Rules of using KNF Webservice network services

date: 22/10/2018
version: 1.2

Table of Contents:

1 Dictionary of terms

User - a user of the Webserwis KNF network service

SOA – Service Oriented Architecture

WSDL – Web Service Definition Language – the language defining network services, which uses the XML language to describe those services and define parametres necessary for calling those services.

SOAP – Simple Object Access Protocol – communications protocol using the XML to build network services calls defined through the WSDL.

PCKS-12 – *.p12 archival file format for storing many cryptographic objects in one file. The package of private keys with X.509 certificate or the package of public certificates, so-called trust chain, is commonly used.

X.509 – a standard that defines a scheme for digital certificates and their attributes

CA – Certification Authority – a certification authority which issues/revokes certificates, and certifies other CAs

HTTPS - Hypertext Transfer Protocol Secure – is a protocol providing a safe communication within computer network being in common use on the Internet

OTA – Over-The-Air – services provided remotely, wirelessly

Single-use link - a URL together with specially crafted parametres directing to the Registration System. After clicking, it calls a single-time system action after which the link becomes inactive

2 Introduction

The ***KNF Webservice*** is a universal, safe channel for exchanging information between the Polish Financial Supervision Authority and external entities (service users). The service allows sending structured information to the Polish Financial Supervision Authority in the form of a file having a strictly defined format and name, and the reception of a feedback regarding sent data.

This is a standardised network service (Web Service) in the SOA architecture allowing to entities both integration with their own IT systems and using any client enabling a communication compliant with the WSDL standard.

3 Access to the Webserwis KNF service

The access to the service requires having a valid digital certificate issued by the KNF CA certification authority. The process of acquiring the certificate by a user, its renewal, as well as revocation are described in documents on the following website: https://www.knf.gov.pl/for_rynku/MiFIR/raportowanie_transakcji_art_26_MiFIR/Dostep_do_uslugi_sieciowej_Webservice_KNF

4 The process of using the service

The transfer of a file by using the ***Webserwis KNF*** service requires the realisation of the following steps:

a) The user connects with the Internet via the HTTPS safe protocol at the address of the network service (the address is indicated in the appendix to this document). In the process, the user authentication takes place by means of a digital certificate, including the verification of a current status of the certificate.

b) The user, after the successful authentication, receives the access to service, including detailed information in the form of WSDL file, necessary for a remove calling the communication methods of the channel.

c) The user, by using any client of the WSDL service constructs an inquiry in the SOAP standard and calls a correct method of the service depending on a type of an information to be sent. Names, formats and dates of file transferring must be compliant with applicable regulations.

d) On-line service:
   - performs the authorisation of the user by verifying, on the basis of a type and input parametres of a method being called, whether owns required authorisations for the service,
   - performs initial technical validations of sent information, including the correctness of the file name in a package.

e) Should the authorisation and technical validation be finished successfully, in the return message of **Webserwis KNF**, the user will receive an answer containing:
   - name of the file sent,
   - date and time of receipt of data by the KNF,
   - unique package identifier - it is necessary for further download of results for further file processing in the KNF,
   - package status - ***Accepted for processing*.**

f) Should authorisation or validation end with an error in the return message of the **Webserwis KNF** service, the user will receive an answer containing:
   - name of the file sent,
   - date and time of a data by the KNF,
   - package status - ***Rejected***
   - description and the error number.

g) Data sent are subject to further processing by the KNF. After the completion of the processing process, the user will receive a notification via e-mail (at the address indicated in the application for the access) about the completion of the processing containing information on:
   - processing results, including the list of errors, if the result of processing is negative,
   - sharing a confirmation file for download

Confirmation file download takes place by using the same **Webserwis KNF** network service. In a method being called, it is appropriate to provide a parametre containing a unique package identifier received in the service return message (see pt. 5e). The confirmation file's iformat name is compliant with ESMA requirements.

h) Additional technical details of the service, including the method of connecting are described in the appendix to this document.

5 Technical standards and safety

5.1 Applied technical standards

KNF network service made available by the Polish Financial Supervision Authority is in conformity with the following standards:

- WSDL (https://www.w3.org/TR/wsdl) - with regard to the definition of the service,
- SOAP (https://www.w3.org/TR/soap/) - with regard to the service communication protocol,
- MTOM (https://www.w3.org/TR/soap12-mtom/) - with regard to the transmission of binary files.

5.2 Safety

The whole communication between the user and the Polish Financial Supervision Authority is secured by an encrypted channel with the use of the HTTPS protocol.

5.3 Access to service

The access to the service is protected by means of the certification via a digital certificate in the X.509 standard generated by the KNF certification authority. Certificates are valid for a year.

User's private and public key is stored in PCKS-12 archive file intended for storing cryptographic keys. The archive is encrypted and protected by a password. PCKS-12 file will be distributed through the Internet network in the form of a single-use link sent at the e-mail contact address provided in the application for the access - in the event of the provision of more than 1 address in the contact e-mail box, the link will be sent at the first provided address. The user, by clicking ion the link, will download the certificate and the link will become inactive afterwards.

The installation of the certificate on the user's station requires a password to be provided. The password to install the certificates from PCKS-12 file will be sent - after the certificate download - in the form of a single-use link included in an e-mail address sent at the same e-mail address as the certificate.

In the event of the necessity to download the certificate again, it will necessary to generate a new link.

In the process of user authentication it is verified whether:

- the certificate used for authentication within the Webserwis KNF service was generated from KNF CA
- the certificate neither expired nor was withdrawn or invalidated
- the user has authorisations to use a called service method

In case of improper authentication, the access to the service will not be possible.

5.4 Principles of conduct with KNF CA certificate

Certificates issued by the KNF CA, in order to protect them, are subject to the following principles:

a) A person downloading the certificate is responsible for its safe storage and making it available to be used, including:

- Providing safety to a working station, on which the certificate has been installed through the use of software having individual settings, in compliance with current IT safety internationals standards. It is appropriate to ensure adequate means, including, particularly, the protection against viruses and malicious software, preventing password stealing, as well as the procedures of improving safety level and implementing corrections to software. Any such means and procedures have to be updated regularly.
- Accounts of the user using the certificate on working stations should not have administrator rights. Rights should be granted according to the
  "as little rights as possible" principle.
- The provision of a continuous protection for computer systems used in order to provide the Internet-based access to the ***Webserwis KNF*** system through:
- assurance of a continuous protection of computer systems and working stations against unauthorised access - physical and network - by applying firewall at all times for the purpose of protecting computer systems and working stations against data received from the Internet, as well as working stations against an unauthorised access through the intranet and allowing to communicate outside only to authorised programs.
- regular updating and supplementation with corrections according to the latest version. This concerns particularly an operating system, internet browser and add-ons.
- protection of all critical, internal data flows to working stations and from those stations against their disclosure and harmful changes, particularly in the event of file transfer through the network.

