Zasady korzystania z usługi sieciowej Webservice KNF

data: 2018-10-22
wersja: 1.2

Spis treści

1 Słownik pojęć

Użytkownik – użytkownik usługi sieciowej Webserwis KNF

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

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

2 Wstęp

Usługa ***WebService KNF*** jest uniwersalnym, bezpiecznym kanałem do wymiany informacji pomiędzy KNF a podmiotami zewnętrznymi (użytkownikami usługi). Usługa umożliwia przesyłanie do KNF ustrukturyzowanych informacji w postaci pliku o ściśle zdefiniowanych formacie i nazwie oraz odebranie informacji zwrotnej dotyczącej przesłanych danych.

Jest to wystandaryzowana usługa sieciowa (Web Service) w architekturze SOA, umożliwiająca podmiotom zarówno integrację z własnymi systemami informatycznymi jak i korzystanie z dowolnego klienta umożliwiającego komunikację zgodną ze standardem WSDL.

3 Dostęp do usługi *Webserwis KNF*

Dostępu do usługi wymaga posiadania ważnego certyfikatu cyfrowego wystawiony przez centrum certyfikacji CA KNF. Proces pozyskania certyfikatu przez użytkownika, jego odnowienia a także unieważnienia opisany jest w dokumentach na stronie: https://www.knf.gov.pl/dla_rynku/MiFIR/raportowanie_transakcji_art_26_MiFIR/Dostep_do_uslugi_sieciowej_Webservice_KNF

4 Proces korzystania z usługi

Przesłanie pliku z wykorzystaniem usługi ***Websewis KNF*** wymaga realizacji poniższych kroków:

a) Użytkownik łączy się z sieci Internet z wykorzystaniem bezpiecznego protokołu HTTPS pod adresem usługi sieciowej (adres jest wskazany w załączniku do niniejszego dokumentu). W procesie tym następuje uwierzytelnienie użytkownika za pomocą certyfikatu cyfrowego, w tym weryfikacja aktualnego statusu certyfikatu.

b) Po poprawnej autentykacji użytkownik uzyskuje dostęp do usługi, w tym szczegółowe informacje w postaci pliku WSDL potrzebne do zdalnego wywołania metod komunikacyjnych kanału.

c) Użytkownik, wykorzystując dowolnego klienta usługi WSDL, konstruuje zapytanie w standardzie SOAP i wywołuje właściwą metodę usługi w zależności od rodzaju informacji, którą zamierza przesłać. Nazwy, formaty i terminy przesyłania plików muszą być zgodne z obowiązującymi regulacjami.

d) Usługa w trybie online:
   - dokonuje autoryzacji użytkownika weryfikując, na podstawie rodzaju i parametrów wejściowych wywoływanej metody, czy użytkownik posiada wymagane uprawnienia do usługi,
   - dokonuje wstępnych walidacji technicznych przesłanych informacji, w tym poprawność nazwy pliku w przesyłce.

e) Jeśli autoryzacja i walidacja techniczna zakończyły się poprawnie w komunikacie zwrotnym usługi ***Webserwis KNF*** użytkownik otrzymuje odpowiedź zawierającą:
   - nazwę przesłanego pliku,
   - datę i czas odebrania danych przez KNF,
   - unikalny identyfikator przesyłki - jest on niezbędny do późniejszego pobrania wyników dalszego przetwarzania pliku w KNF,
   - status przesyłki - ***Przyjęta do przetwarzania***.

f) Jeśli autoryzacja lub walidacja zakończyły się błędem w komunikacie zwrotnym usługi ***Webserwis KNF*** użytkownik otrzymuje odpowiedź zawierającą:
   - Nazwę przesłanego pliku,
   - datę i czas przesłania danych do KNF,
   - status przesyłki - ***Odrzucona***
   - opis i numer błędu.

g) Przesłane dane podlegają dalszemu przetwarzaniu w KNF. Po zakończeniu procesu przetwarzania użytkownik otrzymuje powiadomienie mailowe (na wskazany we wniosku o dostęp adres techniczny) o zakończeniu przetwarzania zawierający informacje o:
   - wyniki przetwarzania, w tym listę błędów jeśli wynik przetwarzania jest negatywny,
   - udostępnieniu do pobrania pliku potwierdzenia.

Pobieranie pliku potwierdzenia odbywa się z wykorzystaniem tej samej usługi sieciowej ***Webserwis KNF***. W wywoływanej metodzie należy podać parametr zawierający unikalny identyfikator przesyłki otrzymany w komunikacie zwrotnym usługi (por. pkt 5e). Nazwa i format pliku potwierdzenia jest zgodny z wymogami ESMA.

h) Dodatkowe szczegóły techniczne usługi, w tym sposób podłączenia, opisane są w załączniku do niniejszego dokumentu.

5 Standardy techniczne i bezpieczeństwo

5.1 Zastosowane standardy techniczne

Udostępniona przez KNF usługa sieciowa jest zgodna z poniższymi standardami:

- WSDL (https://www.w3.org/TR/wsdl) - w zakresie definicji usługi,
- SOAP (https://www.w3.org/TR/soap/) - w zakresie protokołu komunikacyjnego usługi,
- MTOM (https://www.w3.org/TR/soap12-mtom/) - w zakresie transmisji plików binarnych.

5.2 Bezpieczeństwo

Całość komunikacji pomiędzy użytkownikiem a KNF zabezpieczona jest kanałem szyfrowanym z wykorzystaniem protokołu HTTPS.

5.3 Dostęp do usługi

Dostęp do usługi chroniony jest poprzez uwierzytelnienie za pomocą certyfikatu cyfrowego w standardzie X.509, wygenerowanego przez centrum certyfikacji KNF. Certyfikaty są ważne przez rok.

Klucz prywatny i publiczny użytkownika składowany jest w pliku archiwum PCKS-12 służącym do przechowywania kluczy kryptograficznych. Archiwum jest szyfrowane i chronione hasłem.

Plik PCKS-12 będzie dystrybuowany przez sieć Internet w postaci jednorazowego linku przesłanego na podany we wniosku o dostęp adres e-mail do kontaktów – w przypadku podania więcej niż 1 adresu w polu e-mail do kontaktów link zostanie przesłany na adres podany jako pierwszy. Użytkownik klikając w link pobierze certyfikat, po czym link stanie się nieaktywny.

Instalacja certyfikatu na stacji użytkownika wymaga podania hasła. Hasło do instalacji certyfikatów z pliku PCKS-12 będzie przesyłane - po pobraniu certyfikatu - w formie linku jednorazowego w wiadomości e-mail wysłanej na ten sam adres co certyfikat.

