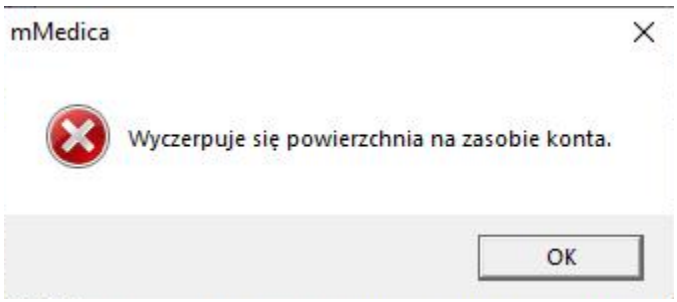
Wybranie przycisku „Zakończ” przekierowuje użytkownika do głównego panelu zarządzającego kontem i wyświetlana informacje o stanie konta. Po poprawnej aktywacji konta użytkownik otrzymuje możliwość rejestracji certyfikatów systemu P1, których przekazanie jest wymagane w przypadku chęci skorzystanie z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

a) ważność konta
b) wielkość konta oraz stan jego wykorzystania
c) 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.

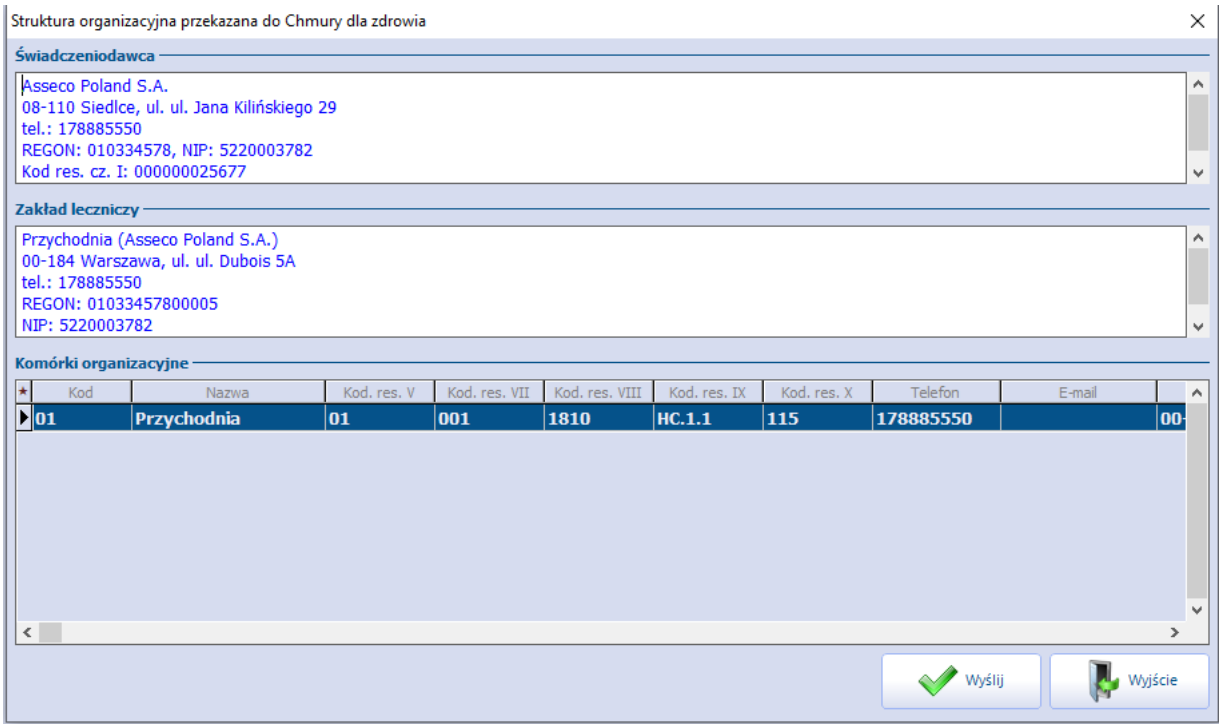


1.1.3 Aktualizacja certyfikatów dla konta tenanta od wersji 8.2.1 aplikacji mMedica

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"



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".