b) Storage of certificates

- The certificate should be located in accordance with the requirements of an internet browser, e.g. in so-called certificate store.
- certificates being stored in the certificate store should be encrypted according to the recommendations of the safety policy applicable in an organisation of an entity. In the event of lack of such guidelines, the certificate should be encrypted on the basis of general recommendations for a given operational system being used by a supervised entity.

c) In order to limit the risk for its IT system, a supervised entity continuously complies with the following principles of management:

- determination of the users management practice guaranteeing the establishment and maintenance of only accounts of authorised users within the system, as well as the maintenance of an accurate and up-to-date list of authorised users;

- comparing a daily data flow in order to detect incompatibilities between an authorised and actual data flow, both those being sent and received.

d) Moreover, it is recommended to:

- organise periodic revisions of the working stations of users controlling the status of storage and certificates securing that prevents them against being exported outside of designated working stations.
- in order to limit continuously an output data flow from working stations to websites being of the greatest significance for the activity of an entity, as well as to website necessary for the conducting authorised and justified software updates
- conducting periodic inspections of users with regard to the use of the certificate

Appendix no. 1

Technical instruction on connecting to the Webserwis KNF service

1 Address of the service

The address, at which the service is available is as follows:

Production environment: https://ws.knf.gov.pl

Test environment: https://test-ws.knf.gov.pl/

2 Authentication by means of the certificate

Every service user (external entity) will receive a generated x.509 certificate (private and public key) in the form of p12 file.
This is a password-protected file.

3 Selection of a service client

In order to connect with the service, it is appropriate to use any SOAP client. However, it is appropriate to configure the client in such a manner that it is able to make a safe SSL session with the server via an attached digital certificate.

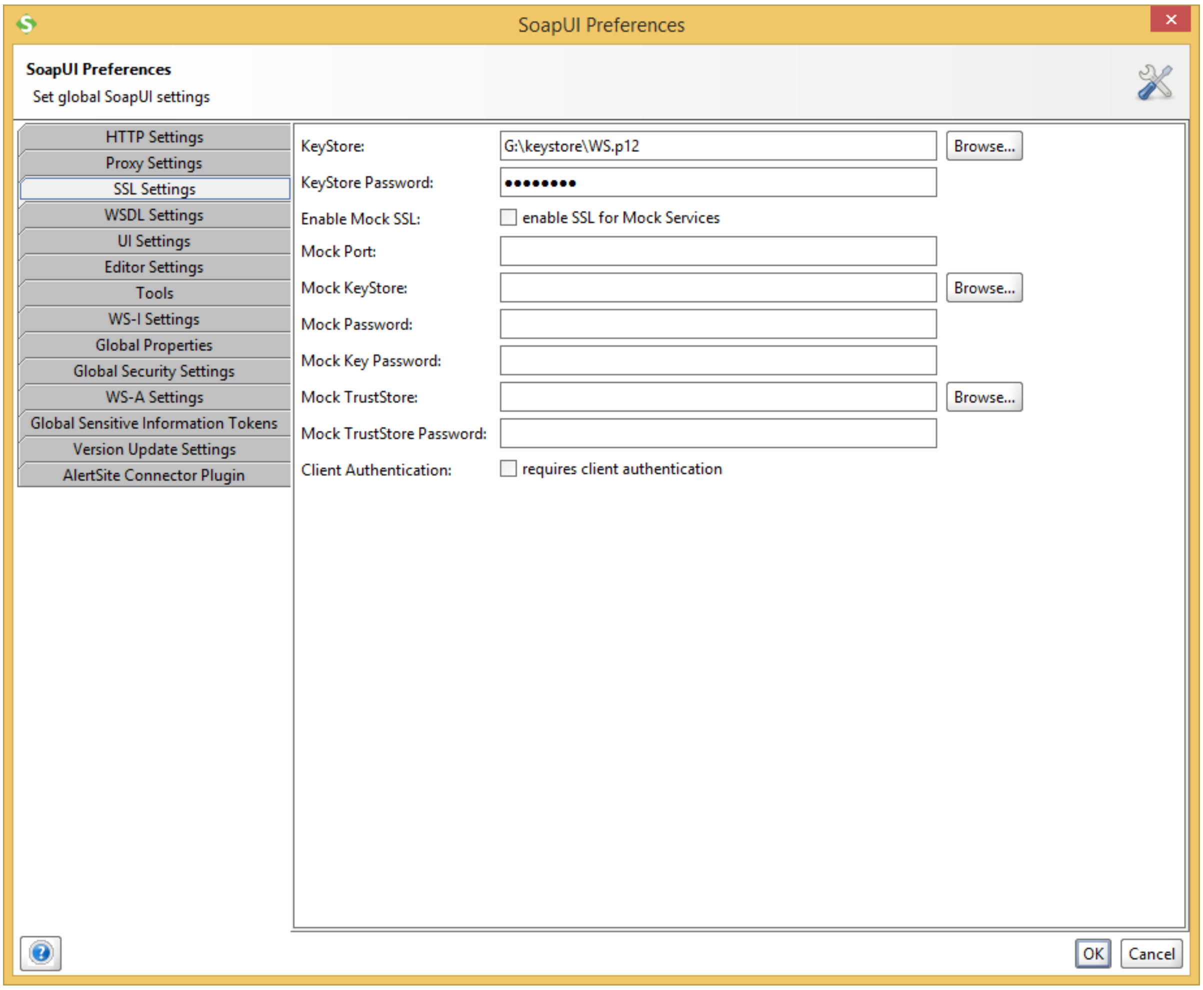
4 Example of a SOAP-UI client configuration

SOAP-UI application (https://www.soapui.org/downloads/soapui.html) in OpenSource version is available for download free of charge and enables communication and testing SOPA Web Services.

In order to make a safe SSL connection it is appropriate to connect an authenticating certificate at first.
To this end, in File->Preferences menu, select SSL Settings tab.

In KeyStore box, select p12 file with the certificate, and in KeyStore Password box enter the password to p12 file.

Click Ok and proceed to the a project creation.