W przypadku konieczności ponownego pobranie certyfikatu konieczne będzie wygenerowanie nowego linku.

W procesie uwierzytelniania użytkowników weryfikowana jest czy:

- wykorzystany do uwierzytelnienia w usłudze ***Webserwis KNF*** certyfikat, został wygenerowany z CA KNF
- certyfikat nie wygasł, nie został odwołany ani unieważniony
- użytkownik ma uprawnienia do korzystania z wywoływanej metody usługi

W przypadku nieprawidłowego uwierzytelnienia dostęp do usługi nie będzie możliwy.

5.4 Zasady postępowania z certyfikatem CA KNF

Certyfikaty wydawane przez CA KNF podlegają, w celu ich ochrony, podlegają poniższym zasadom:

a) Osoba pobierająca certyfikat jest odpowiedzialna za jego bezpieczne przechowywanie i udostępnianie do wykorzystania, w tym:
   - Zapewnienie bezpieczeństwa stacji roboczej, na której został zainstalowany certyfikat poprzez korzystanie z oprogramowania posiadających indywidualne ustawienia zgodne z aktualnymi międzynarodowymi standardami bezpieczeństwa IT. Należy zapewnić odpowiednie środki, w tym w szczególności ochronę przed wirusami i złośliwym oprogramowaniem, zapobiegające wykradaniu haseł, jak również procedury podnoszenia poziomu bezpieczeństwa oraz wprowadzania poprawek do oprogramowania. Należy regularnie aktualizować wszelkie takie środki i procedury.
   - Konta użytkownika korzystającego z certyfikatu na stacjach roboczych nie powinny mieć uprawnień administratora. Uprawnienia należy przyznawać zgodnie z zasadą „jak najmniejszych uprawnień".
   - Zapewnienie ciągłej ochronę systemów komputerowych używanych w celu dostępu przez Internet do systemu ***Webserwis KNF*** poprzez:
   - zapewnienie stałej ochrony systemów komputerowych i stacji roboczych przed nieuprawnionym dostępem – fizycznym i sieciowym – poprzez stosowanie przez cały czas zapory sieciowej (firewall) dla osłony systemów komputerowych i stacji roboczych przed danymi odbieranymi z Internetu, jak również stacji roboczych przed nieuprawnionym dostępem przez sieć wewnętrzną oraz umożliwiającej komunikowanie się na zewnątrz wyłącznie autoryzowanym programom.
   - regularną aktualizację i uzupełniane poprawkami zgodnie z najnowszą wersją. Dotyczy to w szczególności systemu operacyjnego, przeglądarki internetowej oraz dodatków.
   - ochronę wszystkich krytycznych wewnętrznych przepływów danych do stacji roboczych i z tych stacji przed ujawnieniem i szkodliwymi zmianami, w szczególności w razie przesyłania plików przez sieć.

b) Przechowywanie certyfikatów
   - certyfikat powinien być umieszczony zgodnie z wymaganiami przeglądarki Internetowej, np. w tzw. magazynie certyfikatów.
   - certyfikaty przechowywane w magazynie certyfikatów powinny być szyfrowane zgodnie z zalecaniami polityki bezpieczeństwa w organizacji podmiotu. W przypadku braku takich wytycznych certyfikat powinien być szyfrowany na zasadzie ogólnych zaleceń dla danego systemu operacyjnego wykorzystywanego przez podmiot nadzorowany.

c) Dla ograniczenia ryzyka dla swojego systemu informatycznego podmiot nadzorowany stale stosuje się do następujących zasad zarządzania:
   - ustalenie praktyki zarządzania użytkownikami zapewniającej zakładanie i utrzymywanie w systemie jedynie kont uprawnionych użytkowników, jak również utrzymywanie dokładnej i aktualnej listy uprawnionych użytkowników;

- porównywanie dziennego przepływu danych w celu wykrycia niezgodności pomiędzy autoryzowanym a faktycznym przepływem danych, zarówno wysyłanych, jak i otrzymanych.

d) Zaleca się ponadto:
   - organizowanie okresowych przeglądów stacji roboczych użytkowników kontrolujących stan przechowywania i zabezpieczenie certyfikatów uniemożliwiające ich eksportowanie poza wyznaczone stacje robocze.
   - aby w sposób ciągły ograniczać wychodzący przepływ danych ze stacji roboczych do stron mających największe znaczenie dla działalności podmiotu, jak również do stron koniecznych dla przeprowadzania uprawnionych i uzasadnionych aktualizacji oprogramowania
   - prowadzenie okresowych kontroli użytkowników w zakresie wykorzystywania certyfikatu.

Załącznik nr 1

instrukcja techniczna podłączenia do usługi Webserwis KNF

1 Adres usługi

Adres pod którym dostępna jest usługa to:

Środowisko produkcyjne: https://ws.knf.gov.pl

Środowisko testowe: https://test-ws.knf.gov.pl/

2 Uwierzytelnienie za pomocą certyfikatu

Każdy użytkownik usługi (podmiot zewnętrzny) otrzyma wygenerowany certyfikat x.509 (klucz prywatny i publiczny) w postaci pliku p12.
Plik ten jest chroniony hasłem.

3 Wybór klienta usługi

W celu połączenia się z usługą należy skorzystać z dowolnego klienta SOAP, należy jednak wcześniej tak skonfigurować klienta aby mógł nawiązać bezpieczną sesję SSL z serwerem za pomocą dołączonego certyfikatu cyfrowego.

