

Usługa sieciowa (WebService) do wymiany danych

wersja: 1.1

Słownik pojęć

Użytkownik – podmiot chcący uzyskać dostęp do usługi sieciowej

SOA – Service Oriented Architecture – architektura zorientowana na usługę

WSDL – Web Service Definition Language – język definiujący usługi sieciowe, wykorzystuje język XML do opisu tych usług oraz definicji parametrów potrzebnych do wywołania tych usług

SOAP – Simple Object Access Protocol – protokół komunikacyjny, wykorzystujący XML do budowania wywołań usług sieciowych zdefiniowanych w przez WSDL

PCKS-12 – format pliku archiwum *.p12 do przechowywania wielu obiektów kryptograficznych w jednym pliku. Powszechnie używany jest pakiet kluczy prywatnych z certyfikatem X.509 lub pakietem certyfikatów publicznych tzw. łańcucha zaufania

X.509 – standard definiujący schemat dla certyfikatów cyfrowych oraz ich atrybutów.

CA – Certification Authority – Centrum Certyfikacji, urząd certyfikacji, wystawia/unieważnia certyfikaty, certyfikuje inne CA

HTTPS - Hypertext Transfer Protocol Secure – jest protokołem zapewniającym bezpieczną komunikację w sieci komputerowej powszechnie stosowanej w Internecie

OTA – Over-The-Air – usługi świadczone zdalnie, bezprzewodowo

System Rejestracji – aplikacja www dostępna z sieci Internet umożliwiająca wypełnienie formularza elektronicznego (wniosku) stanowiącego podstawę do utworzenia konta i udostępnienia certyfikatu cyfrowego potrzebnego do uzyskania dostępu do usługi sieciowej

Jednorazowy link – adres url wraz z specjalnie spreparowanymi parametrami kierujący do Systemu Rejestracji, po jego kliknięciu wyzwalana jest jednorazowa akcja systemowa a po jej wykonaniu link staje się bezużyteczny

Wstęp

Projekt ma na celu utworzenie uniwersalnego bezpiecznego kanału do wymiany informacji pomiędzy UKNF a podmiotami zewnętrznymi (odbiorcami usługi), które muszą przesłać do UKNF ustrukturyzowane informacje w postaci ściśle zdefiniowanego pliku (nazwa, format). Kanał ten udostępniony zostanie jako ustandaryzowana usługa sieciowa (Web Service) w architekturze SOA. Dzięki temu odbiorcy usługi będą mogli w łatwy sposób zintegrować z nią swoje systemy informatyczne lub skorzystać z dowolnego klienta umożliwiającego komunikację zgodną ze standardem WSDL.