KeyStore: G:\keystore\WS.p12

KeyStore Password: ••••••••

Enable Mock SSL: □ enable SSL for Mock Services

Mock Port:

Mock KeyStore:

Mock Password:

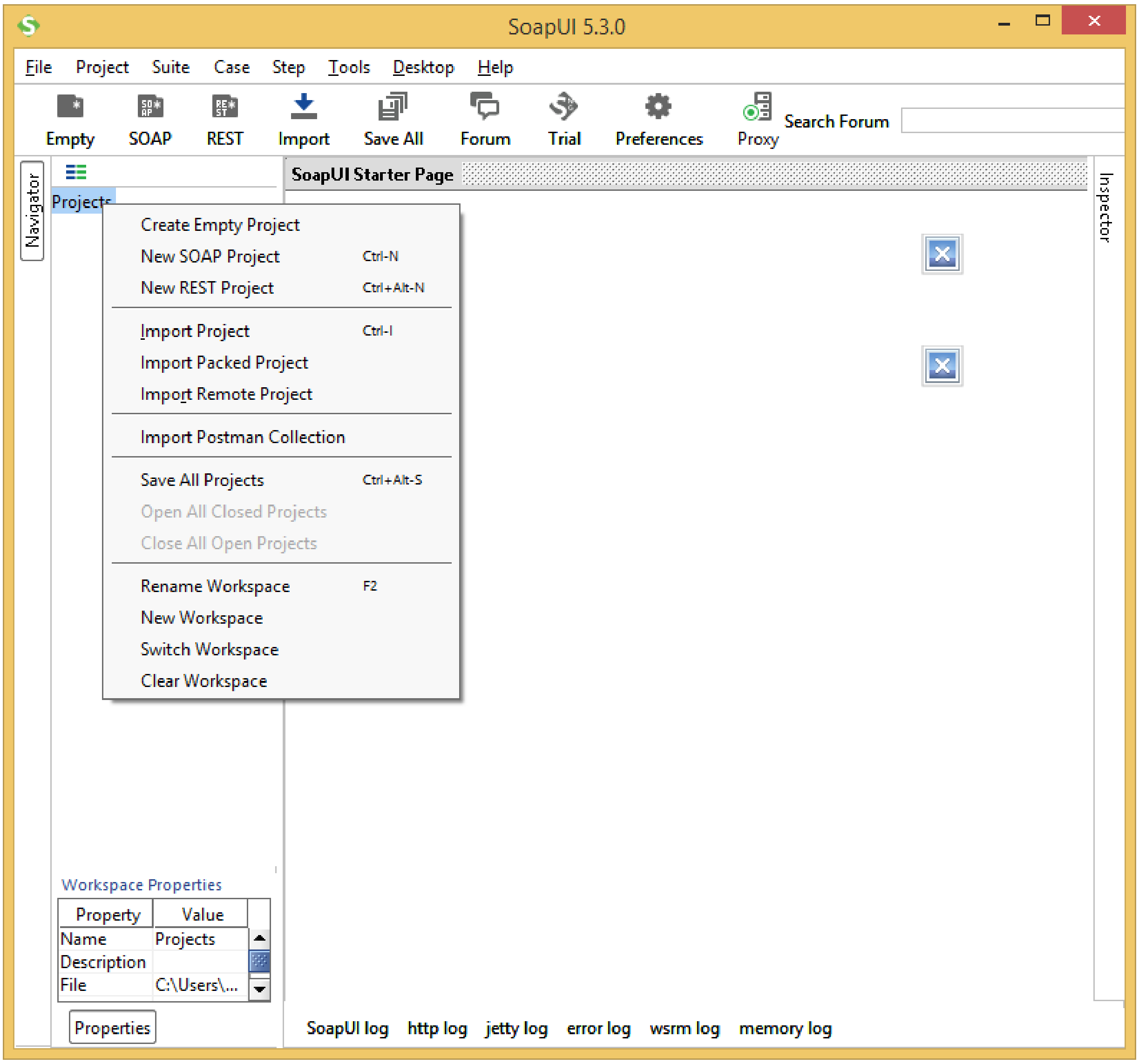
Mock Key Password:

Mock TrustStore:

Mock TrustStore Password:

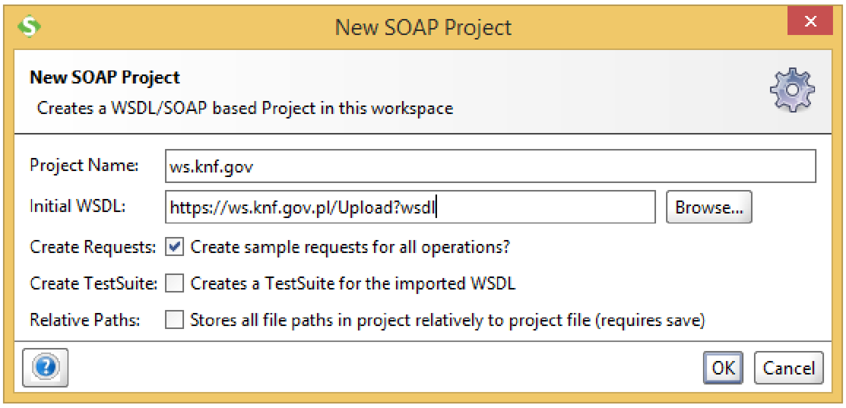
Client Authentication: □ requires client authentication

Right-click on the left-hand dialogue box on an available Project branch and select New SOAP Project option in the contextual menu.



Property	Value
Name	Projects
Description	
File	C:\Users\...

A new dialogue box will pop up, in which in Initial WSDL box enter the address of the service.