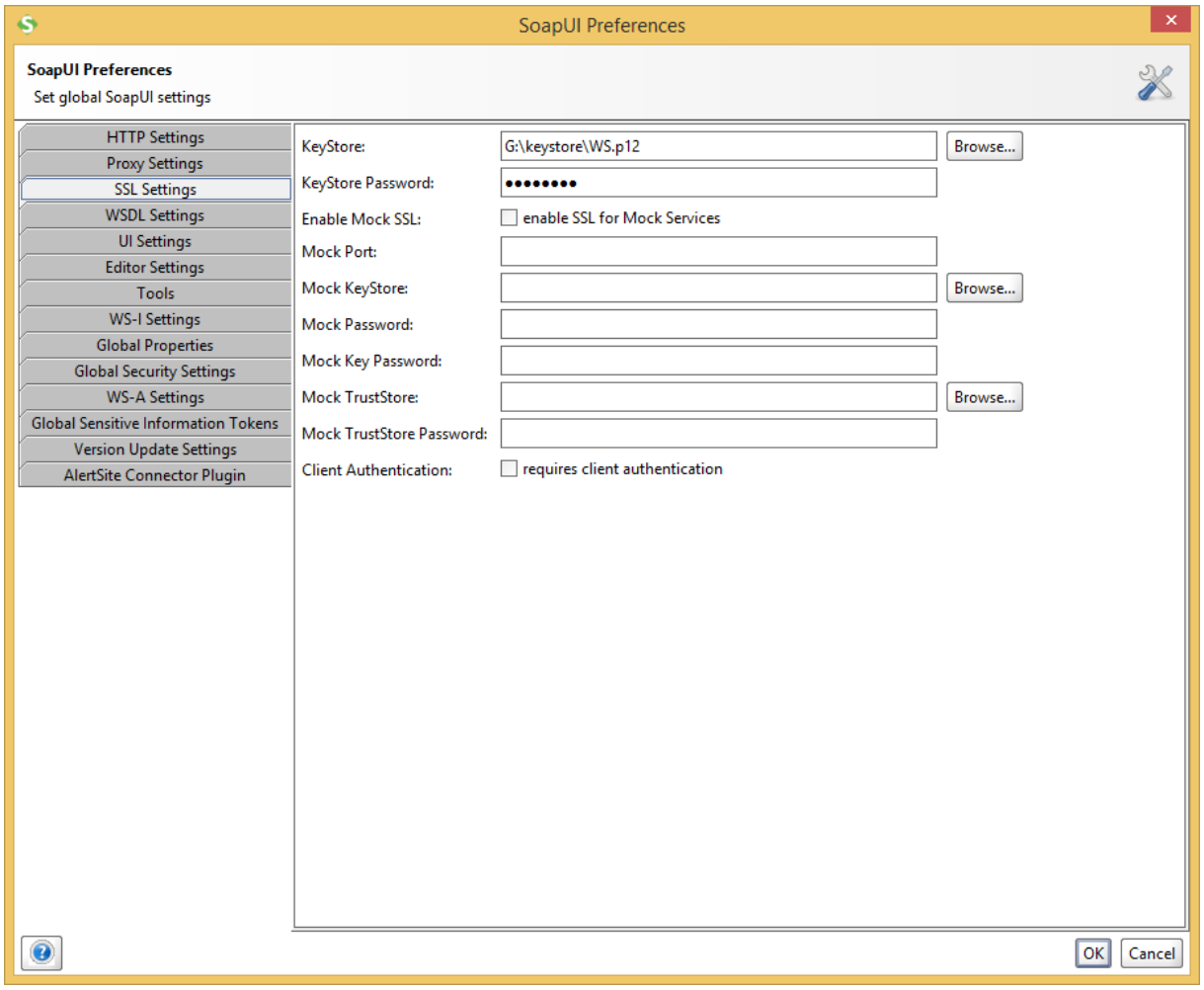
4 Przykład konfiguracji klienta SOAP-UI

Aplikacja SOAP-UI (https://www.soapui.org/downloads/soapui.html) w wersji OpenSource jest dostępna za darmo do pobrania i umożliwia komunikację i testowanie usług SOAP Web Service.

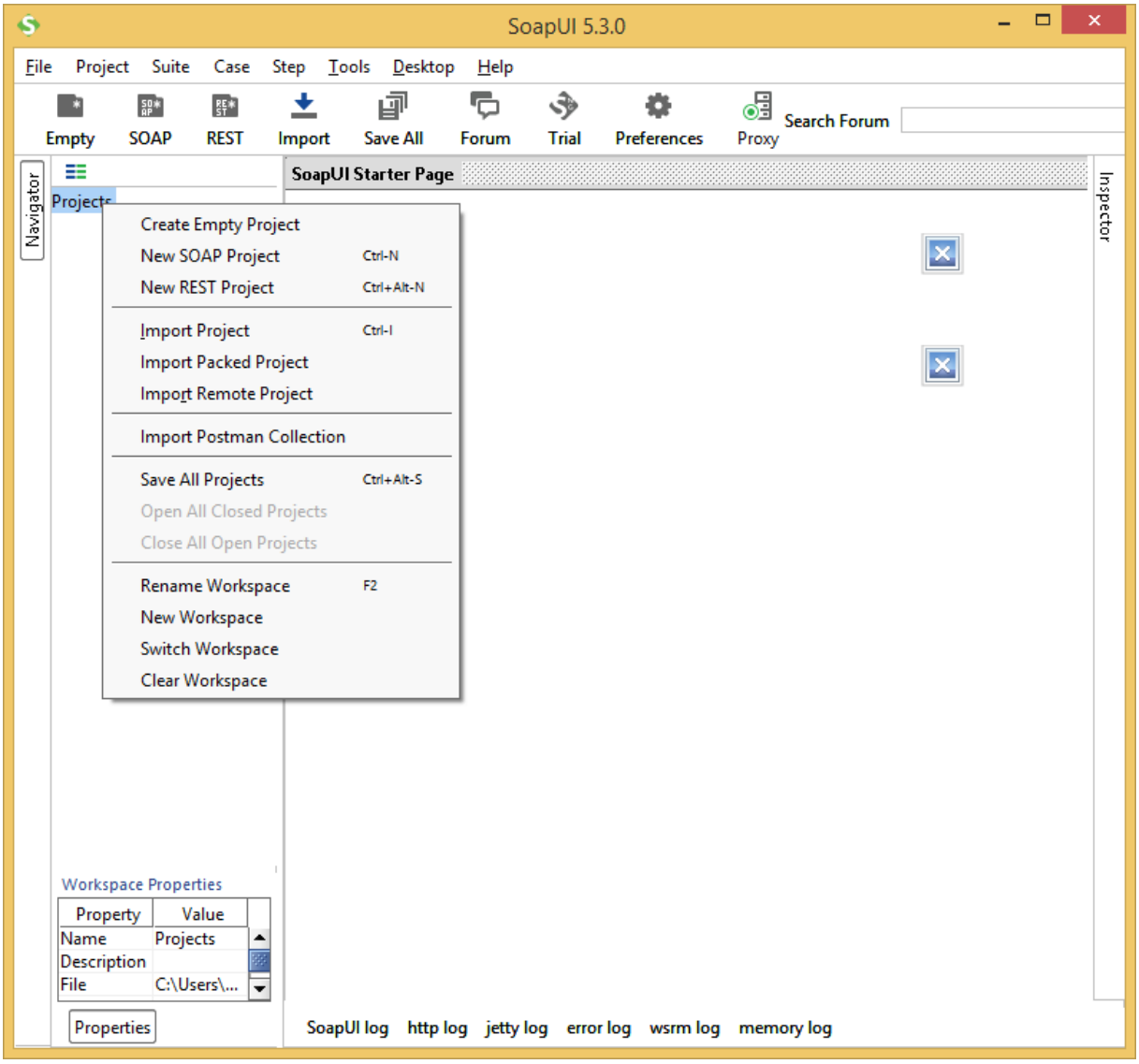
W celu nawiązania bezpiecznego połączenia SSL należy najpierw podłączyć certyfikat uwierzytelniający. W tym celu w menu File->Preferences wybieramy zakładkę SSL Settings.

