System eWUS

Opis interfejsu dostępowego

v. 1.1

Warszawa 2012

Wprowadzenie

Przedstawiony dokument opisuje interfejs dostępowy z wykorzystaniem usług sieciowych, w oparciu o mechanizm WSBroker, umożliwiający sprawdzenie z systemie eWUS pojedynczego statusu uprawnienia do świadczeń dla wybranego świadczeniobiorcy.

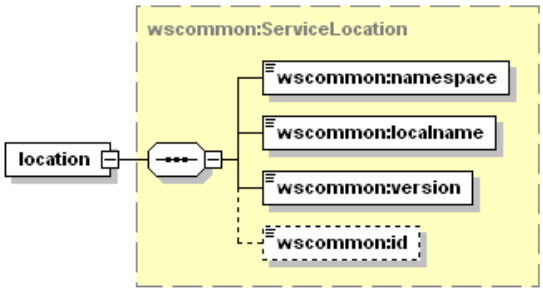
Opis ogólnego mechanizmu obsługi komunikatów (WSBroker)

Proces przekazywania komunikatów pomiędzy klientem, a OW NFZ jest mechanizmem wymiany danych pracującym w ogólnej sieci publicznej. Z uwagi na charakter przesyłanych danych (czyste dane tekstowe – XML oraz dane binarne – pliki w różnych formatach) zastosowano mechanizm wymiany danych oparty na usługach sieciowych (WS) z wykorzystaniem mechanizmu MTOM do przesyłania danych binarnych.

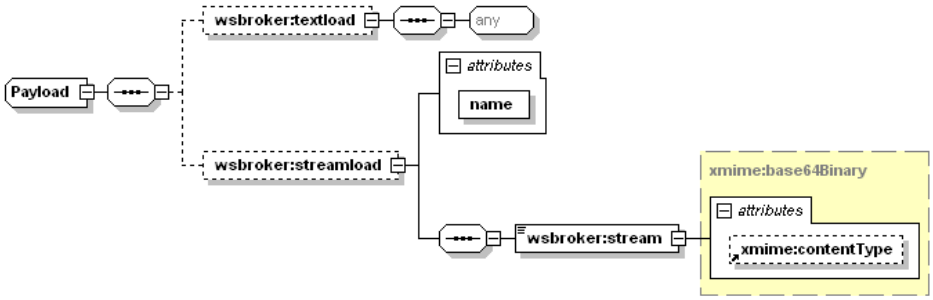
Uwzględniając fakt, że wymiana danych będzie odbywała się w środowisku publicznej sieci internetowej, mechanizm został oparty na następujących założeniach:

- Wykorzystanie protokołu HTTPS (zabezpieczenie danych na poziomie transmisji) jako podstawowego mechanizmu transportu dla komunikatu – klucz 1024 lub 2048 bitów.
- Wprowadzenie stanowości komunikatów – kolejne wywołania usług mogą pracować w ramach wspólnej sesji z możliwością zapamiętania stanu usługi.
- Umożliwienie kontroli uprawnień w oparciu o serwer autoryzacyjny KAAS stosowany w OW NFZ do autoryzowania operatorów korzystających z systemu Portal SZOI. Konto operatora wraz z wszelkimi ograniczeniami wykorzystywane w aplikacjach WWW może być wykorzystane przy dostępie do dowolnej usługi wymagającej ograniczonego dostępu na takich samych zasadach jak dla innych aplikacji.
- Przekazywanie danych binarnych w taki sam sposób, jak danych tekstowych. Podział następuje na poziomie mechanizmu transportu, a nie pliku opisowego. Zastosowanie mechanizmu MTOM w połączeniu z protokołem HTTPS pozwala na przesyłanie dużych załączników (do kilkuset megabajtów) poza samym komunikatem XML, co znacznie zwiększa wydajność rozwiązania, nie powodując dodatkowego przetwarzania pliku XML (zmniejszenie zapotrzebowania zasobów po stronie systemu przetwarzającego dokument XML) w stosunku do umieszczenia danych binarnych wprost w strukturze dokumentu XML (Base64).
- W celu optymalizacji procesu przetwarzania i budowania komunikatów wprowadzono specjalną super-usługę dostępową (broker), której zadaniem jest opakowanie danych związanych z transportem i funkcjami dodatkowymi w jednolity sposób, pozostawiając użytkownikowi skupienie się na szczegółach związanych z daną dziedziną. Komunikaty są przetwarzane w jednolity sposób i udostępniają taki sam interfejs dla obsługi błędów. Udostępnione usługi są wywoływane z zachowaniem takiego samego protokołu ich obsługi.
- Do identyfikacji poszczególnych komunikatów wykorzystywane są następujące mechanizmy:
    - **Identyfikator schematu dziedzinowego** – określa grupę akcji związaną z daną dziedziną (dowolny ciąg znaków, przyjmuje się nazwę schematu XML wykorzystywaną do opisania danych dziedzinowych). Opisuje grupę usług udostępnionych dla danej dziedziny.