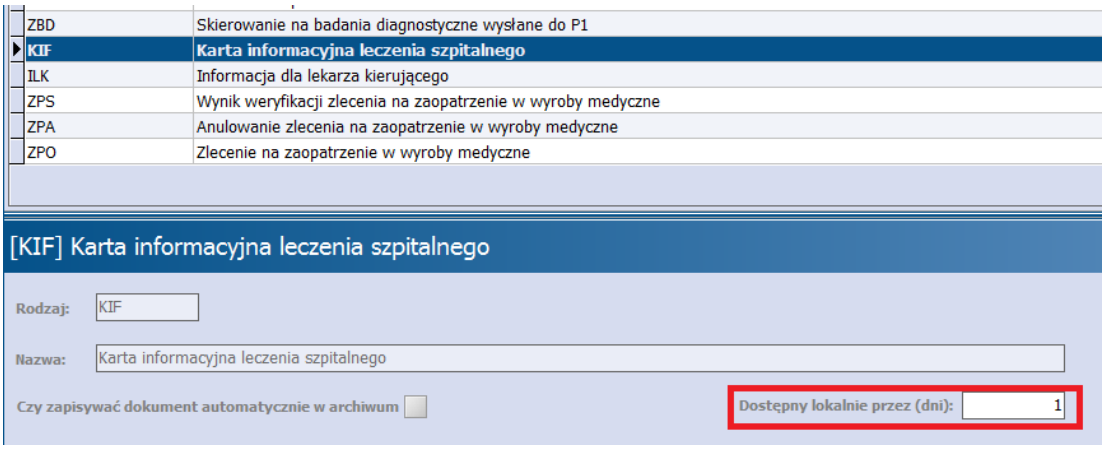
Po przejściu do powyższej ścieżki, w górnym oknie *Rodzaje dokumentów* prezentowane są rodzaje dokumentów, które mogą być przekazywane z programu do zewnętrznego repozytorium. Przykładowe dokumenty wymienione poniżej:

- **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 Gabinecie.
- **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:
a) e-Recepta
b) e-Skierowanie do specjalisty
c) e-Skierowane do szpitala
d) 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.



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-Skierowane do szpitala
d) e-Skierowanie na badanie diagnostyczne podlegające wysyłce do P1.

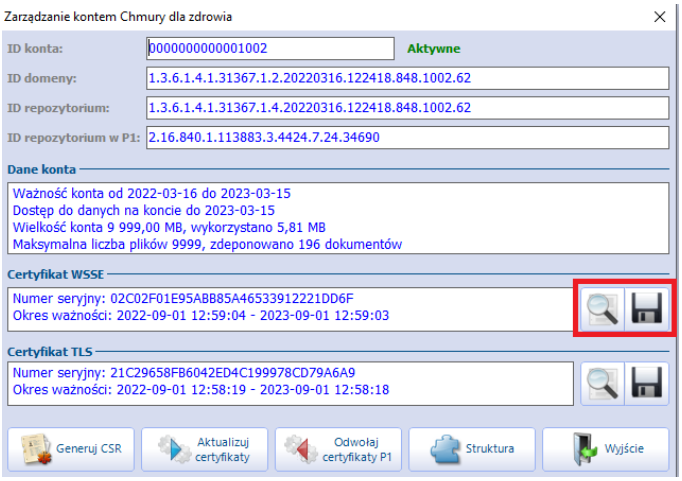
Pozostałe typy dokumentów, które są wytwarzane w podmiocie leczniczym jako dokumenty PIK HL7 CDA lub zostały pobrane z zewnętrznych repozytoriów innych świadczeniodawców będą przenoszone do zewnętrznego repozytorium.

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 zarządzający takimi zasobami jak:

a) Panel administracyjny konta tenanta
b) Portal eAnkiety

Powyższe zasoby dostępne są pod adresami:

a) Panel administracyjny konta tenanta

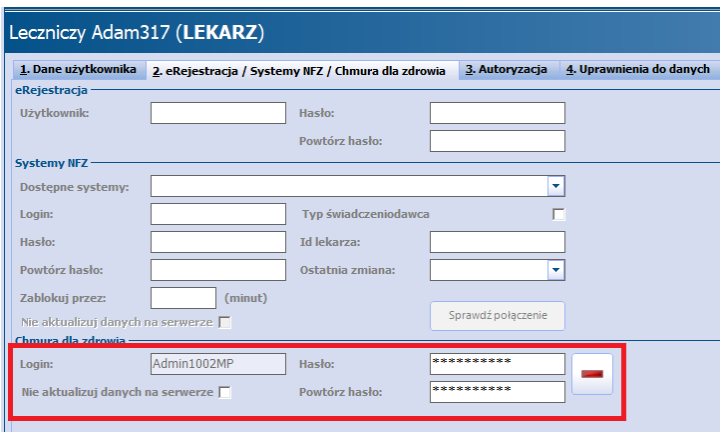
https://konto.chmuradlazdrowia.pl/services/id konta/app