W polu KeyStore wybieramy plik p12 z certyfikatem, a w polu KeyStore Password wprowadzamy hasło do pliku p12.

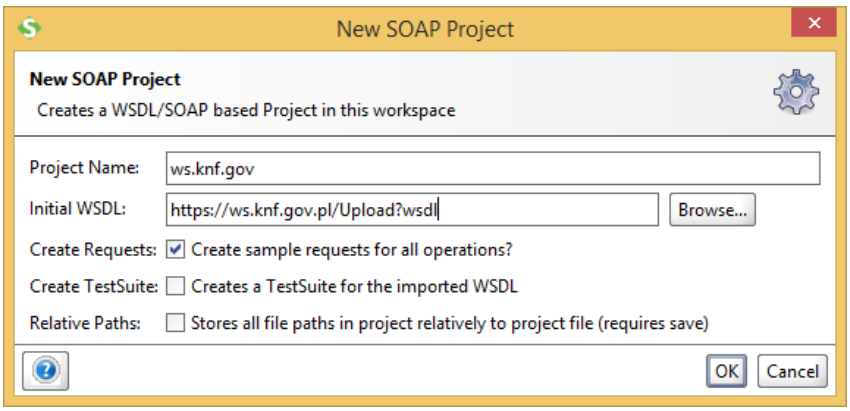
Klikamy Ok i przechodzimy do utworzenia projektu.


SoapUI Preferences
SoapUI Preferences
Set global SoapUI settings
HTTP Settings
Proxy Settings
SSL Settings
WSDL Settings
UI Settings
Editor Settings
Tools
WS-I Settings
Global Properties
Global Security Settings
WS-A Settings
Global Sensitive Information Tokens
Version Update Settings
AlertSite Connector Plugin
KeyStore:
G:\keystore\WS.p12
Browse...
KeyStore Password:
Enable Mock SSL:
enable SSL for Mock Services
Mock Port:
Mock KeyStore:
Browse...
Mock Password:
Mock Key Password:
Mock TrustStore:
Browse...
Mock TrustStore Password:
Client Authentication:
requires client authentication
OK
Cancel

W lewym oknie dialogowym klikamy prawym klawiszem na dostępnej gałęzi Project i z menu kontekstowego wybieramy opcję New SOAP Project.

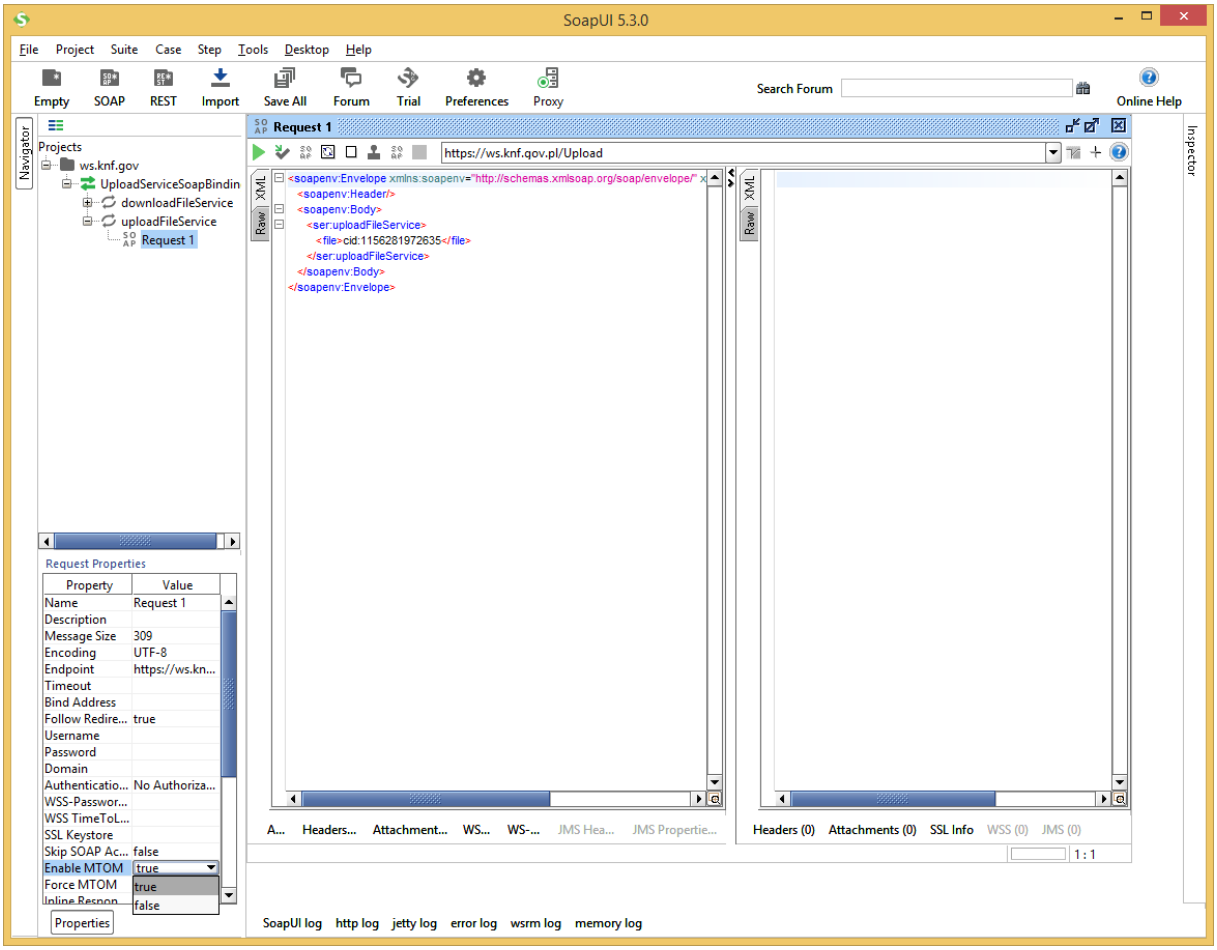


Pojawi się nowe okno dialogowe w którym w polu Initial WSDL wprowadzamy adres usługi.