- **Identyfikator akcji w ramach schematu dziedzinowego** – pozwala na wybór akcji pracującej na takiej samej dziedzinie danych. Jest to odpowiednik funkcji w programie, pozwala na dowolne wywołanie usługi z danej grupy.
- **Identyfikator wersji** – pozwala dodatkowo identyfikować sposób obsługi dla wybranej akcji w związku ze zmianą sposobu obsługi (taki mechanizm pozwala to na współistnienie wielu klientów podczas aktualizacji oprogramowania na serwerze w celu bezpiecznej zmiany mechanizmu obsługi).
- **Identyfikator komunikatu** – unikalny techniczny identyfikator komunikatu pozwalający na pełną identyfikację komunikatu w systemie klienta (gdy wymagany).



- Do przekazywania danych dziedzinowych zostały przewidziane dwa poziomy:
  - **Dane tekstowe** – zgodne z typem **any** (XML Schema). W tej sekcji mogą zostać umieszczone dowolne dane spełniające wymogi komunikatu XML. W celu zachowania pewnego protokołu i uniknięcia niejednoznaczności interpretacji danych, każdy taki komunikat wewnętrzny musi posiadać zdefiniowaną przestrzeń nazw. Taki sposób zapisu definicji w pliku WSDL pozwala w przyszłości na przekazywanie dowolnych komunikatów zgodnych z formatem XML bez konieczności jakiejkolwiek przebudowy mechanizmu transportowego.
  - **Dane binarne** – dowolne dane strumieniowe (automatycznie kodowane na format wymagany przez mechanizm transportowy) zgodne z typem xmime:base64Binary. W przypadku przekazywania danych binarnych przyjęto założenie, że należy określić nazwę pliku z danymi w celu optymalizacji procesu przetwarzania. W ten sposób mogą być transportowane całe raporty wewnętrzne bez jakiejkolwiek ingerencji w ich zawartość. Zaleca się, aby wszelkie dane przekazywane w ten sposób zostały wcześniej poddane procesowi pakowania (format ZIP), co pozwala naturalnie przekazywać w jednym polu nazwę pliku z archiwum, a w drugim samego archiwum. W celu ujednolicenia sposobu obsługi zakłada się, że komunikat może zawierać ci najwyżej jeden zestaw danych binarnych. W celu przekazania wielu osobnych elementów w jednym komunikacie należy je zapisać we wspólnym archiwum i odpowiednio zinterpretować w lokalnej klasie zdefiniowanej dla obsługi konkretnej usługi.