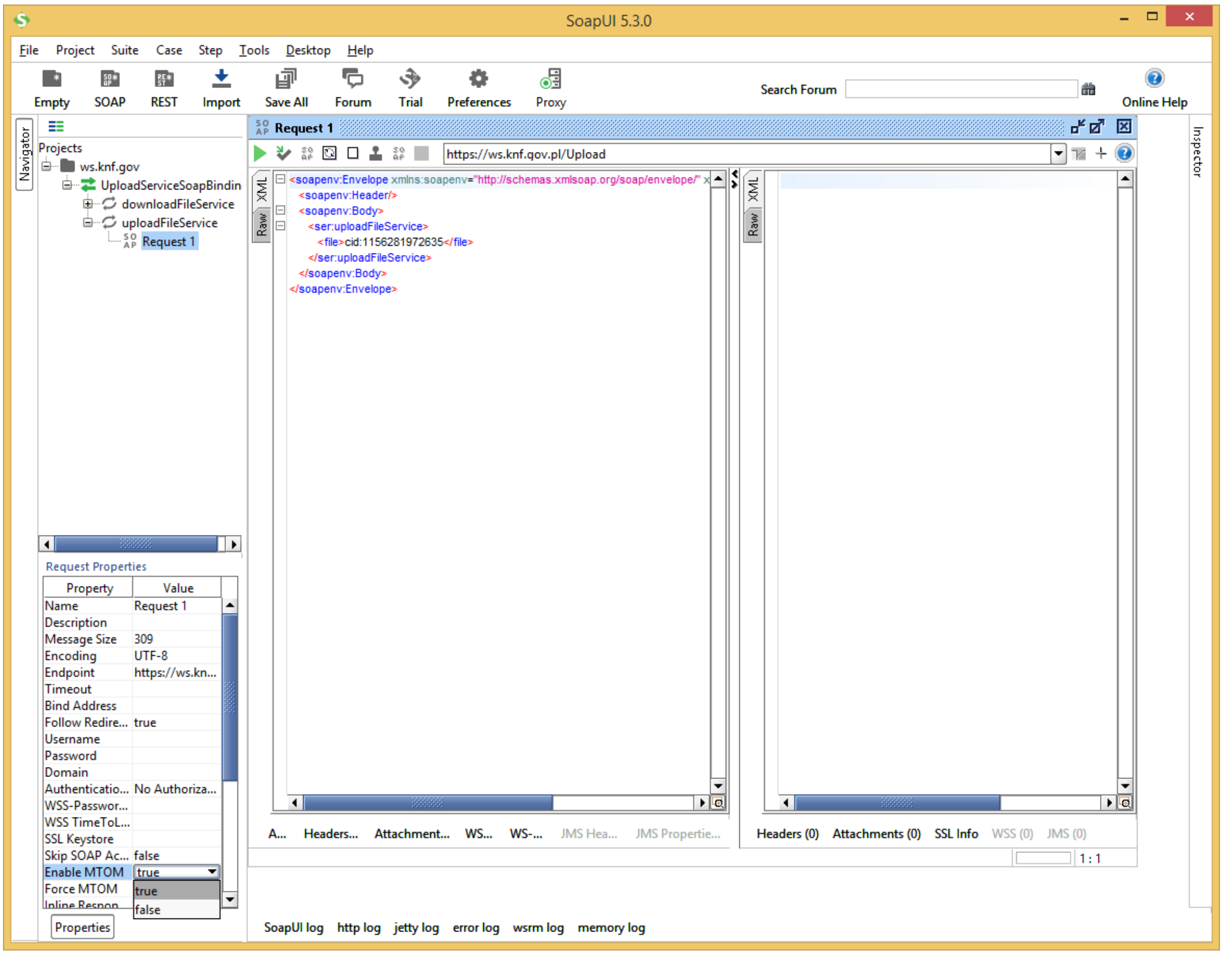


New SOAP Project
Creates a WSDL/SOAP based Project in this workspace

Project Name: ws.knf.gov
Initial WSDL: https://ws.knf.gov.pl/Upload?wsdl
Create Requests: ☑ Create sample requests for all operations?
Create TestSuite: □ Creates a TestSuite for the imported WSDL
Relative Paths: □ Stores all file paths in project relatively to project file (requires save)

Click OK and the application will automatically make a connection with the server and open a so-called link and request.

Expand the project tree in order to find Request 1 branch and click on it, so that a box for the SOAP request definition appear in the right-hand panel.


SoapUI 5.3.0
File Project Suite Case Step Tools Desktop Help
Empty SOAP REST Import Save All Forum Trial Preferences Proxy
Search Forum
Online Help
Navigator
Inspector
Projects
ws.knf.gov
UploadServiceSoapBindin
downloadFileService
uploadFileService
Request 1
XML
Raw
A... Headers... Attachment... WS... WS-... JMS Hea... JMS Propertie...
Headers (0) Attachments (0) SSL Info WSS (0) JMS (0)
1 : 1
Properties
SoapUI log http log jetty log error log wsrm log memory log