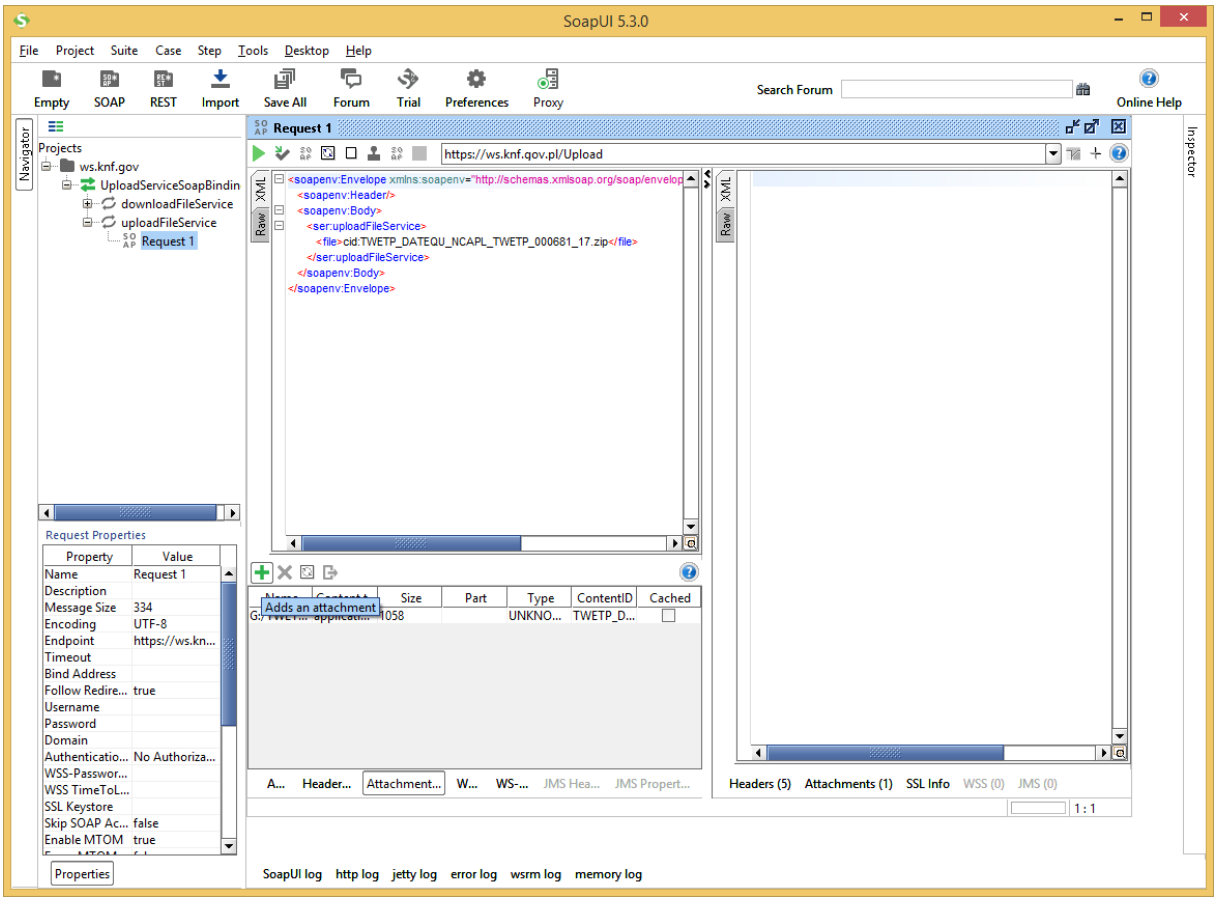
Klikamy OK i aplikacja automatycznie nawiązuje połączenie z serwerem i tworzy tzw. dowiązanie oraz request.

Rozwijamy drzewko projektu w poszukiwaniu gałęzi Request 1 i klikamy na niej aby w prawym panelu pojawiło się okienko do definicji SOAP requestu.

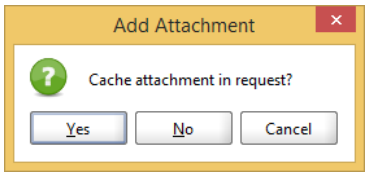


W lewym panelu w opcjach Request Properties zmieniamy wartość dla opcji Enable MTOM na true.

W panelu Request1 w lewym okienku klikamy na dolnym pasku klikamy w opcję Attachments



Następnie dodajemy załącznik ikoną „plus", wskazując go na dysku i klikamy OK. Pojawia okienko:



W 1 przesyłce (plik zip) może być tylko 1 plik xml. Nazwa pliku zip musi być zgodna z nazwą pliku xml.

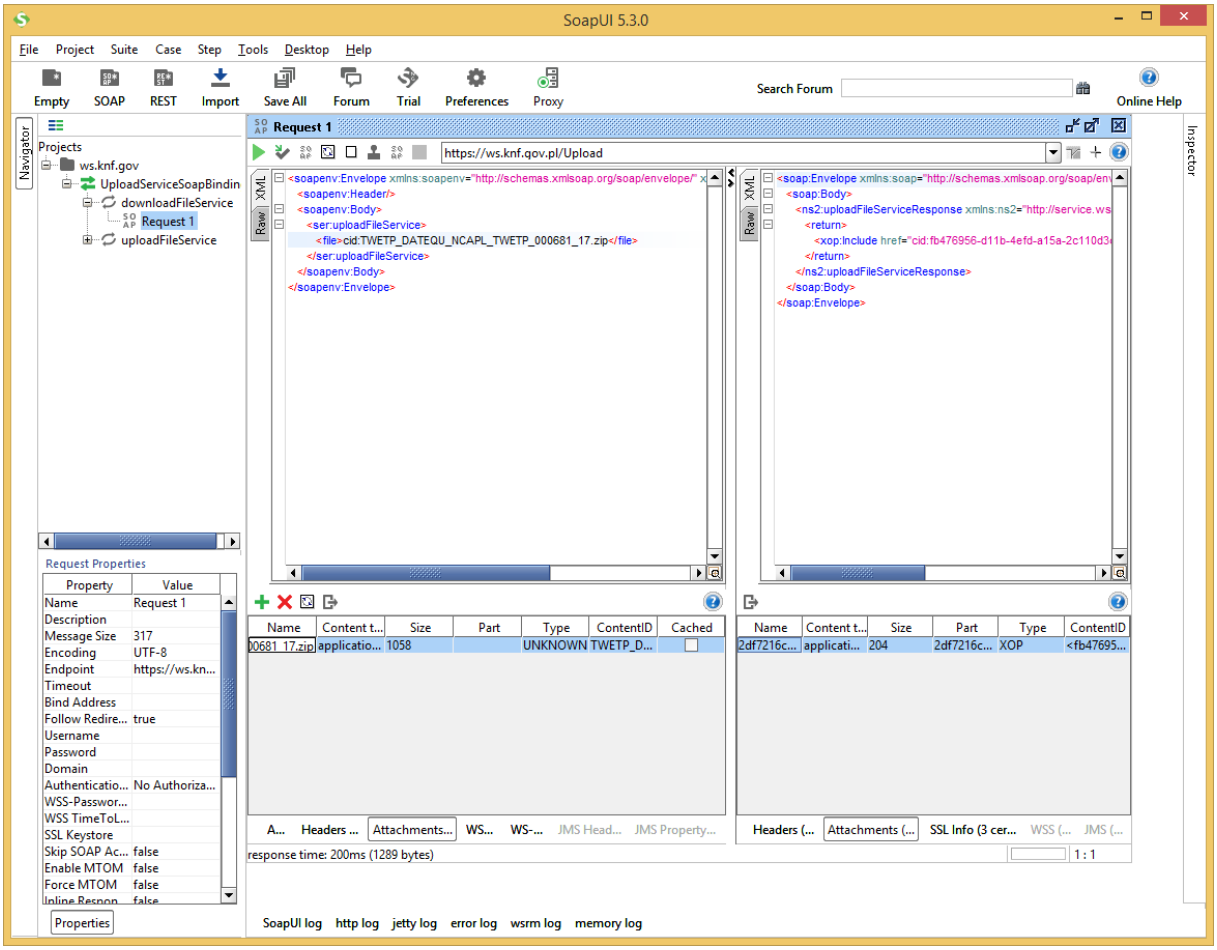
Jeśli załącznik przekracza 1Mb na pytanie o cacheowanie załącznika odpowiadamy No.