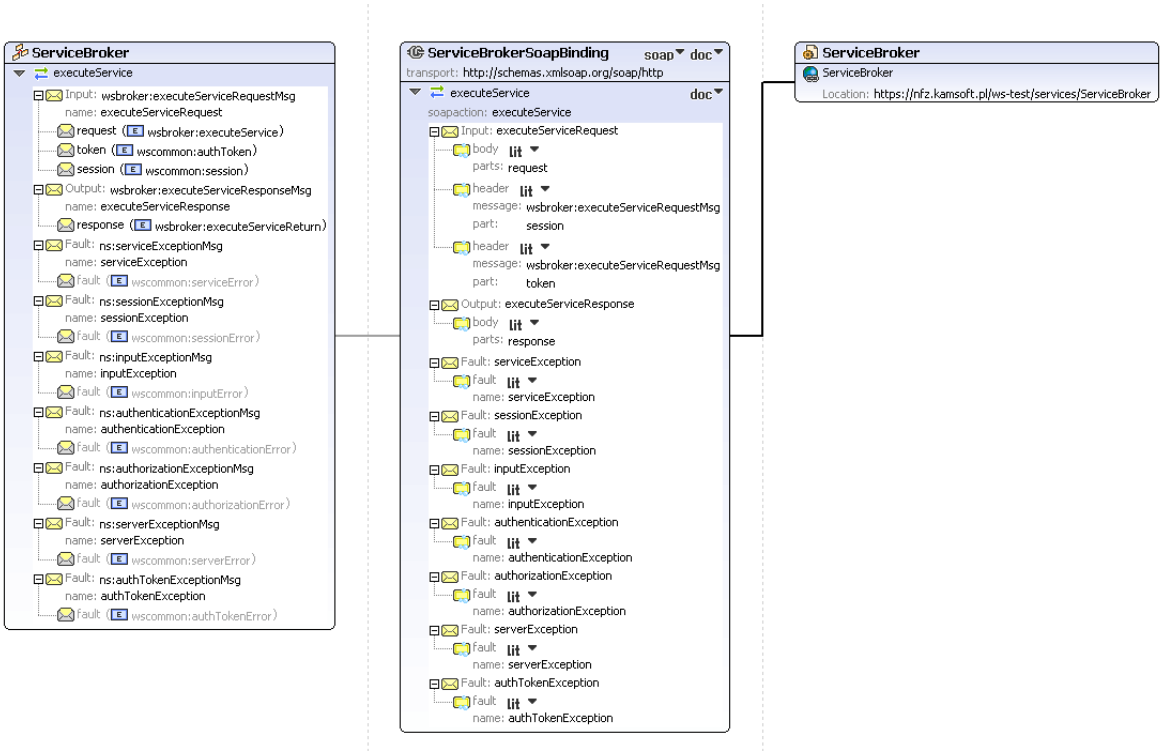
- Wykorzystanie danego poziomu przekazywania danych jest zależne jedynie od sposobu implementacji obsługi danego komunikatu. W jednym komunikacie mogą wystąpić jednocześnie dane tekstowe i binarne.
- W celu unifikacji obsługi sytuacji awaryjnych wprowadzono predefiniowany mechanizm obsługi błędów na każdym z poziomów obsługi komunikatu. W celu unifikacji zachowania ze światem zewnętrznym mechanizm tez został dodany do definicji usługi (WSDL). Mechanizm ten jest dostępny na poziomie warstwy transportowej, co automatycznie unifikuje obsługę komunikatów błędów dla wszystkich usług korzystających z systemu.
- Błędy generowane przez mechanizm obsługi komunikatów zostały podzielone na następujące typy:
    - **AuthenticationException** – brak uwierzytelnienia – wymagane jest ponowne logowanie do systemu.
    - **AuthorizationException** – brak autoryzacji - wymagane jest nadanie odpowiedniego uprawnienia w systemie autoryzacyjnym i ponowne logowanie do systemu.
    - **ServiceException** – błąd generowany przez serwis (do dowolnego wykorzystania przez klasę obsługującą komunikat). Dla każdego z komunikatów zostanie dostarczona lista standardowych błędów mogących się pojawić podczas procesu obsługi komunikatu. Są to tylko te błędy, które zostały precyzyjnie zdefiniowane w procesie obsługi i stanowią jego integralną część. Błędy, które nie zostały przewidziane w procesie obsługi są klasyfikowane jako błędy typy ServerException.
    - **AuthTokenException** – brak lub niepoprawny token autoryzacyjny – wymagane ponowne logowanie do systemu,
    - **ServerException** – nieznany błąd serwera, jest to błąd na poziomie wewnętrznym serwera udostępniającego usługi, który nie został przewidziany do obsłużenia w danym procesie przetwarzania.
    - **InputException** – błąd w parametrach wejściowych dla komunikatu, spowodowany niepoprawną wartością wymaganego parametru wejściowego koniecznego do zapewnienia prawidłowego przetworzenia komunikatu.
    - **SessionException** – błąd sesji - wymagane ponowne logowanie do systemu.

- Implementacja podstawowej obsługi błędów po stronie klienta pozwala na automatyzację obsługi, np. w przypadku wygaśnięcia sesji może zostać automatycznie uruchomiony proces ponownego logowania do systemu w celu kontynuacji rozpoczętego procesu obsługi danego zagadnienia biznesowego.
- W przypadku wykorzystania mechanizmów autoryzacyjnych udostępnianych przez klasy obsługi komunikatów należy za każdym razem przekazywać identyfikatory sesji i identyfikator tokenu autoryzacyjnego otrzymane podczas pierwszego logowania do