1 Usługa sieciowej dla kanału do wymiany informacji

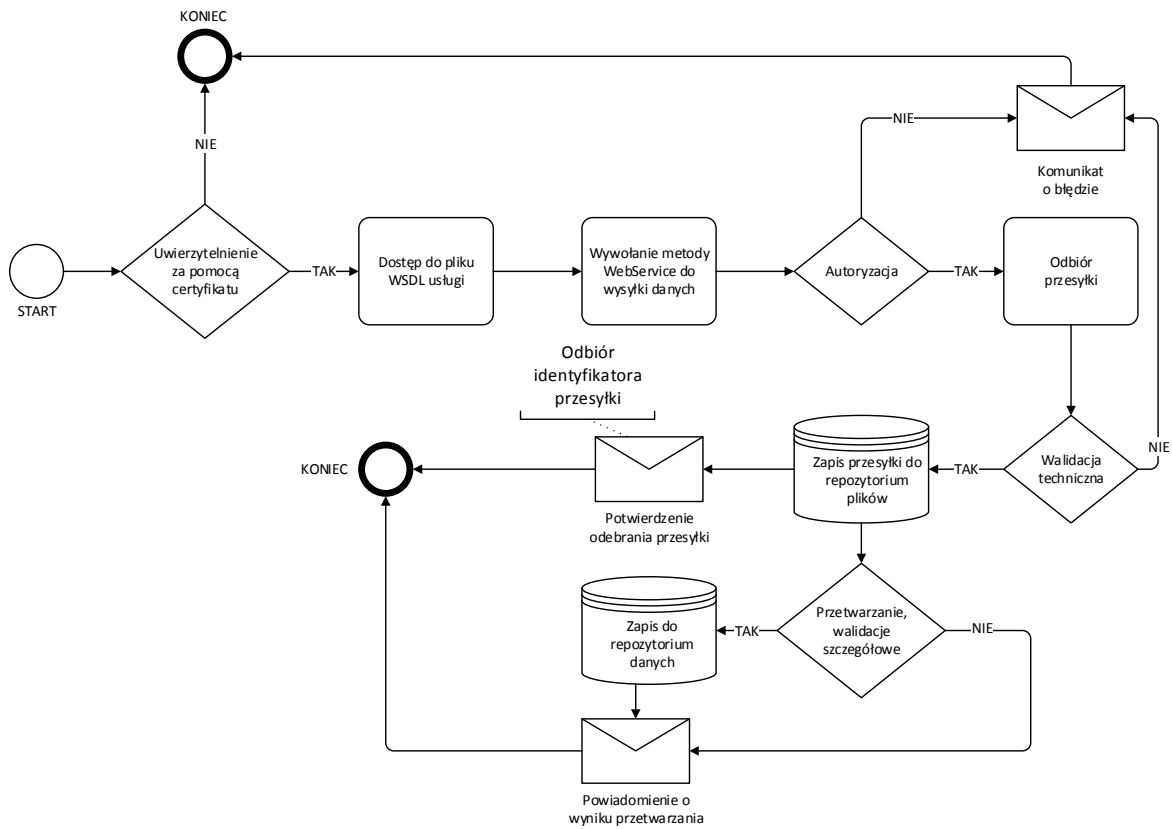
Użytkownik (podmiot) w celu dostępu do usługi musi posiadać ważny certyfikat cyfrowy wystawiony przez centrum certyfikacji UKNF. Proces pozyskania certyfikatu przez użytkownika stanowi oddzielny proces i szczegółowo opisany został w kolejnych rozdziałach.