Następnie w okienku requestu XML wprowadzamy nazwę załączonego pliku

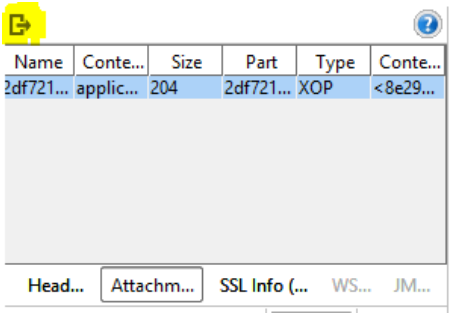
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://service.ws.gate.knf.gov.pl/">
  <soapenv:Header/>
  <soapenv:Body>
    <ser:uploadFileService>
      <file>cid:nazwa_pliku</file>
    </ser:uploadFileService>
  </soapenv:Body>
</soapenv:Envelope>
```

Następnie klikamy na zieloną ikonę trójkąta w górnym menu w oknie requestu, następuje wysyłka pliku na serwer.

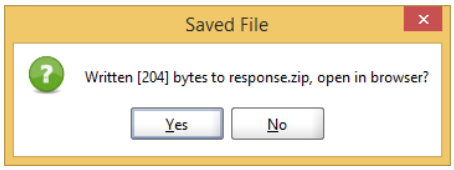
Po poprawnym wysłaniu usługa odpowiada w postaci pliku który można pobrać w prawym oknie requestu klikając w jego dolnym menu na Attachments.



Aby pobrać plik załącznika klikamy na ikonę



Zapisujemy plik pod nazwą z rozszerzeniem zip i klikamy OK. Pojawia się okno dialogowe czy otworzyć plik.



Kliknięcie ok otworzy plik zip. W środku znajduje się plik xml potwierdzenia.

Przykładowy plik poprawnej odpowiedzi powinien wyglądać następująco:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
    <file>
            <sender>XXX</sender>
            <received format="yyyy-MM-dd HH:mm:ss">2017-12-01 00:00:00</received>
            <name>TXXX_DATEQU_NCAPL_TXXX_000681_17.zip</name>
            <checksum alg="SHA-
256">e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855</checksum>
            <confirmationId>00000000-0000-0000-0000-000000000000</confirmationId>
            <status id="100" code="ACCEPTED">Accepted for processing</status>
    </file>
</response>
```

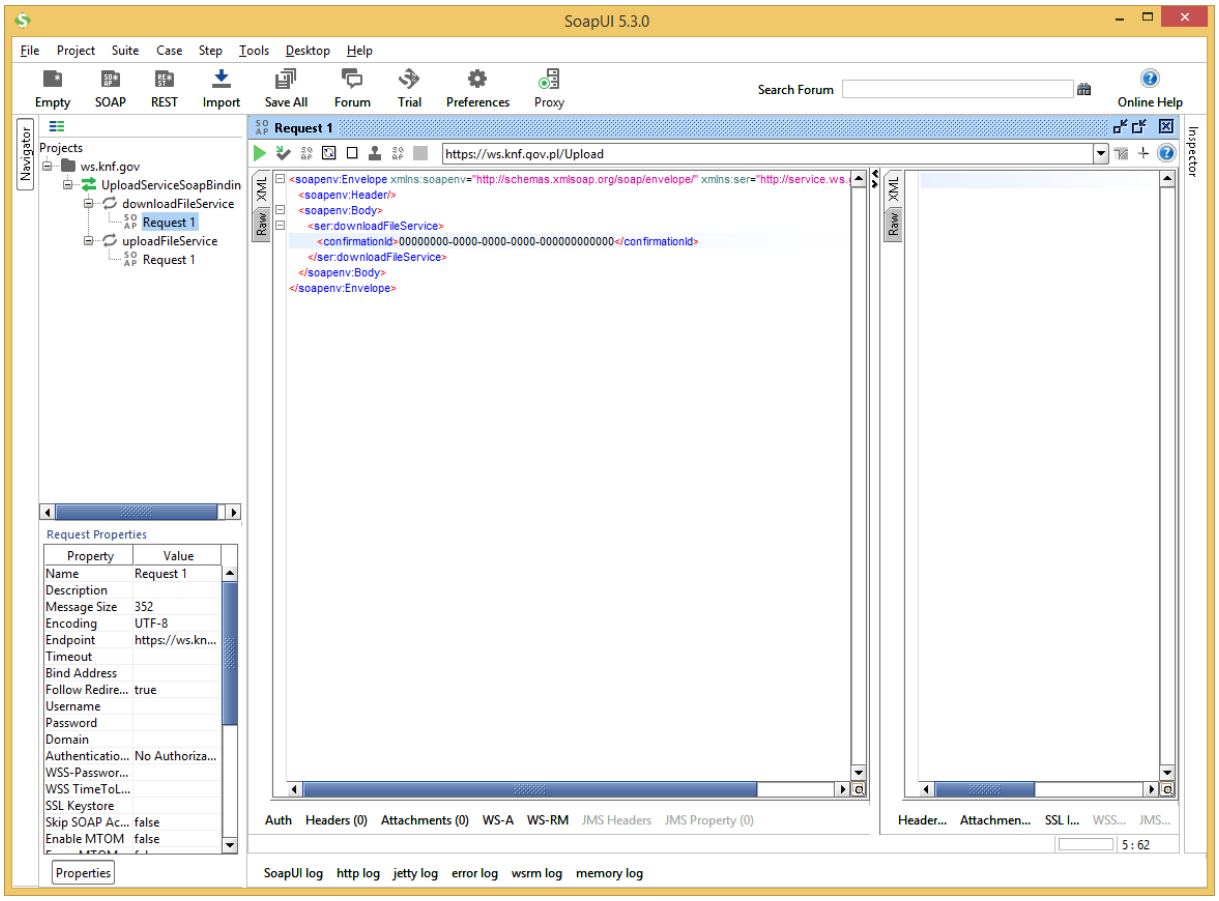
Każdy inny status należy uznać za błędny. W przypadku błędu nie zostanie wygenerowany identyfikator potwierdzenia confirmationId a plik nie będzie dalej przetwarzany.