b) Portal eAnkiety

https://konto.chmuradlazdrowia.pl/services/id konta/e-survey-gui/#/login

Aby poprawnie uruchomić ekrany logowania należy:

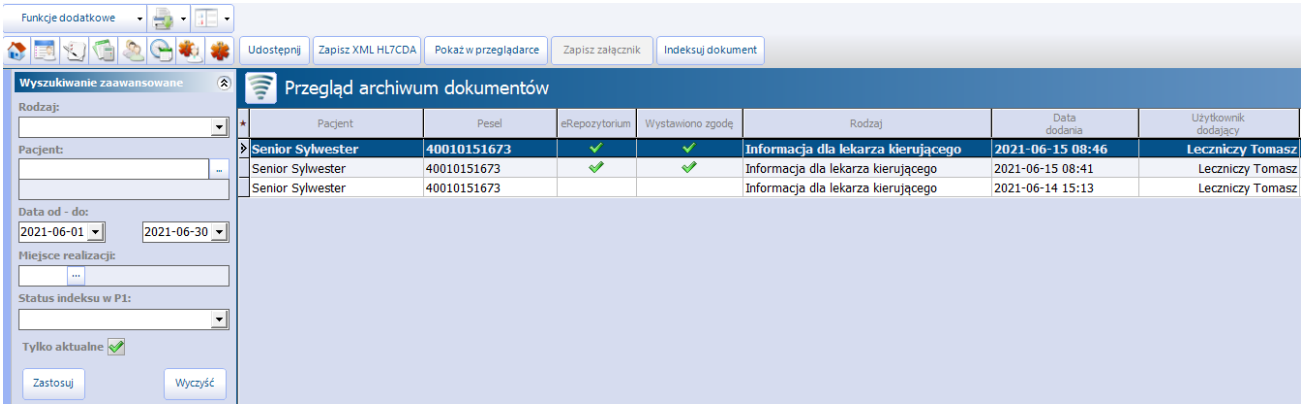
1. Zaczytać certyfikat TLS w przeglądarce wykorzystywanej do połączenia z powyższymi paneli.
2. **Zmodyfikować powyższy link** i w miejsce „id konta” **wpisać właściwy numer tenanta,** otrzymany po zakupie usługi w BOK
3. Pierwsze logowanie do powyższych aplikacji należy przeprowadzić za pomocą konta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

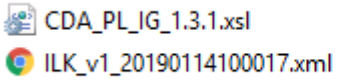


Opis przycisków znajdujących się w górnej części okna:

- **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.

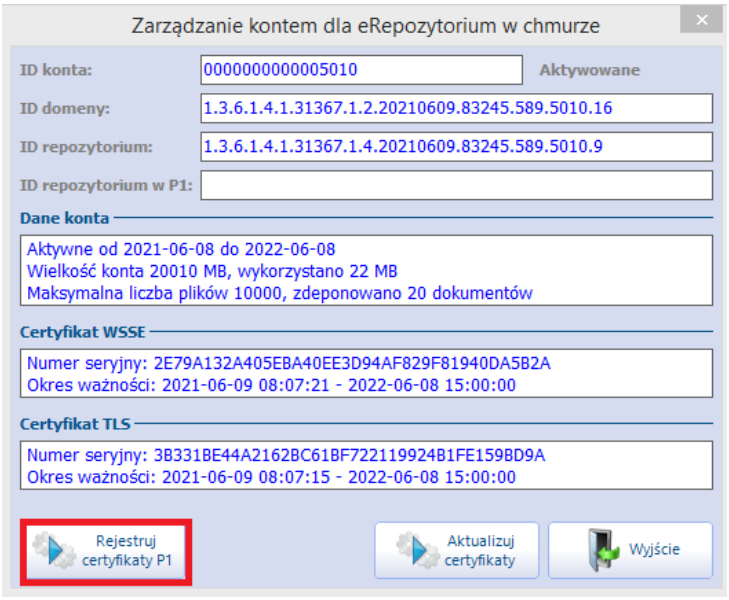


Z kolei wizualizacja elektronicznego dokumentu medycznego następuje poprzez wyświetlenie go w postaci strony HTML. Aby podejrzeć wygenerowany dokument, należy wybrać przycisk **Pokaż w przeglądarce**.