1.1 Opis procesu wymiany danych

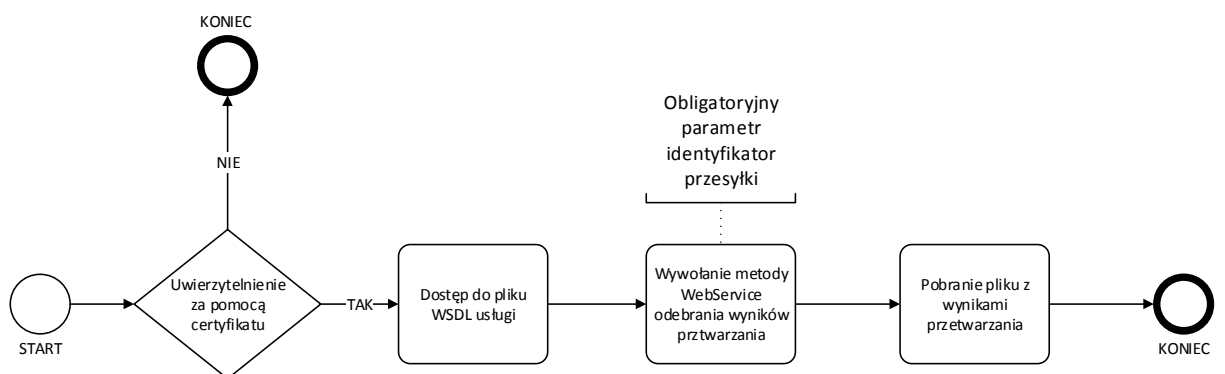
1. Użytkownik łączy się z sieci Internet pod adresem usługi sieciowej, z wykorzystaniem bezpiecznego protokołu HTTPS. W procesie tym następuje uwierzytelnienie użytkownika za pomocą certyfikatu cyfrowego oraz weryfikacja aktualnego statusu tego certyfikatu. Po poprawnej autentykacji użytkownik uzyskuje dostęp do usługi, w tym szczegółowe informacje w postaci pliku WSDL potrzebne do zdalnego wywołania metod komunikacyjnych kanału.
2. Użytkownik, wykorzystując dowolnego klienta usługi WSDL, konstruuje zapytanie w standardzie SOAP i wywołuje metodę usługi transmitując dane w zależności od rodzaju informacji którą zamierza przesłać.
3. Usługa w trybie online dokonuje autoryzacji użytkownika weryfikując czy ma nadany dostęp do usługi na podstawie rodzaju i parametrów wejściowych wywoływanej metody oraz dokonuje wstępnych walidacji technicznych obejmujących strukturę nazwy plików w przesyłce oraz ich poprawność semantyczną np. w przypadku plików XML zgodność z XSD.
4. W przypadku pozytywnej autoryzacji oraz wstępnej walidacji użytkownik system odbiera przesyłkę.
5. Użytkownik w komunikacie zwrotnym usługi otrzymuje informację zawierającą datę i czas odebrania danych oraz unikalny identyfikator przesyłki – przesyłka ma *status przyjęta do przetwarzania*. Unikalny identyfikator jest niezbędny do pobrania wyników dalszego przetwarzania,
6. Przesyłka trafia do kolejki przetwarzania, a użytkownik czeka na powiadomienie o zakończeniu przetwarzania.
7. Po zakończeniu przetwarzania wysyłany jest mail z informacją o wyniku pozytywnym lub negatywnym oraz udostępnieniu wyników przetwarzania do pobrania.
8. Pobieranie wyników (pliku potwierdzenia) odbywa się również za pomocą usługi sieciowej. W wywoływanej metodzie należy podać obligatoryjnie parametr zawierający unikalny identyfikator przesyłki otrzymany w pkt 5.
9. Pobrany plik potwierdzenia zawiera informacje o statusie przetworzenia – status może mieć wartość:
 - pozytywny
 - Błąd - w tej sytuacji plik zawiera również listę błędów

1.2 Schematy procesów

1.2.1 Proces przesyłania danych



1.2.2 Proces odbioru wyników przetwarzania



1.3 Szczególny techniczne

1.3.1 Standardy techniczne

Usługa sieciowa będzie zgodna ze standardami

- WSDL (<https://www.w3.org/TR/wsdl>) w zakresie definicji usługi
- SOAP (<https://www.w3.org/TR/soap/>) w zakresie protokołu komunikacyjnego usługi
- WS-SECURITY (<https://www.oasis-open.org/committees/wss/>) w zakresie przesyłania danych dot. uwierzytelnionego użytkownika certyfikatem cyfrowym w standardzie x.509
- MTOM (<https://www.w3.org/TR/soap12-mtom/>) w zakresie transmisji plików binarnych

1.3.2 Uwierzytelnienie użytkowników

Uwierzytelnianie użytkowników (podmiotów zewnętrznych) będzie odbywać się za pomocą certyfikatów cyfrowych w standardzie X.509, weryfikowana będzie tożsamość użytkownika w zakresie czy certyfikat którym się legitymuje został wygenerowany z CA UKNF, czy nie wygasł, został odwołany lub unieważniony.

1.3.3 Autoryzacja użytkowników

Autoryzacja użytkowników weryfikować będzie dostęp do poszczególnych metod usługi sieciowej.

1.4 Bezpieczeństwo

Całość komunikacji pomiędzy użytkownikiem zabezpieczona będzie kanałem szyfrowanym z wykorzystaniem protokołu HTTPS.

Dostęp do usługi sieciowej chroniony będzie poprzez uwierzytelnienie za pomocą certyfikatu cyfrowego w standardzie X.509 wygenerowanego z centrum certyfikacji UKNF. Certyfikaty będą ważne przez rok, natomiast miesiąc przed wygaśnięciem system będzie powiadamiał użytkowników, za pomocą wiadomości e-mail, o konieczności jego odnowienia. Proces odnowienia opisany w rozdziale 3.2.