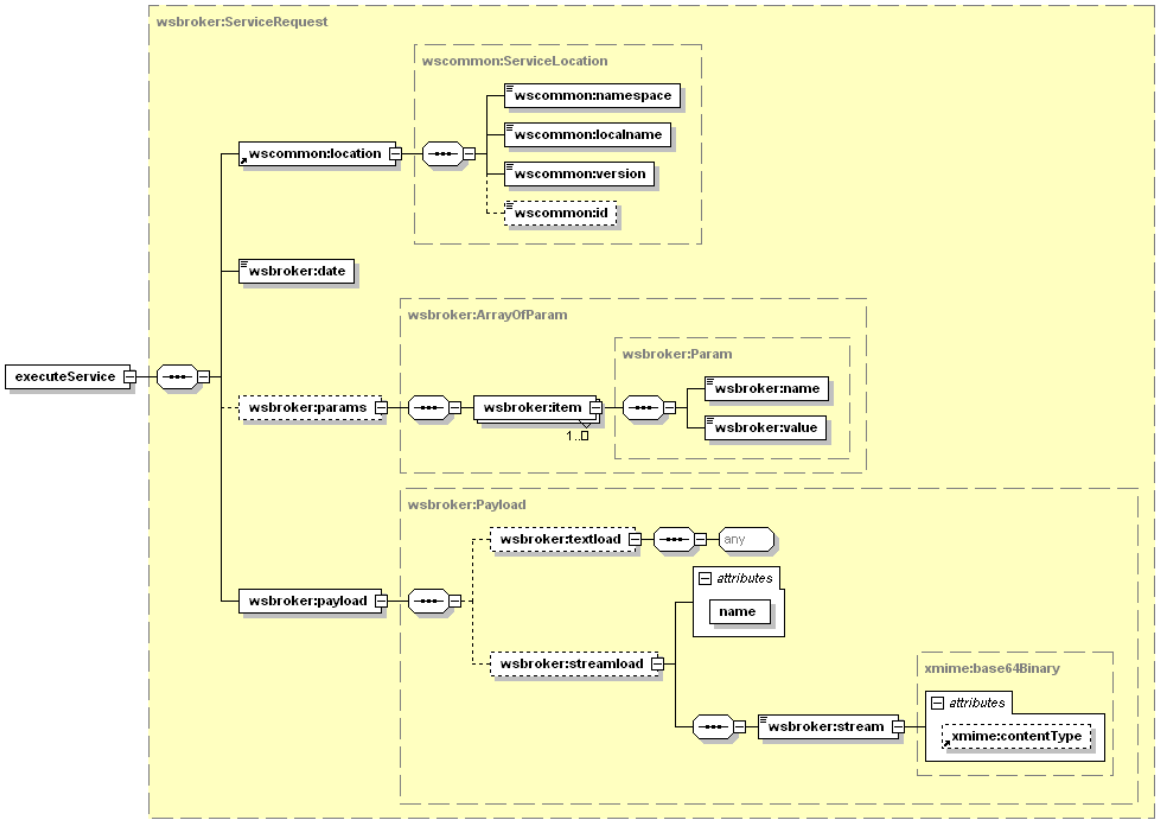
systemu w nagłówku każdego komunikatu przesyłanego do serwera – w przeciwnym wypadku zostanie wygenerowany odpowiedni wyjątek (brak tokenu autoryzacyjnego).

- Podczas pracy z mechanizmem autoryzacji wymagana jest aktywna sesja na poziomie warstwy transportowej, sesja te jest tworzona automatycznie podczas operacji logowania.
- Możliwe jest zastosowanie dowolnych mechanizmów związanych z bezpieczeństwem wymiany informacji w zależności od dodatkowych wymagań zewnętrznych (np. podpisywanie komunikatów, szyfrowanie komunikatów, itp.) zarówno na poziomie transportowym (WSBroker), jak i na poziomie samego ładunku.