Request 1

https://ws.knf.gov.pl/Upload

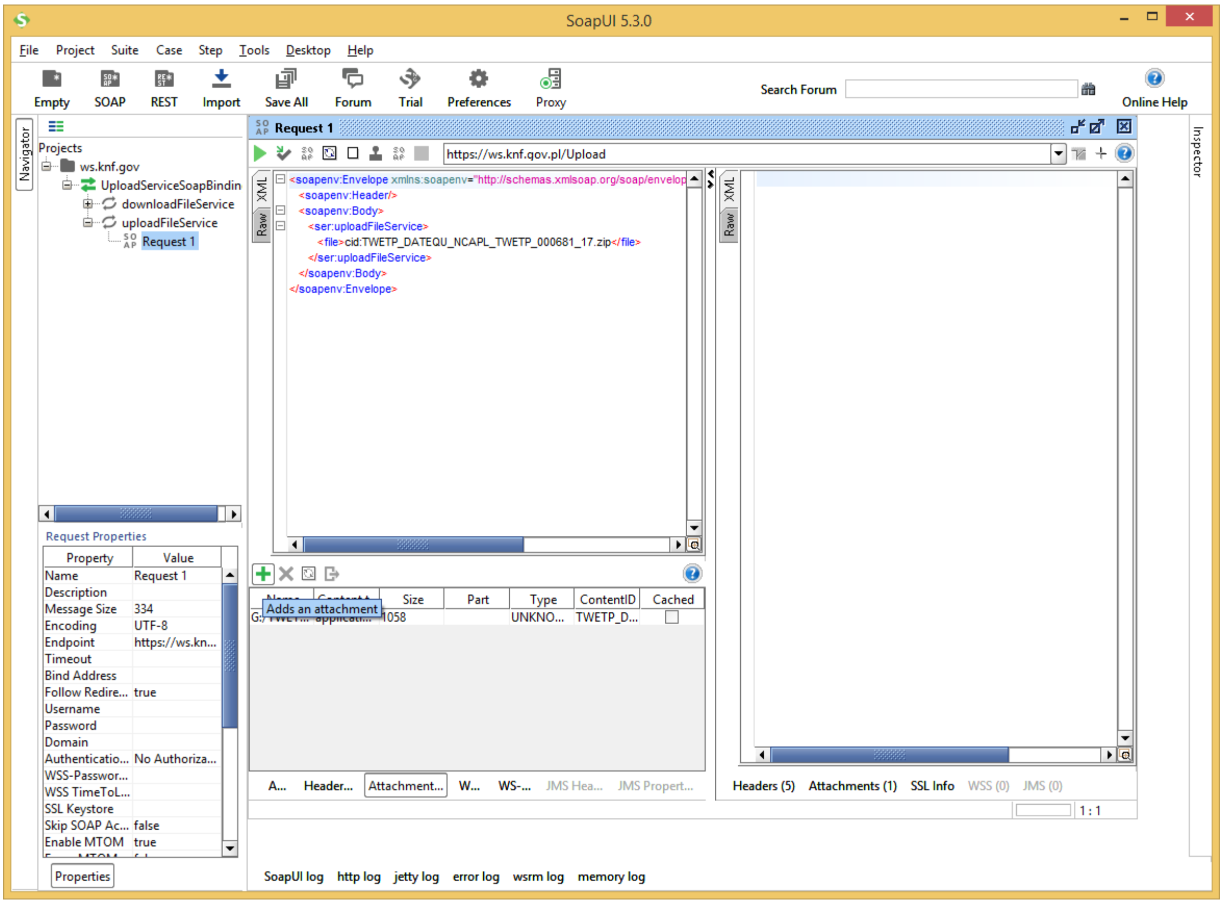
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" x
   <soapenv:Header/>
   <soapenv:Body>
      <ser:uploadFileService>
         <file>cid:1156281972635</file>
      </ser:uploadFileService>
   </soapenv:Body>
</soapenv:Envelope>
```

Request Properties

Property	Value
Name	Request 1
Description	
Message Size	309
Encoding	UTF-8
Endpoint	https://ws.kn...
Timeout	
Bind Address	
Follow Redire...	true
Username	
Password	
Domain	
Authenticatio...	No Authoriza...
WSS-Passwor...	
WSS TimeToL...	
SSL Keystore	
Skip SOAP Ac...	false
Enable MTOM	true true false
Force MTOM	
Inline Respon	

In the left-hand panel in Request Properties options change a value for Enable MTOM option to true.

In Request1 panel in the left-hand box, click on an Attachments option in the lower bar



SoapUI 5.3.0
File Project Suite Case Step Tools Desktop Help
Empty SOAP REST Import Save All Forum Trial Preferences Proxy
Search Forum
Online Help
Navigator
Projects
ws.knf.gov
UploadServiceSoapBindin
downloadFileService
uploadFileService
Request 1
Inspector
XML
Raw
Adds an attachment
A... Header... Attachment... W... WS-... JMS Hea... JMS Propert...
Headers (5) Attachments (1) SSL Info WSS (0) JMS (0)
1 : 1
Properties
SoapUI log http log jetty log error log wsrm log memory log

Request 1

https://ws.knf.gov.pl/Upload

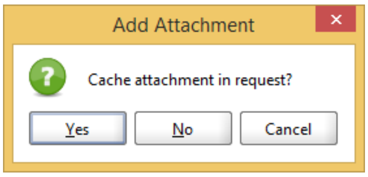
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelop
  <soapenv:Header/>
  <soapenv:Body>
    <ser:uploadFileService>
      <file>cid:TWETP_DATEQU_NCAPL_TWETP_000681_17.zip</file>
    </ser:uploadFileService>
  </soapenv:Body>
</soapenv:Envelope>
```

Request Properties

Property	Value
Name	Request 1
Description	
Message Size	334
Encoding	UTF-8
Endpoint	https://ws.kn...
Timeout	
Bind Address	
Follow Redire...	true
Username	
Password	
Domain	
Authenticatio...	No Authoriza...
WSS-Passwor...	
WSS TimeToL...	
SSL Keystore	
Skip SOAP Ac...	false
Enable MTOM	true

Name	Content t	Size	Part	Type	ContentID	Cached
G:/ TWET...	applicati...	1058		UNKNO...	TWETP_D...	□

Then add and attachment by using the “plus” icon, indicating it on a disc, then click OK. The following window will appear:



Add Attachment

Cache attachment in request?

1 package (zip file) can contain only 1 xml file. Zip file name must be compliant with the xml file. If

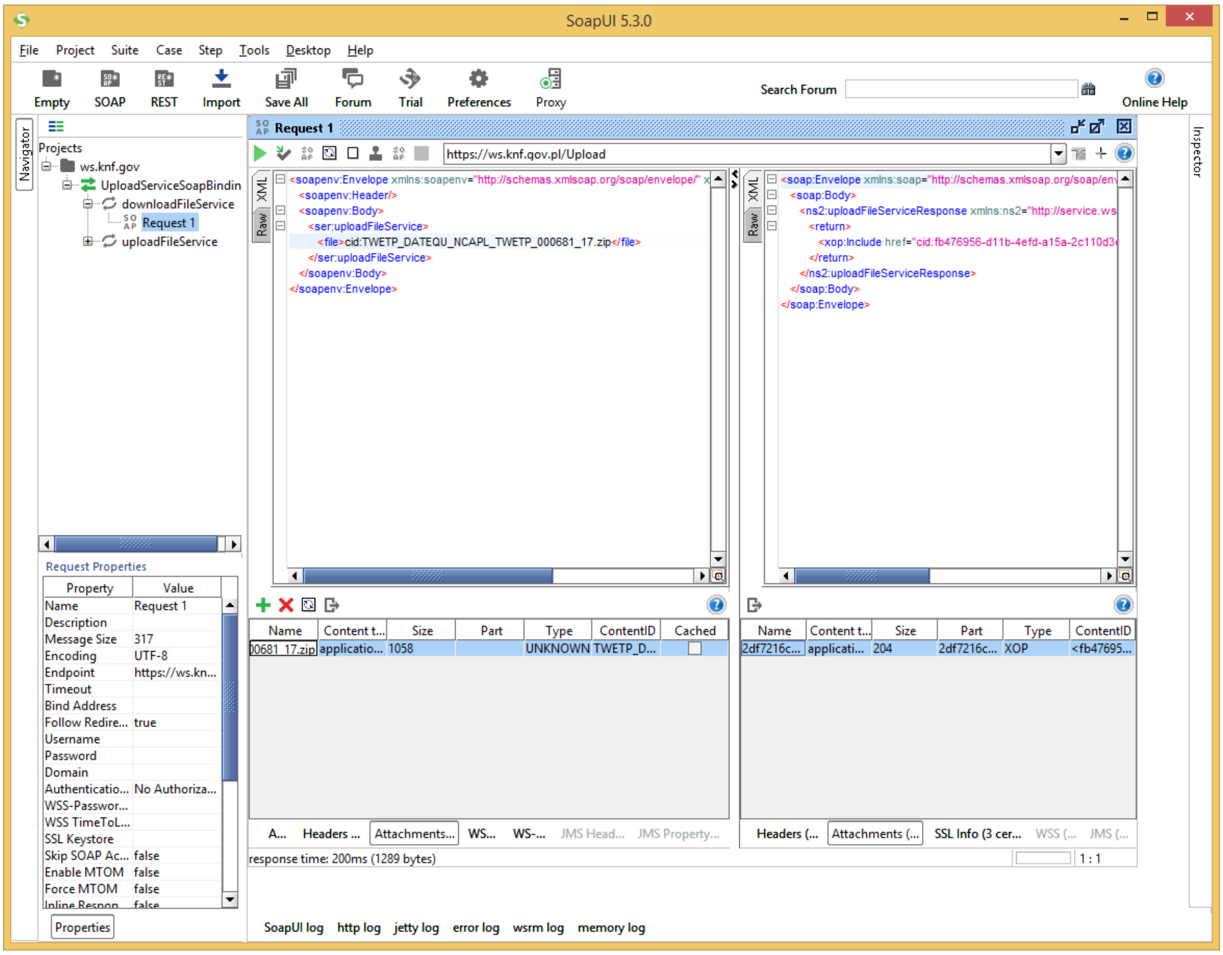
the attachment size exceeds 1Mb, answer “No” to the question about caching.