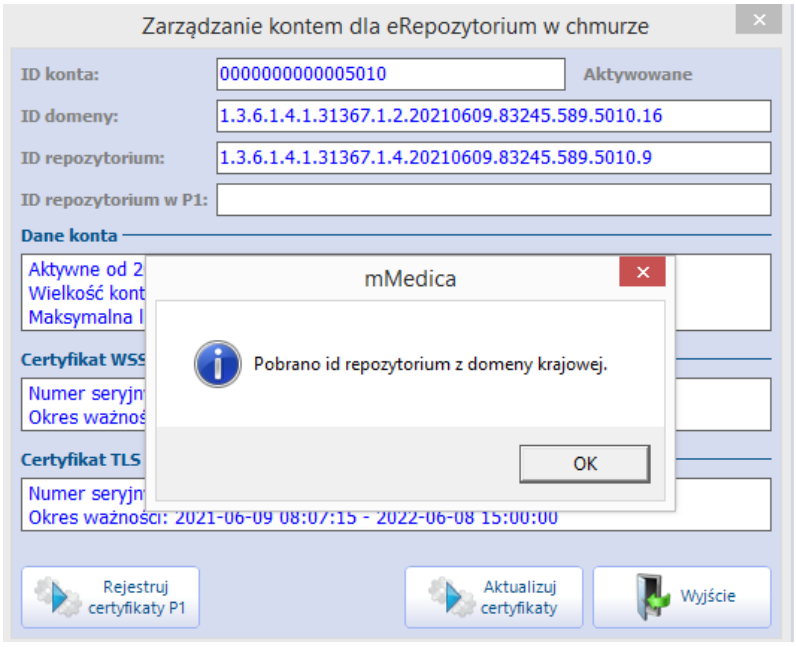
1.3. Rejestracja „eRepozytorium w Chmurze” w domenie krajowej (System P1).

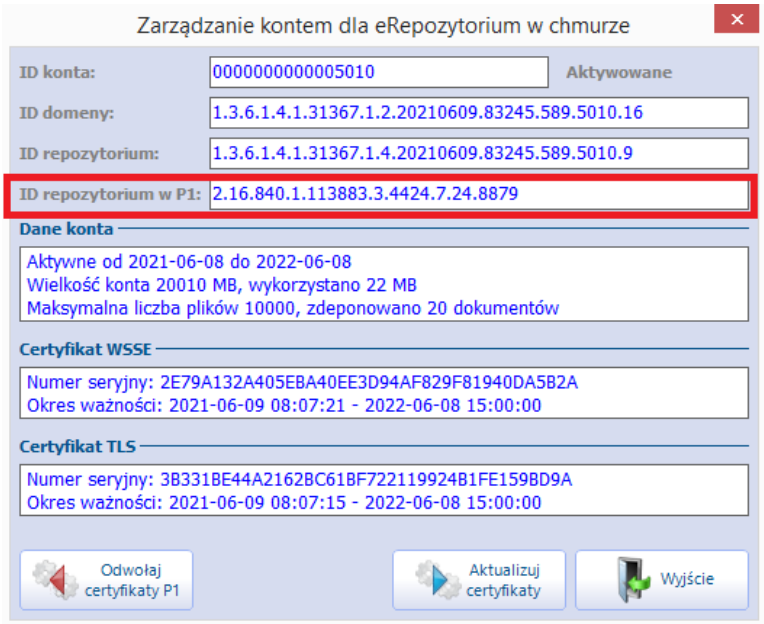
Ścieżka: Zarządzanie > Konfiguracja > Konfigurator, obszar: Funkcje dodatkowe> Zarządzanie kontem dla eRepozytorium w chmurze

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.