Opis usługi brokera



Przykładowy komunikat brokera



Wymiana informacji o statusie uprawnienia do świadczeń pomiędzy świadczeniodawcą, a NFZ

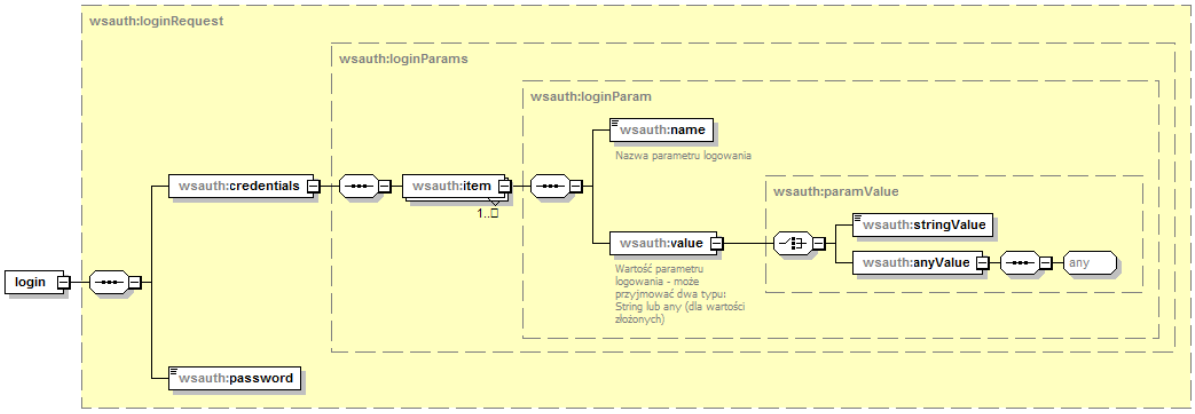
Mechanizm transportowy do wymiany informacji

Jako mechanizm transportowy został wykorzystany opisany powyżej broker komunikatów, dostępny za pośrednictwem protokołu HTTPS w publicznej sieci Internet. W celu zachowania jednolitych standardów bezpieczeństwa, dostęp z poziomu klienta usług musi zostać poprzedzony odpowiednim procesem logowania w celu uwierzytelnienia i autoryzacji do poszczególnych elementów systemu.

Po poprawnym zalogowaniu klient otrzymuje identyfikator sesji klienta i identyfikator sesji autoryzacyjnej. Identyfikatory te muszą być przekazywane w każdym następnym żądaniu do serwera (identyfikatory muszą zostać umieszczone w nagłówku komunikatu). W połączeniu z protokołem HTTPS i bezpośrednim połączeniem klienta z serwerem usług, stanowi podstawę do bezpiecznej wymiany danych pomiędzy klientem, a serwerem.

W opisywanym przypadku, do parametrów identyfikacyjnych operatora należy dodatkowo dodać identyfikator OW NFZ właściwego ze względu na posiadane konto dostępowe wraz z właściwym identyfikatorem świadczeniodawcy w lokalnym OW NFZ.

Budowa standardowego komunikatu logowania



Z uwagi na wykorzystanie istniejących identyfikatorów operatorów z poziomu OW NFZ, zakres danych wymaganych do zalogowania zależy od typu operatora (świadczeniodawca, lekarz) oraz od kodu OW NFZ. Podstawowe zależności zostały zawarte w poniższej tabeli.

Kod OW NFZ	Typ operatora	Wymagane parametry
01,04,05,06,08,09,11,12	Lekarz	domain={id_OW} type=LEK login
02,03,07,10,13,14,15,16	Lekarz	domain={id_OW} login
01,04,05,06,08,09,11,12	Świadczeniodawca	domain={id_OW} type=SWD idntSwd={id_SWD} login
02,03,07,10,13,14,15,16	Świadczeniodawca	domain={id_OW} login

Przykłady komunikatów logowania zostały zawarte w dołączonym projekcie testowym – po jednym dla reprezentanta OW NFZ z powyższych grup (TestSuite OW01 LEK, TestSuite OW01 SWD, TestSuite OW15 LEK, TestSuite OW15 SWD). Opis znaczenia poszczególnych parametrów logowania i ich dopuszczalne wartości został zawarty w pliku XSD dla typu http://xml.kamsoft.pl/ws/kaas/login_types (do pobrania z serwera dostarczającego usługę zgodnie z opisem w pliku WSDL).

Opis parametrów konfiguracyjnych komunikatu brokera dla sprawdzenia statusu uprawnienia do świadczeń

Na potrzeby mechanizmu obsługi wymiany danych o statusie ubezpieczenia został opracowany następujący interfejs opisujący usługę, który będzie wykorzystywany do komunikacji pomiędzy świadczeniodawcą a NFZ.