Plik schema xsd odpowiedzi znajduje się w pkt 7.

Po poprawnym przyjęciu do przetwarzania plik trafia do kolejki, gdzie będzie szczegółowo dalej walidowany pod względem poprawności technicznej i merytorycznej.

Po zakończeniu przetwarzania system wysyła wiadomość email o zakończeniu przetwarzania i od tej chwili możliwe jest pobranie pliku komunikatu zwrotnego.

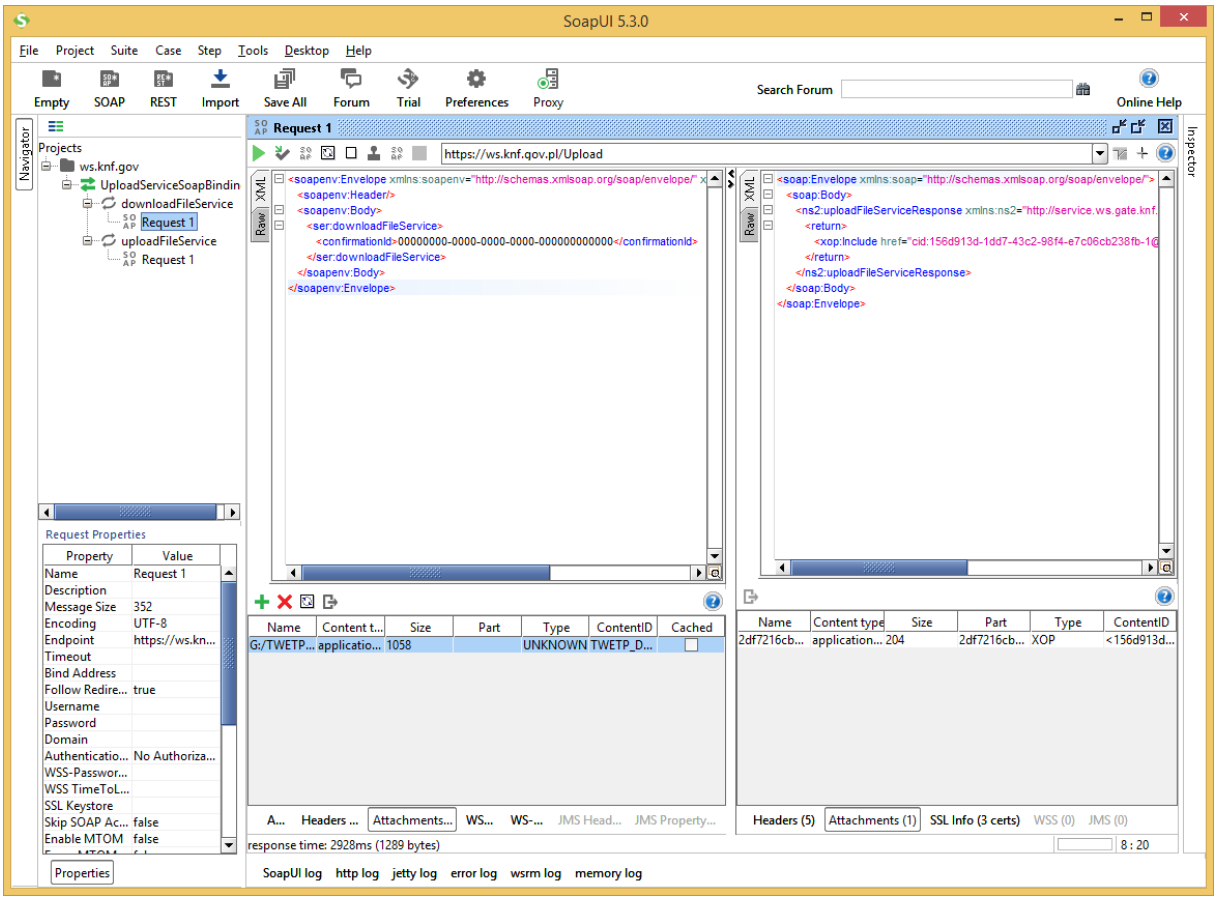
Należy w tym celu posłużyć się drugą metodą.