Klucz prywatny i publiczny użytkownika składowany będzie w pliku archiwum PCKS-12 służącym do przechowywania kluczy kryptograficznych, które jest szyfrowane i chronione hasłem. Plik ten będzie dystrybuowany w sieci Internet poprzez przesłanie tzw. linku jednorazowego. Użytkownik klikając w link jednorazowo pobierze certyfikat, po czym link stanie się bezużyteczny. Ponowne pobranie certyfikatu możliwe będzie po wygenerowaniu nowego linku i przesłaniu go na adres email użytkownika.

Hasło do instalacji certyfikatów z pliku PCKS-12 docelowo będą wysyłane w wiadomości SMS, jednakże w okresie przejściowym mogą być również przesyłane za pomocą wiadomości e-mail.

Usługa sieciowa implementować będzie standard WS-Security z wykorzystaniem certyfikatów cyfrowych w standardzie X.509.

2 Aplikacja do dystrybucji certyfikatów cyfrowych

2.1 Proces rejestracji oraz uzyskania certyfikatu przez użytkownika

1. Użytkownik (podmiot zewnętrzny) będzie mógł zarejestrować się wypełniając elektroniczny formularz rejestracyjny w Systemie Rejestracji tzw. wniosek.
2. Po zakończeniu wprowadzenia danych formularz waliduje wprowadzone informacje pod względem ich kompletności oraz poprawności typu wprowadzanych informacji.
3. Po poprawnym wypełnieniu i wysłaniu formularza zostaje on zapisany w repozytorium danych.
4. Do użytkownika, który wypełnił formularz, na wskazany we wniosku adres e-mail zostaje wysłana wiadomość z jednorazowym linkiem umożliwiającym potwierdzenie adresu e-mail.
5. Kliknięcie użytkownika w przesłany w mailu link powoduje oznacza potwierdzający poprawność wprowadzonego adresu.
6. Wniosek zostaje udostępniony weryfikacji która kończy się jego akceptacją lub odrzuceniem.
7. Odrzucenie wniosku generuje powiadomienie e-mail o tym fakcie do użytkownika.
8. Akceptacja wniosku wyzwala proces generowania certyfikatu cyfrowego z CA UKNF.
9. Do użytkownika na adres e-mail zawarty we wniosku wysyłany jest jednorazowym linkiem do pobrania pliku PCKS-12.
10. Pobranie przez użytkownika powoduje wysłanie do użytkownika nowej wiadomości e-mail z jednorazowym linkiem do pobrania hasła do instalacji pobranego certyfikatu (pliku PCKS-12 klucza prywatnego i publicznego).
11. Docelowo zakłada się uruchomienie oddzielnego medium do dystrybucji haseł za pośrednictwem bramki SMS. Hasła będą wysyłane wiadomością SMS na zdefiniowany we wniosku nr telefonu