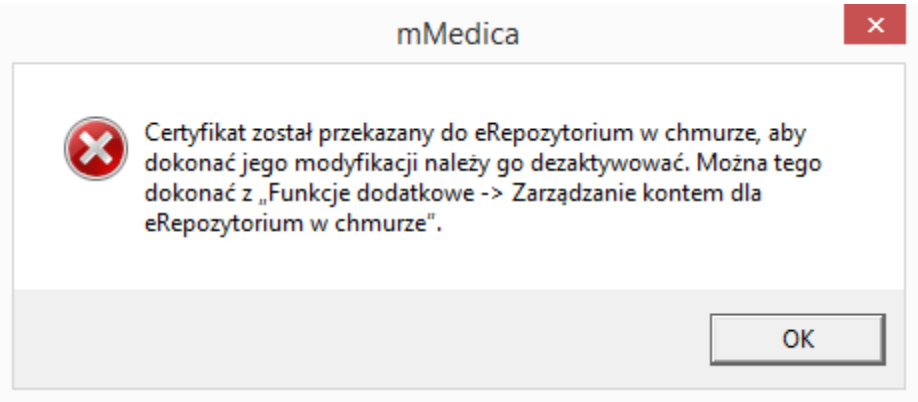


Przekazany przez system P1 identyfikator repozytorium zostanie wykorzystany w procesie indeksowania dokumentów.

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 „Odwołaj 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.