Afterwards, in the XML request window, provide the name of an attached file

```
<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:file_name</file>
    </ser:uploadFileService>
  </soapenv:Body>
</soapenv:Envelope>
```

Then, click on the green triangle icon in the upper menu in the request window, then transfer the file to the server.

After correct transfer, the service answers in the form of a file, which can be downloaded in the right-hand request box by clicking on its lower menu on Attachments.



```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" x
  <soapenv:Header/>
  <soapenv:Body>
    <ser:uploadFileService>
      <file>cid:TWETP_DATEQU_NCAPL_TWETP_000681_17.zip</file>
    </ser:uploadFileService>
  </soapenv:Body>
</soapenv:Envelope>
```

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/env
  <soap:Body>
    <ns2:uploadFileServiceResponse xmlns:ns2="http://service.ws
      <return>
        <xop:Include href="cid:fb476956-d11b-4efd-a15a-2c110d3
      </return>
    </ns2:uploadFileServiceResponse>
  </soap:Body>
</soap:Envelope>
```

Request Properties

Property	Value
Name	Request 1
Description	
Message Size	317
Encoding	UTF-8
Endpoint	https://ws.kn...
Timeout	
Bind Address	
Follow Redire...	true
Username	
Password	
Domain	
Authenticatio...	No Authoriza...
WSS-Passwor...	
WSS TimeToL...	
SSL Keystore	
Skip SOAP Ac...	false
Enable MTOM	false
Force MTOM	false
Inline Respon...	false

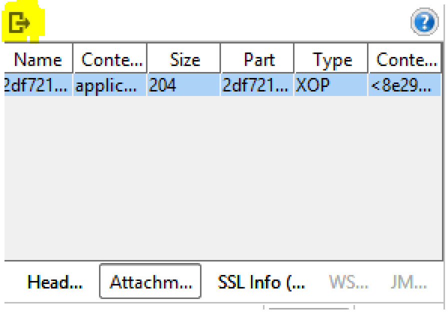
Name	Content t...	Size	Part	Type	ContentID	Cached
00681_17.zip	applicatio...	1058		UNKNOWN	TWETP_D...	☐

Name	Content t...	Size	Part	Type	ContentID
2df7216c...	applicati...	204	2df7216c...	XOP	<fb47695...

A... Headers ... Attachments... WS... WS-... JMS Head... JMS Property...
Headers (... Attachments (... SSL Info (3 cer... WSS (... JMS (...

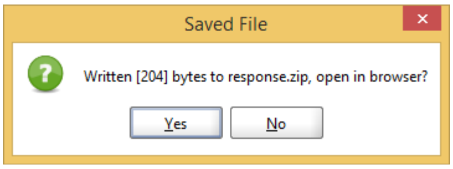
response time: 200ms (1289 bytes)

Click on an icon in order to download the attached file



Name	Conte...	Size	Part	Type	Conte...
2df721...	applic...	204	2df721...	XOP	<8e29...

Save the file under the name with zip extension and click OK. A dialogue box with the question whether to open the file will appear.



Saved File

Written [204] bytes to response.zip, open in browser?

Click OK to open the zip file. xml confirmation file is inside. An exemplary

file of a correct answer should be as follows:

```
<?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>
```

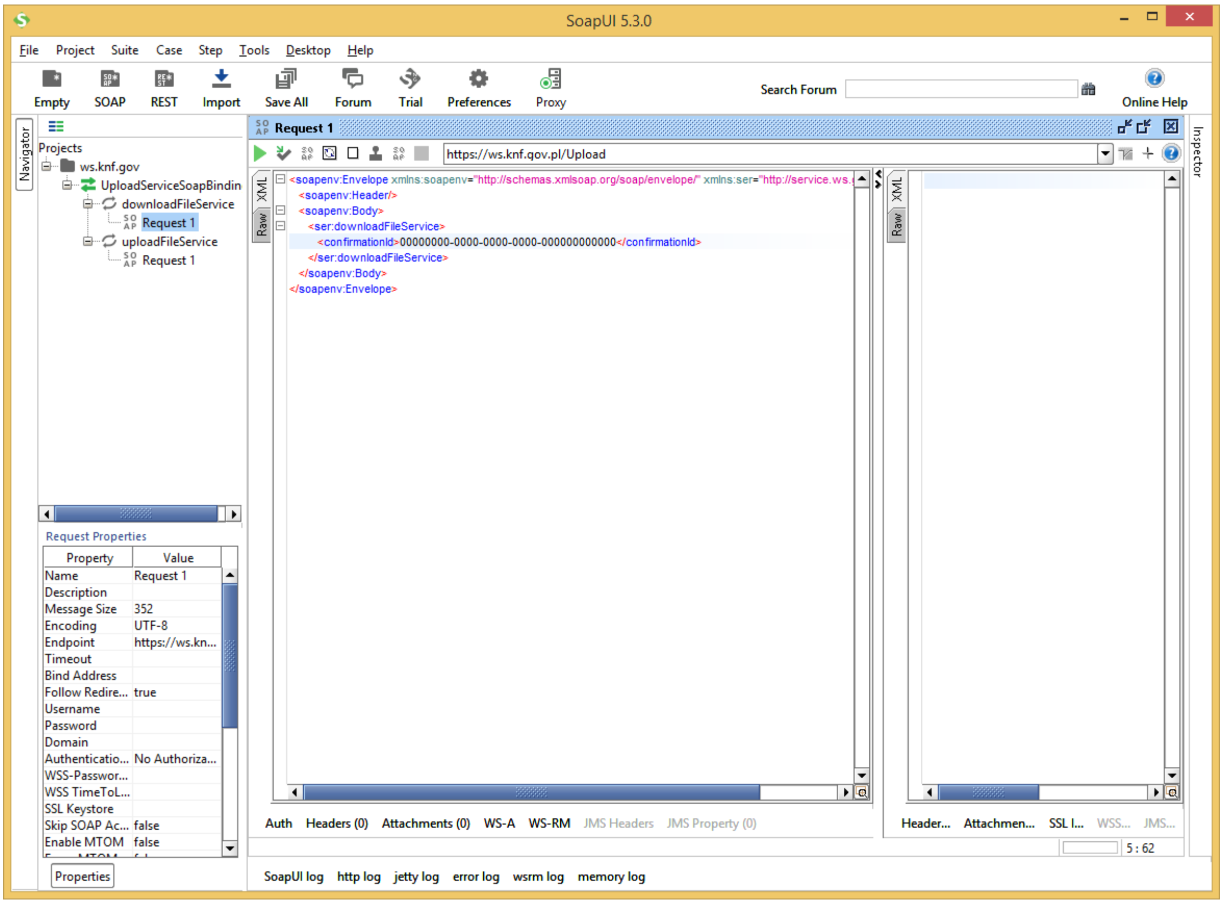
Any other status shall be considered to be the erroneous. In case of an error, the confirmationId confirmation identifier will be generated and the file will be processed further.

schema xsd answer file is located in pt. 7.

The file, after a correct acceptance to processing, goes to the queue where it will be further validated in detail for technical and substantive correctness.

After the completion of processing, the system will send the e-mail message about the completion of processing and, from this time onward, it will be possible to download the return message file.

To this end, it is appropriate to use the second method.


SoapUI 5.3.0
File Project Suite Case Step Tools Desktop Help
Empty SOAP REST Import Save All Forum Trial Preferences Proxy
Search Forum
Online Help
Navigator
Inspector
Projects
ws.knf.gov
UploadServiceSoapBindin
downloadFileService
Request 1
uploadFileService
Request 1
Request 1
XML
Raw
Auth Headers (0) Attachments (0) WS-A WS-RM JMS Headers JMS Property (0)
Header... Attachmen... SSL I... WSS... JMS...
5 : 62
Properties
SoapUI log http log jetty log error log wsrm log memory log

https://ws.knf.gov.pl/Upload

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

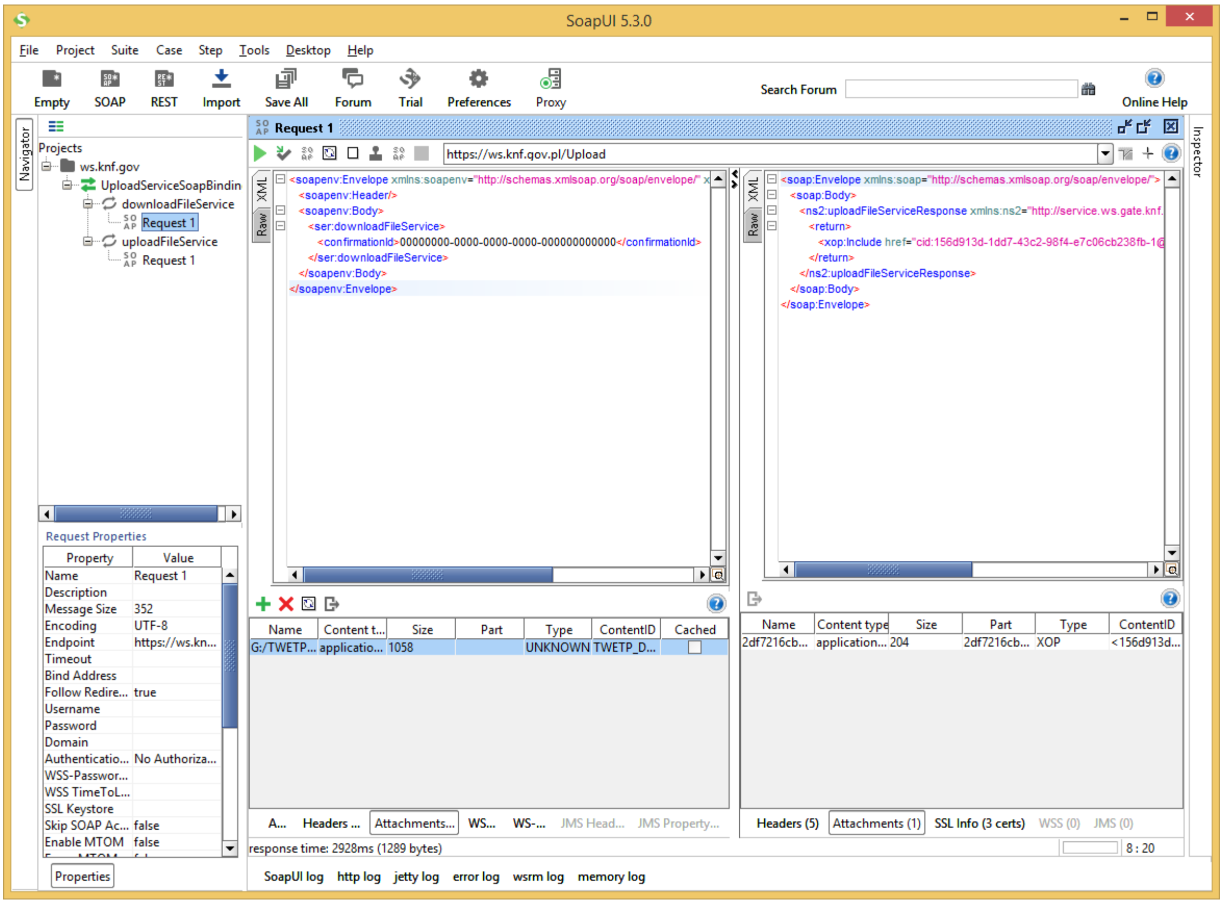
Request Properties

Property	Value
Name	Request 1
Description	
Message Size	352
Encoding	UTF-8
Endpoint	https://ws.kn...
Timeout	
Bind Address	
Follow Redire...	true
Username	
Password	
Domain	
Authenticatio...	No Authoriza...
WSS-Passwor...	
WSS TimeToL...	
SSL Keystore	
Skip SOAP Ac...	false
Enable MTOM	false

While calling this service, it is appropriate to provide a mandatory id confirmation parametre