W wywołaniu tej usługi należy podać obowiązkowy parametr id potwierdzenia

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://service.ws.gate.knf.gov.pl/">
  <soapenv:Header/>
  <soapenv:Body>
    <ser:downloadFileService>
      <confirmationId>00000000-0000-0000-0000-000000000000</confirmationId>
    </ser:downloadFileService>
  </soapenv:Body>
</soapenv:Envelope>
```

W odpowiedzi metoda zwraca plik w postaci skompresowanego pliku zip w formacie XML ISO20022.



5 Przesyłanie plików za pomocą usługi Web Service

Plik powinien zostać załączony do parametru i powinien zostać przesłany z wykorzystaniem standardu MTOM. Wszystkie pliki są w formacie XML ISO20022, każdy z plików składa się z nagłówka ogólnego, nagłówka BAH (Businness Application Header), oraz pliku XML z danymi. Poniżej przedstawiono obowiązujące schematy XSD

- schemat dla nagłówka BAH head.003.001.01.xsd dla wszystkich plików
- schemat dla head.001.001.01_ESMAUG_1.0.0.xsd dla wszystkich plików

Pliki dla modułu TRANSPARENCY to pliki pozyskiwane z rynków DATETR, DATNTR, DATEQU, DATNQU, wymagane schematy XSD

- plik DATETR schemat DRAFT5auth.032.001.01_ESMAUG_DATETR_1.0.0.xsd
- plik DATNTR schemat DRAFT5auth.033.001.01_ESMAUG_DATNTR_1.0.1.xsd
- plik DATEQU schemat DRAFT6auth.040.001.01_ESMAUG_DATEQU_1.0.0.xsd
- plik DATNQU schemat DRAFT5auth.041.001.01_ESMAUG_DATNQU_1.0.0.xsd

Pliki dla TREM - pliki DATTRA

- schemat dla pliku DRAFT15auth.016.001.01_ESMAUG_Reporting_1.0.3

Pliki dla RDS – DATINS oraz DATNWD:

- plik DATINS schemat DRAFT13auth.017.001.01_ESMAUG_DATINS_1.0.0.xsd
- plik DATNWD schemat DRAFT4auth.039.001.01_ESMAUG_DATNWD_1.0.0.xsd

Plik dla Dobuble Volume Cap – DATDVC:

- plik DATDVC schemat MiFIR_DRAFT5auth.035.001.01- Trading Volume Cap Reporting.xsd

Nazwy plików:

a) Dla DATETR; DATNTR; DATEQU; DATNQU; zgodnie z dokumentacją ESMA.
b) Dla DATDVC:

Receiver_FileType_System_TMIC_FileNumber_Year
(5x) (6x) (5x) (5x) (6x) (2x)

Gdzie:

Receiver – NCAPL
FileType – DATDVC
System – DVCAP
MIC – T+kod MIC
FileNumber – unikalny numer pliku
Year – ostatnie dwie cyfry roku

Przykład: **NCAPL_DATDVC_DVCAP_TXWAR_001234_18**

c) Dla DATINS; DATNWD:

MIC_FileType_Date_FileNumber
(4x) (6x) (8x) (3x)
Gdzie:

MIC – kod MIC podmiotu
FileType – DATINS lub DATNWD
Date – data w formacie RRRRMMDD
FileNumber – kolejny numer pliku w danym dniu. Pierwszy plik danego dnia ma numer 000

Przykład: **WBON_DATINS_20171220_000**
XWAR_DATNWD_20180123_001

d) Dla DATTRA:

Sender_FileType_Receipient_Key1_Key2_Year

(20x) 6(x) 5(x) 3(n) 6(n) 2(n)

Gdzie:

Sender – kod LEI podmiotu

FileType – DATTRA

Recipient – PFSA

Key1 – ARM lub FIN (firma inwestycyjna)

Key2 – unikalny numer pliku od danego wysyłającego

Year – dwie ostatnie cyfry roku

Przykład: **1234567890ABCDEFGHIJ_DATTRA_PFSA_FIN_000001_17**

ABCDEFGHIJ1234567890_DATTRA_PFSA_ARM_987654_17

6 Odbieranie potwierdzenia przesłania pliku

Po poprawnym przesłaniu pliku metoda zwraca skompresowany plik odpowiedzi. Plik odpowiedzi w postaci archiwum zip, które po rozkompresowaniu powinno zawierać plik xml zapisany w formacie ISO 20022. Pliki odpowiedzi mają nazwę utworzoną w sposób następujący:

plik FDBETR jest odpowiedzią dla pliku DATETR

plik FDBNTR jest odpowiedzią dla pliku DATNTR

plik FDBEQU jest odpowiedzią dla pliku DATEQU

plik FDBNQU jest odpowiedzią dla pliku DATNQU

plik FDBINS jest odpowiedzią dla pliku DATINS

plik FDBDVC jest odpowiedzią dla pliku DATDVC

plik FDBNWD jest odpowiedzią dla pliku DATNWD

obowiązującym schematem XSD dla w/w plików jest auth.031.001.01_ESMAUG_FDB_1.0.0.xsd.

plik FDBTRA jest odpowiedzią dla pliku DATTRA

obowiązującym schematem XSD dla w/w pliku jest
DRAFT4auth.031.001.01_ESMAUG_FDBTRA_1.0.1.xsd

W przypadku DATTRA zamianie ulega pole „Recipient" i „Sender"

Przykład:

Plik przychodzący: **1234567890ABCDEFGHIJ_DATTRA_PFSA_FIN_000001_17**

Plik odpowiedź: **PFSA_FDBTRA_1234567890ABCDEFGHIJ _FIN_000001_17**

7 Schema XSD dla odpowiedzi XML dla metody uploadFileService

```
<?xml version="1.0" encoding="utf-8"?>

<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://service.ws.gate.knf.gov.pl/">
 <xs:element name="response">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="file">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="sender" type="xs:string" />
       <xs:element name="received">
        <xs:complexType>
         <xs:simpleContent>
          <xs:extension base="xs:string">
           <xs:attribute name="format" type="xs:string" use="required" />
          </xs:extension>
         </xs:simpleContent>
        </xs:complexType>
       </xs:element>
       <xs:element name="name" type="xs:string" />
       <xs:element name="checksum">
        <xs:complexType>
         <xs:simpleContent>
          <xs:extension base="xs:string">
           <xs:attribute name="alg" type="xs:string" use="required" />
          </xs:extension>
         </xs:simpleContent>
        </xs:complexType>
       </xs:element>
       <xs:element name="confirmationId" type="xs:string" minOccurs="0" />
       <xs:element name="status">
        <xs:complexType>
         <xs:simpleContent>
          <xs:extension base="xs:string">
           <xs:attribute name="id" type="xs:string" use="required" />
           <xs:attribute name="code" type="xs:string" use="required" />
          </xs:extension>
         </xs:simpleContent>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

8 Metryka zmian w dokumencie

Wersja	Opis zmiany	Data dokumentu
1.0	Nowy dokument	2017–12–22
1.1	**Rozdział 3:** link do strony „dostęp do usługi sieciowej Webservice KNF” **Rozdział 5-6:** dodano obsługę plików DATDVC; DATINS; DATNWD. Rozszerzono opis dla pliku odpowiedzi FDB **Rozdział 7:** korekta schemy z *<xs:element name="recived">* na *<xs:element name="received">* **Załącznik nr 1; punkt 1) Adres usługi:** link do środowiska testowego	2018–05–07
1.2	Rozdział 6: zmiana schemy pliku odpowiedzi dla DATTRA na DRAFT4auth.031.001.01_ESMAUG_FDBTRA_1.0.1.xsd	2018-10-22