Lista rozkazów dla usługi sprawdzającej uprawnienie do świadczeń	
Przestrzeń pracy	**nfz.gov.pl/ws/broker/cwu**
Wersja	**1.0**

Lista zadań

checkCWU	Sprawdzenie statusu uprawnienia do świadczeń danego świadczeniobiorcy w systemie CWU – dane zapytania dodawane są w postaci komunikatu xml zgodnego z definicją xsd (status_cwu.xsd)

Wywołanie usługi

Parametry

Brak parametrów

Ładunek

Text	Pytanie o status świadczeniobiorcy zgodnie ze schemą xsd (status_cwu_pyt)
Stream	Brak

Odpowiedź z usługi

Parametry

Brak parametrów

Ładunek

Wariant I	Przekazane dane zostały poprawnie przetworzone przez system.
Text	Komunikat odpowiedzi zgodny z definicją zawartą w pliku XSD (status_cwu_odp).
Stream	Brak

Lista obsługiwanych błędów

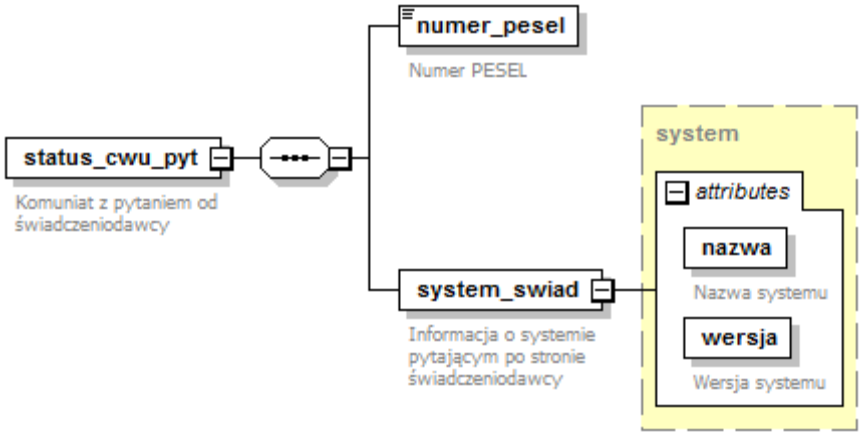
Typ	Opis
InputException	Błąd w parametrach wejściowych dla komunikatu, szczegółowy opis błędu zawarty jest w sekcji <messages> standardowego opisu błędu.
ServiceException	Błąd generowany przez serwis w przypadku wystąpienie planowanych sytuacji wyjątkowych
ServerException	Nieznany błąd serwera (błąd na poziomie wewnętrznym serwera udostępniającego usługi).
AuthorizationException	Brak uprawnienia - wymagane jest nadanie odpowiedniego uprawnienia w systemie autoryzacyjnym i ponowne logowanie do systemu.

AuthTokenException	Brak lub niepoprawny token autoryzacyjny – wymagane ponowne logowanie do systemu
SessionException	Błąd sesji - wymagane ponowne logowanie do systemu
AuthenticationException	Brak autentykacji – wymagane jest ponowne logowanie do systemu