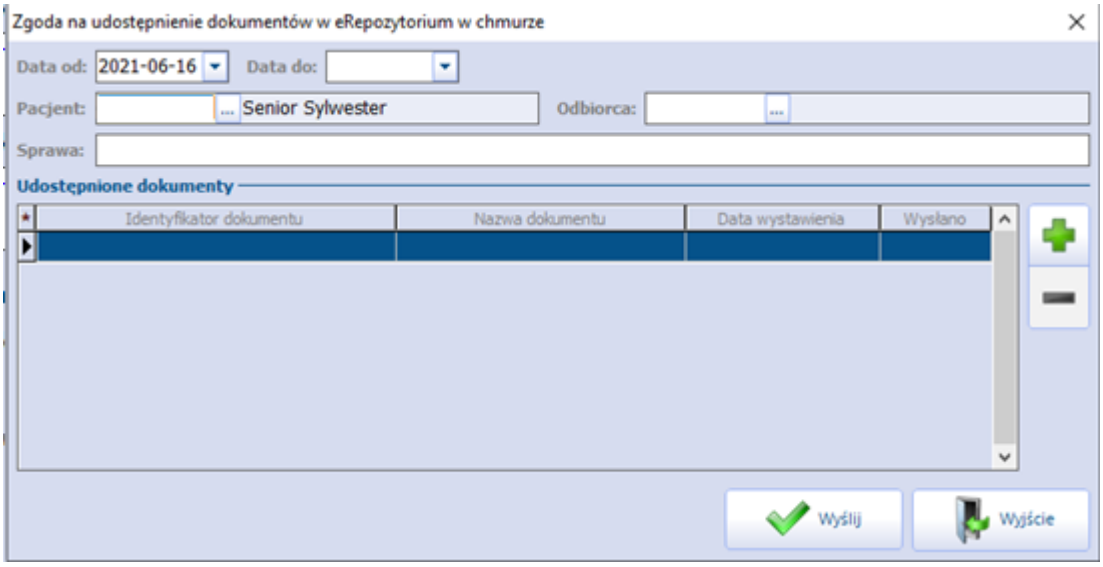


1.4. Rejestr zgód.

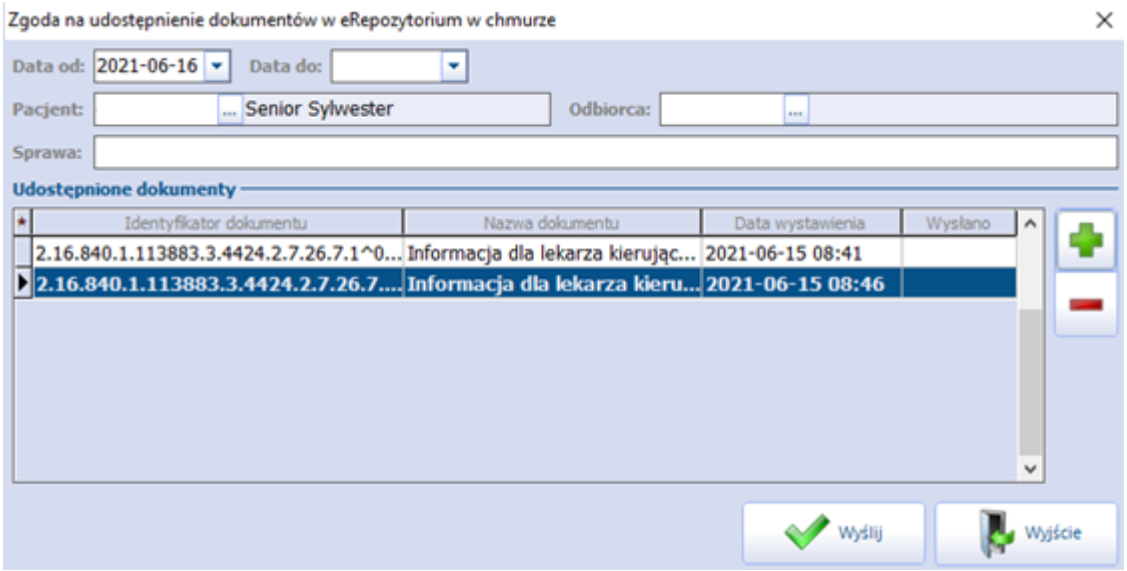
Ścieżka: Zarządzanie > Ochrona danych osobowych > Rejestr zgód dla eRepozytorium w chmurze

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

a) Zakres czasowy w którym dokument ma być widoczny w Portalu eRejestracja. Pola „Data od", „Data do"
b) Pacjenta, dla którego został wytworzony udostępniany dokument
c) Odbiorcę dokumentu
d) Przyczynę potrzeby udostępnienia dokumentu. Pole „Sprawa"



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



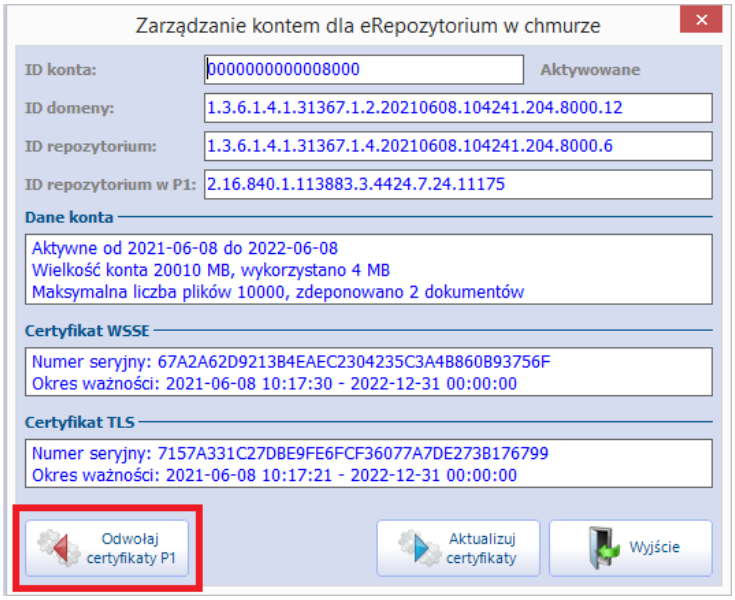
Wybranie przycisku „Wyślij" uruchamia proces udostępniania.