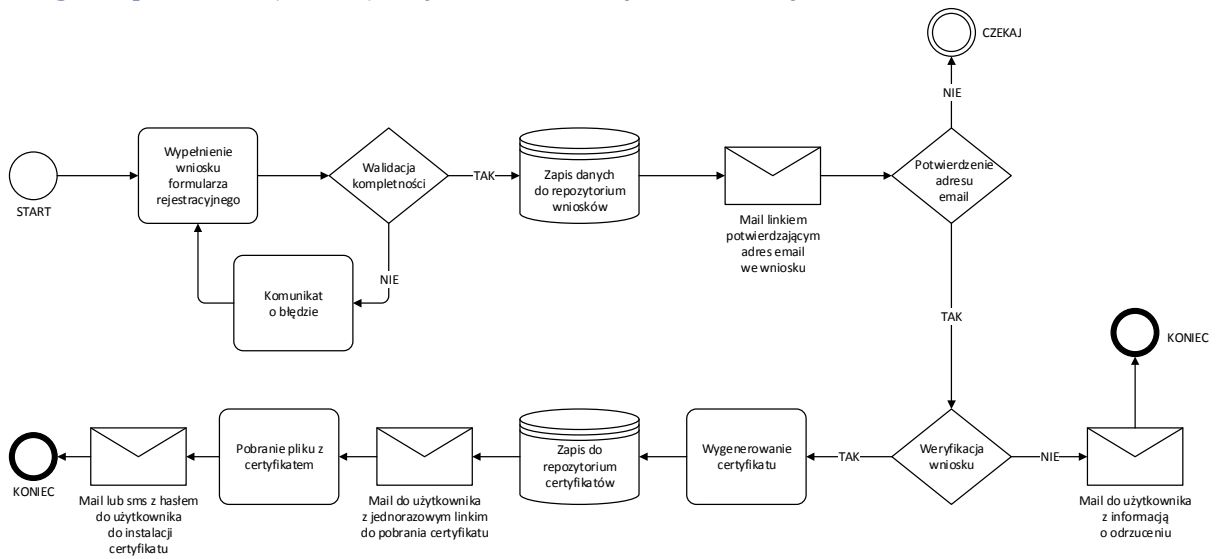
2.2 Proces odnowienia certyfikatu przez użytkownika

Certyfikat cyfrowy wystawiony przez UKNF ważny jest przez rok czasu. Na miesiąc przed wygaśnięciem certyfikatu do użytkowników na adresy email wysyłana będzie informacja o konieczności odnowienia certyfikatu wraz z jednorazowym linkiem do pobrania odnowionego certyfikatu w postaci pliku PCKS-12. Proces wygląda następująco:

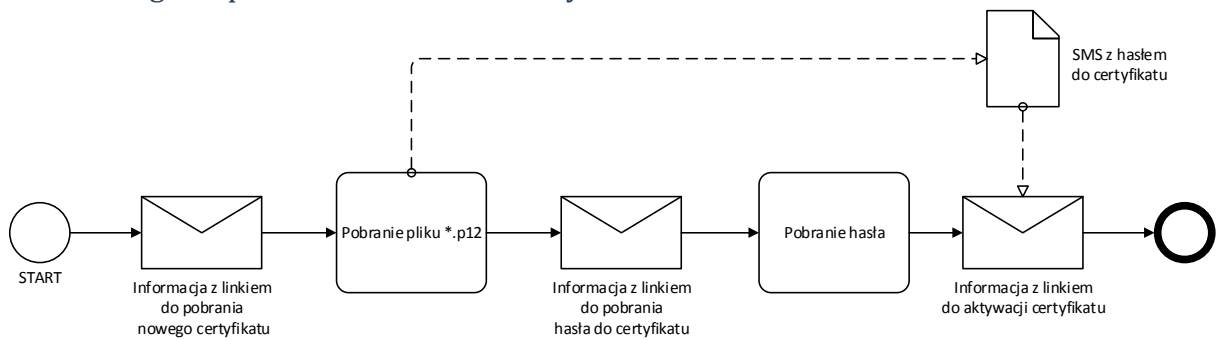
1. Użytkownik klika w link i pobiera plik.
2. Po pomyślnym pobraniu pliku system wyśle kolejną wiadomość e-mail z jednorazowym linkiem do pobrania hasła do pliku lub wysyła hasło wiadomością SMS na zdefiniowany we wniosku nr telefonu.
3. Po kliknięciu w link i pobraniu hasła system generuje kolejny jednorazowy link do aktywacji nowego certyfikatu.
4. Użytkownik instaluje certyfikat do swojej aplikacji klienckiej.
5. Kliknięcie w link aktywacyjny z pkt3. uruchomi proces aktywacji nowego certyfikatu. Poprzedni certyfikat pozostaje nadal aktywny do końca swojego okresu ważności.

2.3 Diagramy

2.3.1 Diagram procesu rejestracji użytkownika i uzyskania certyfikatu



2.3.2 Diagram procesu odnowienia certyfikatu



2.4 Architektura aplikacji

Poniżej znajduje się poglądowy schemat połączeń pomiędzy elementami infrastruktury.