```
<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>
```

In the answer, the method returns the file in the form of a compressed zip file in XML ISO20022 format.


SoapUI 5.3.0
File Project Suite Case Step Tools Desktop Help
Empty SOAP REST Import Save All Forum Trial Preferences Proxy
Search Forum
Online Help
Navigator
Projects
ws.knf.gov
UploadServiceSoapBindin
downloadFileService
Request 1
uploadFileService
Request 1
Request 1
XML
Raw
Inspector
A... Headers ... Attachments... WS... WS-... JMS Head... JMS Property...
Headers (5) Attachments (1) SSL Info (3 certs) WSS (0) JMS (0)
Properties
SoapUI log http log jetty log error log wsrm log memory log

https://ws.knf.gov.pl/Upload

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" x
  <soapenv:Header/>
  <soapenv:Body>
    <ser:downloadFileService>
      <confirmationId>00000000-0000-0000-0000-000000000000</confirmationId>
    </ser:downloadFileService>
  </soapenv:Body>
</soapenv:Envelope>
```

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:uploadFileServiceResponse xmlns:ns2="http://service.ws.gate.knf.
      <return>
        <xop:Include href="cid:156d913d-1dd7-43c2-98f4-e7c06cb238fb-1@
      </return>
    </ns2:uploadFileServiceResponse>
  </soap:Body>
</soap:Envelope>
```

Request Properties

Property	Value
Name	Request 1
Description	
Message Size	352
Encoding	UTF-8
Endpoint	https://ws.kn...
Timeout	
Bind Address	
Follow Redire...	true
Username	
Password	
Domain	
Authenticatio...	No Authoriza...
WSS-Passwor...	
WSS TimeToL...	
SSL Keystore	
Skip SOAP Ac...	false
Enable MTOM	false

Name	Content t...	Size	Part	Type	ContentID	Cached
G:/TWETP...	applicatio...	1058		UNKNOWN	TWETP_D...	□

Name	Content type	Size	Part	Type	ContentID
2df7216cb...	application...	204	2df7216cb...	XOP	<156d913d...

response time: 2928ms (1289 bytes)

8 : 20

5 File transfer via Web Service

The file should be attached to the parametre and sent by means of the MTOM standard. All files are in XML ISO20022 format. Each file consists of a general header, a Businness Application Header, and an XML data file. applicable XSD schemes are presented below

- head.003.001.01.xsd BAH header scheme for all files
- head.001.001.01_ESMAUG_1.0.0.xsd scheme for all files

TRANSPARENCY module files are files acquired from DATETR, DATNTR, DATEQU, DATNQU markets, XSD schemes required

- file: DATETR scheme DRAFT5auth.032.001.01_ESMAUG_DATETR_1.0.0.xsd
- file DATNTR scheme DRAFT5auth.033.001.01_ESMAUG_DATNTR_1.0.1.xsd
- file DATNTR scheme DRAFT5auth.033.001.01_ESMAUG_DATNTR_1.0.1.xsd
- file DATNQU scheme DRAFT5auth.041.001.01_ESMAUG_DATNQU_1.0.0.xsd

files for TREM - files DATTRA

- scheme for file DRAFT15auth.016.001.01_ESMAUG_Reporting_1.0.3

files for RDS – DATINS and DATNWD:

- file DATINS scheme DRAFT13auth.017.001.01_ESMAUG_DATINS_1.0.0.xsd
- file DATNWD scheme DRAFT4auth.039.001.01_ESMAUG_DATNWD_1.0.0.xsd

file for Dobuble Volume Cap – DATDVC:

- file DATDVC scheme MiFIR_DRAFT5auth.035.001.01- Trading Volume Cap Reporting.xsd

File names:

a) for DATETR; DATNTR; DATEQU; DATNQU; according to ESMA documentation.
b) For DATDVC:

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

Wher
e:
Receiver – NCAPL
FileType – DATDVC
System – DVCAP
MIC – T+kod MIC
FileNumber – file unique number
Year – last two digits of a year

Example: **NCAPL_DATDVC_DVCAP_TXWAR_001234_18**

c) For DATINS; DATNWD:

MIC_FileType_Date_FileNumber
(4x) (6x) (8x) (3x)
Where:
MIC – MIC code of an entity
FileType – DATINS or DATNWD
Date – date in the YYYYMMDD format
FileNumber – Subsequent file number on a given day. The first file on a given day has a 000 number

Example: **WBON_DATINS_20171220_000**
XWAR_DATNWD_20180123_001

d) For DATTRA:

Sender_FileType_Receeipient_Key1_Key2_Year

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

Where:

Sender – LEI code of an

entity **FileType** – DATTRA

Recipient – PFSA

Key1 – ARM or FIN (investment company)

Key2 – a unique file number from a given sender

Year – last two digits of a year

Example: **1234567890ABCDEFGHIJ_DATTRA_PFSA_FIN_000001_17**

ABCDEFGHIJ1234567890_DATTRA_PFSA_ARM_987654_17

6 Receiving the confirmation of a file transfer

After successful transfer of the file, the methods returns the compressed answer file. The answer file in the zip archive format, which should contain xml file saved in the ISO 20022 format after decompressing. Answer files have their name created in the following way:

FDBETR file is the answer for DATETR file;

FDBNTR file is the answer for DATNTR file;

FDBEQU file is the answer for DATEQU file;

FDBNQU file is the answer for DATNQU file;

FDBINS file is the answer for DATINS file;

FDBDVC file is the answer for DATDVC file

FDBNWD file is the answer for DATNWD file

Auth.031.001.01_ESMAUG_FDB_1.0.0.xsd file is an applicable scheme XSD for the above-

mentioned files

FDBTRA file is the answer for DATTRA file;

DRAFT4auth.031.001.01_ESMAUG_FDBTRA_1.0.1.xsd file is an applicable scheme XSD for the

above-mentioned file

In case of DATTRA file, „Recipient” and „Sender” boxes are changed. Example:
Incoming file: **1234567890ABCDEFGHIJ_DATTRA_PFSA_FIN_000001_17**

Answer file: **PFSA_FDBTRA_1234567890ABCDEFGHIJ _FIN_000001_17**

7 XSD Scheme for XML answers for the uploadFileService method

```
<?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 Metrics of changes in the document

Version	**Change description**	**Document date**
1.0	New document	2017-12-22
1.1	**Chapter 3:** link to the website: "access to the Webserwis KNF service" **Chapters 5 -6:** DATDVC; DATINS; DATNWD files service was added. Description for FDB answer file was extended **Chapter 7:** correction of the schema from *<xs:element name="recived"> to <xs:element name="received">* **Appendix no. 1; point 1) Address of the service:** link to the test environment	2018-05-07
1.2	**Chapter 6:** Change of FDBTRA schema for DATTRA files	2018-10-22