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

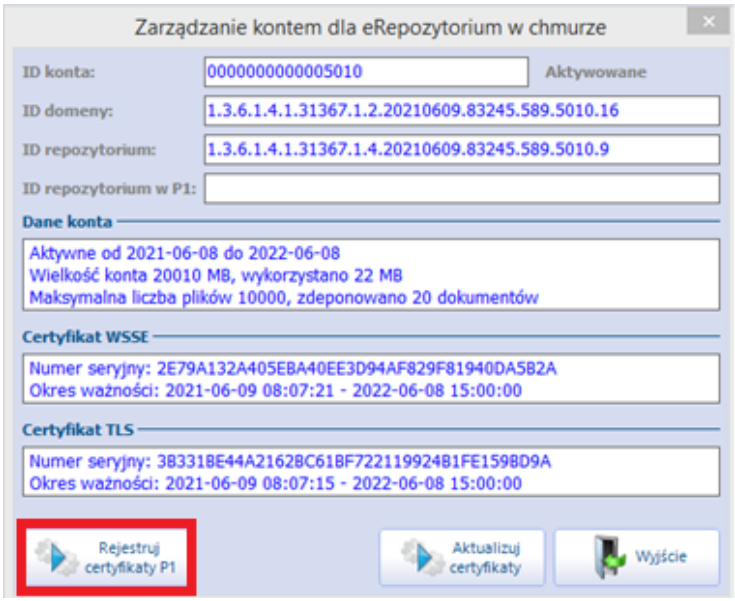
2. Rozwiązania częstych problemów

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”,



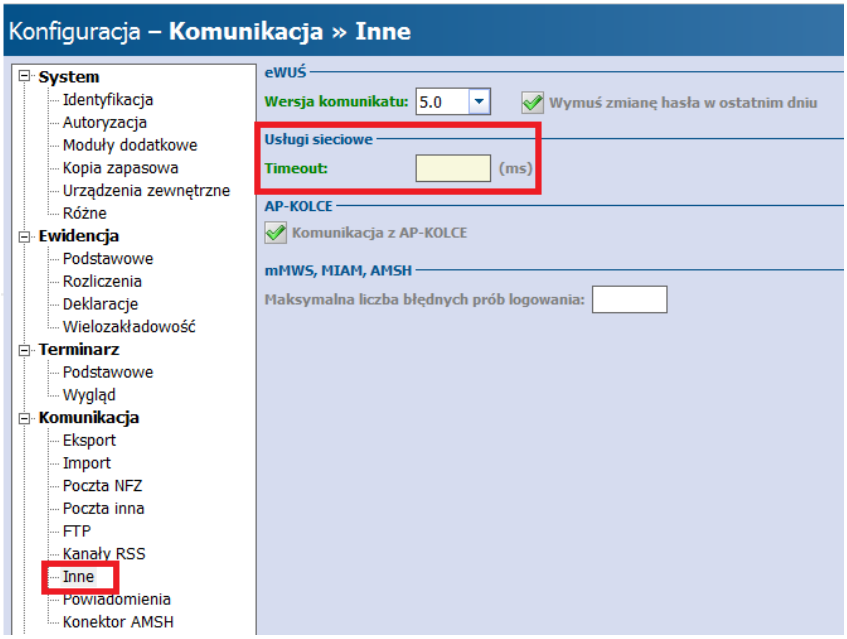
4. W oknie „Zarządzanie kontem dla eRepozytorium w chmurze’ wybrać przycisk „Rejestruj certyfikaty P1”



2.2 **Limit czasu operacji został przekroczony**.

Należy przeprowadzić operację zwiększenia czasu oczekiwania na odpowiedz 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 Requst (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 wiesz poleceń "CMD" w katalogu w których znajdujące się zaczytywane do bazy certyfiakty TLS i WSSE dla usługi „eRepozytorium mMedica w chmurze”
2. W wierszu poleceń wpisać polecenie: certulit "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