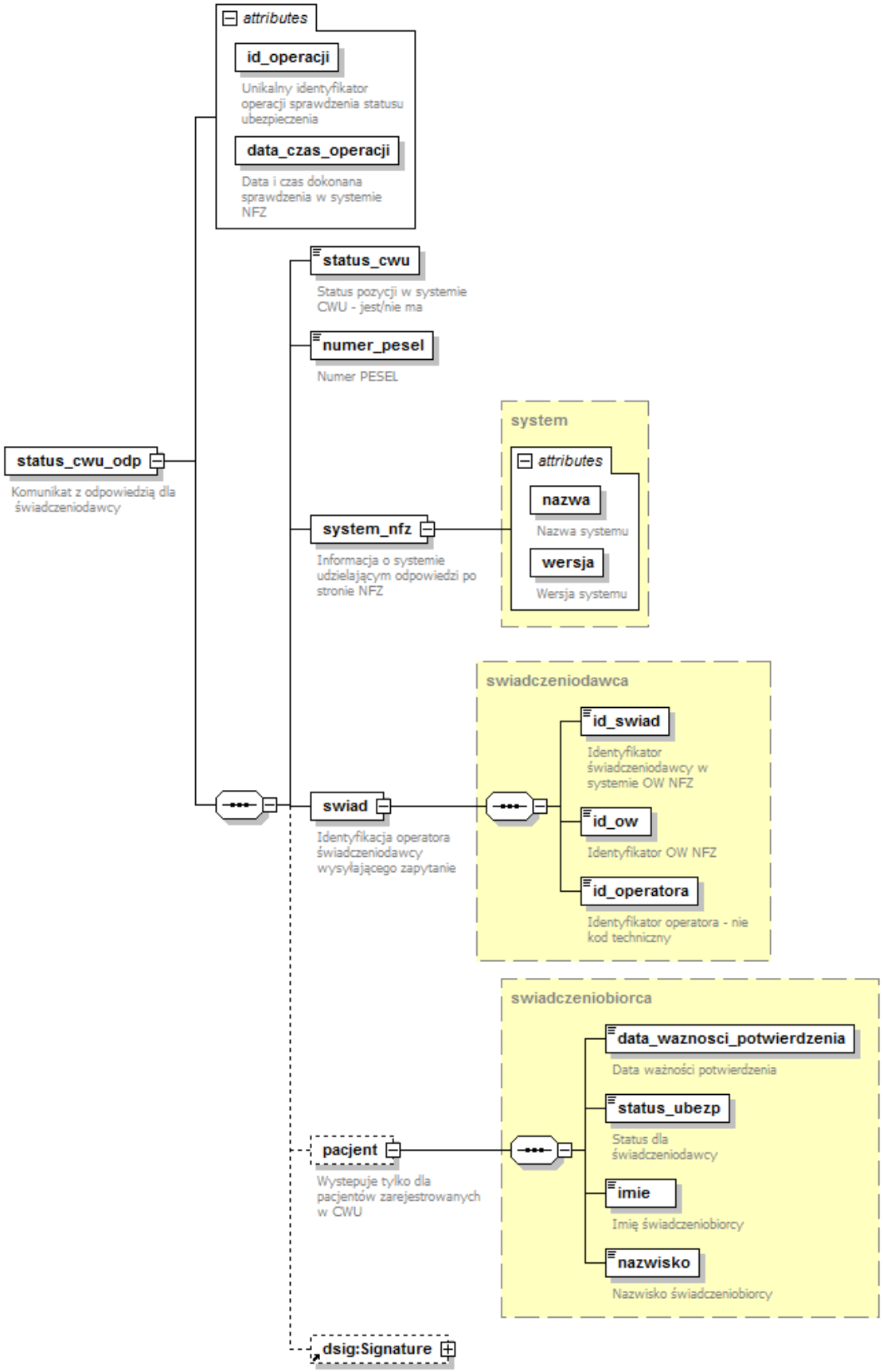
Wymiana informacji o statusie uprawnienia do świadczeń

Budowa komunikatów wewnętrznych dla usługi

Komunikat z pytaniem status_cwu_pyt



Komunikat z odpowiedzią status_cwu_odp



Opis procesu wymiany danych pomiędzy świadczeniodawcą a NFZ

Algorytm sprawdzenia statusu uprawnienia do świadczeń przez świadczeniodawcę w systemie NFZ	
1.	Program po stronie świadczeniodawcy loguje się do systemu eWUS (za pośrednictwem udostępnionej usługi autoryzacyjnej).
2.	Tworzona jest sesja autoryzacyjna, która jest przekazywana do klienta w odpowiedzi na poprawny proces zalogowania. W pozostałych przypadkach zwracana jest informacja o błędzie (kod + opis).
3.	Klient wysyła żądanie **[checkCWU]** wraz z parametrami opisującymi zapytanie o status uprawnienia do świadczeń – zgodnie z przyjętym komunikatem oraz dane sesji autoryzacyjnej uzyskane w procesie logowania.
4.	Serwer zwraca odpowiedź zgodni z przyjętym formatem odpowiedzi.
5.	Świadczeniodawca powtarza operacje z punktu 3 do czasu sprawdzenia statusu wszystkich wymaganych świadczeniobiorców.
6.	Klient po stronie świadczeniodawcy kończy sesję z serwerem poprzez wywołanie żądania **[logout]** - wylogowanie.

Przykład wywołania usługi

W celu przeprowadzenia testu opisanego powyżej procesu, w katalogu z dokumentacją został dołączony plik z projektem testowym dla aplikacji soapUI. Należy uruchomić przygotowany w projekcie TestCase – całość operacji zostanie wykonana automatycznie (logowanie – sprawdzenie statusu - wylogowanie) wraz z odpowiednim przepisywaniem identyfikatorów sesji i tokenu autoryzacyjnego z usługi logowania. Wersja testowa aplikacji dostępna jest na stronie http://www.soapui.org .