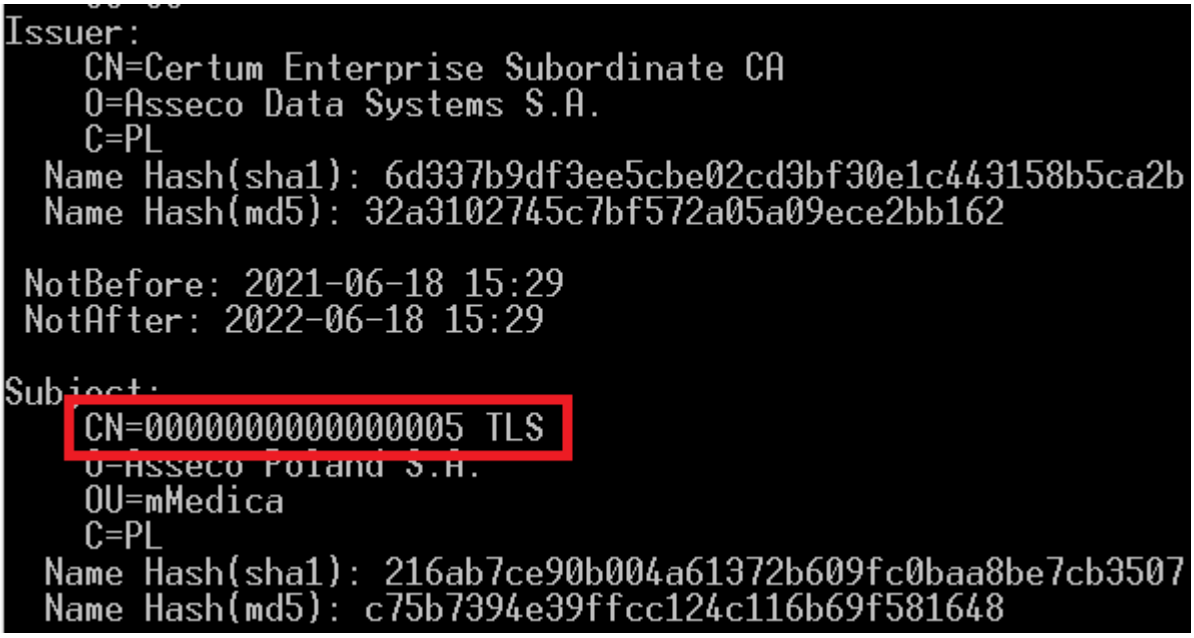
b) WSS

Nazwy plików certyfikatów przyjmują postać:

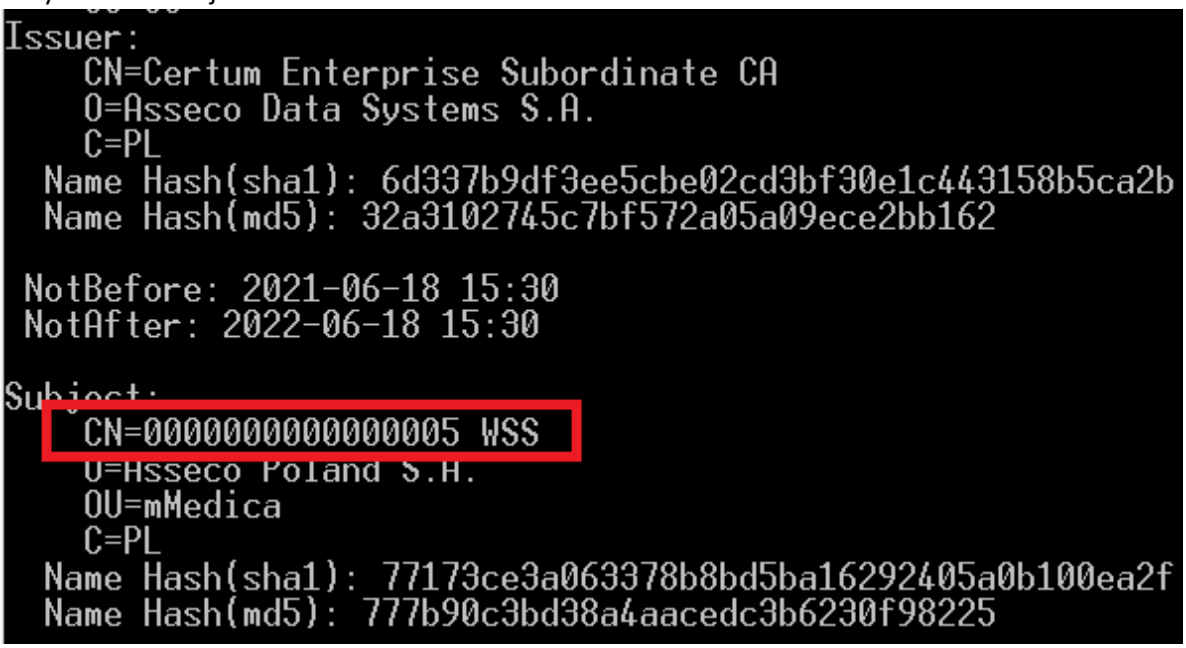
a) TLSnumerseryjny.pem dla certyfikatu w rodzaju TLS
b) WSSnumerseryjny.pem dla certyfikatu w rodzaju TLS

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

1. Certyfikat w rodzaju TLS:



2. Certyfikat w rodzaju WSS:



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@chmuradlazdrowia.pl

2.4 **„Wystąpił błąd: „Forbidden (403)”.**

Komunikat wskazuje, iż nie zostały zarejestrowane na koncie tenenta klucze publiczne. W tym celu zalecały 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@chmuradlazdrowia.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  .