Na potrzeby testu zostały przygotowane trzy przypadki testowe (w ramach każdego zestawu testowego TestSuite dla poszczególnych typów operatorów):

1. Osoba o podanym PESEL posiada uprawnienie do świadczeń (dowolny parzysty numer PESEL) - ***TestCase (osoba uprawniona)***.
2. Osoba o podanym PESEL nie posiada uprawnienia do świadczeń (dowolny nieparzysty numer PESEL) - ***TestCase (osoba bez uprawnień)***.
3. Osoba o podanym PESEL nie występuje w bazie CWU (tylko dla numeru PESEL 01010153201) - ***TestCase (brak osoby w CWU)***.

Uwaga: Wszystkie numery PESEL wykorzystane do testów zostały wygenerowane w sposób losowy zgodnie z przyjętym algorytmem.

Definicje usług

Pliki z opisem usług (WSDL) wraz z niezbędnymi plikami dodatkowymi (XSD) są dostępne do pobrania bezpośrednio z serwera udostępniającego usługi. Aktualny adres serwera zostanie opublikowany na stronach Centrali NFZ (nfz.gov.pl).

Załączniki

Opis komunikatów pytania i odpowiedzi dotyczących statusu uprawnienia do świadczeń
Pliki dodatkowe:

- ***status_cwu.xsd*** – definicja opisująca formaty wymiany danych
- **xmldsig-core-schema.xsd** – definicja pomocnicza – podpis
- **ServiceBrokerCwuAuth2.xml** – plik z projektem testowym dla aplikacji soapUI w celu przetestowania usługi

.

Komunikat zapytania o status uprawnienia do świadczeń

Poziom w hierarchii	Element	Atrybut	Krot-ność	Format [wart. dom.]	Opis	Dodatkowe wyjaśnienia, ograniczenia i zależności
0	status_cwu_pyt				Komunikat zapytania	
1	numer_pesel		1	11 znaków	Numer PESEL	
1	system_swiad		1		Informacja o systemie pytającym po stronie świadczeniodawcy	
		nazwa	1	do 15 znaków	Nazwa systemu	
		wersja	1	do 15 znaków	Wersja systemu	

Komunikat odpowiedzi zawierający informacje o statusie uprawnienia do świadczeń

Poziom w hierarchii	Element	Atrybut	Krotność	Format [wart. dom.]	Opis	Dodatkowe wyjaśnienia, ograniczenia i zależności
0	status_cwu_odp				Komunikat odpowiedzi	
		data_czas_operacji	1	data+czas	Data i czas dokonana sprawdzenia w systemie NFZ	
		id_operacji	1	od 8 do 17	Unikalny identyfikator operacji	

Poziom w hierarchii	Element	Atrybut	Krotność	Format [wart. dom.]	Opis	Dodatkowe wyjaśnienia, ograniczenia i zależności
				znaków	sprawdzenia statusu ubezpieczenia	
1	status_cwu		1	1 znak	Status pozycji w systemie CWU	0 – nie ma 1 – jest
1	numer_pesel		1	11 znaków	Numer PESEL	
1	system_nfz		1		Informacja o systemie udzielającym odpowiedzi po stronie NFZ	
		nazwa	1	do 15 znaków	Nazwa systemu	
		wersja	1	do 15 znaków	Wersja systemu	
1	swiad		1		Identyfikacja operatora świadczeniodawcy wysyłającego zapytanie	
2	id_swiad		1	do 16 znaków	Identyfikator świadczeniodawcy w systemie OW NFZ	
2	id_ow		1	2 znaki	Identyfikator OW NFZ	01 - 17
2	id_operatora		1	do 15 znaków	Identyfikator operatora	
1	pacjent		0-1		Informacja o świadczeniobiorcy	Element występuje tylko dla pacjentów zarejestrowanych w CWU status_cwu_odp/status_cwu = 1
2	data_waznosci _potwierdzenia		1	data	Data ważności potwierdzenia	
2	status_ubezp		1	1 znak	Status dla świadczeniodawcy	0 - brak uprawnień do świadczeń 1 - uprawniony do świadczeń

Poziom w hierarchii	Element	Atrybut	Krotność	Format [wart. dom.]	Opis	Dodatkowe wyjaśnienia, ograniczenia i zależności
2	imie		1	do 20 znaków	Imię świadczeniobiorcy	
2	nazwisko		1	do 40 znaków	Nazwisko świadczeniobiorcy	
1	Signature		1		Element zawierający unikalny podpis komunikatu odpowiedzi	