Instrukcja wymiany danych elektronicznych pomiędzy PSG a ZUD.

Wersja: 1.0

Spis treści:

1 Cel Instrukcji.

Niniejsza Instrukcja określa procedury korzystania ze standardów wymiany danych, w szczególności w zakresie protokołu wymiany, formatu danych i sieci.

2 Definicje.

PSG - Polska Spółka Gazownictwa sp. z o.o. (OSD)
PZD - Pojedyncze Zlecenie Dystrybucji,
ZUD - Zleceniodawca Usługi Dystrybucji
OSD - Operator Systemu Dystrybucyjnego
Umowa – umowa o świadczenie usług dystrybucji paliwa gazowego zawarta z Polską Spółką Gazownictwa sp. z o.o.

3 Protokoły komunikacji dla standardów wymiany danych.

3.1 Protokół dla standardu EDI.

Opis standardu EDI znajduje się na stronie internetowej PSG w zakładce Dla Klienta / Sprzedawca paliwa gazowego / Umowa dystrybucyjna / EDI (https://www.psgaz.pl/edi). Wymiana danych w standardzie XML/EDI odbywa się poprzez protokół AS4 opisany w rozdziale 4 oraz protokół SOAP opisany w rozdziale 5.

3.2 Protokoły dla alternatywnych standardów wymiany danych.

Alternatywnymi Standardami wymiany danych oraz dokumentów pomiędzy OSD oraz ZUD są:

1. Serwis eBOK – aplikacja internetowa udostępniona przez OSD umożliwiająca wymianę danych oraz dokumentów pomiędzy OSD a ZUD w ramach procesu obsługi PZD (dalej „Standard eBOK") – wymiana dwukierunkowa OSD <-> ZUD; Dla serwisu eBok komunikacja pomiędzy OSD a ZUD jest realizowana z wykorzystaniem przeglądarki internetowej i szyfrowanego protokołu HTTPS (Hypertext Transfer Protocol Secure). Instrukcja dla tego standardu znajduje się w . załączniku nr 1 (Instrukcja obsługi aplikacji Elektroniczne Biuro Obsługi Klienta)
2. Serwis SFTP – udostępniona przez OSD usługa umożliwiająca publikowanie plików zawierających dane oraz dokumenty za pomocą protokołu komunikacyjnego SFTP (dalej „Standard SFTP") – wymiana jednokierunkowa OSD -> ZUD. Dla usługi SFTP komunikacja pomiędzy OSD a ZUD jest realizowana z wykorzystaniem szyfrowanego

protokołu SFTP (SSH File Transfer Protocol). Opis komunikacji dla tego standardu znajduje się w rozdziale 7 poniżej.

3.3 Procedura podłączenia nowego podmiotu.

Zasady udostępniania standardów wymiany danych określa Umowa.

3.3.1 Podłączenie w ramach Standardu EDI.

1. ZUD dostosowuje swoje systemy informatyczne do warunków technicznych określonych w punkcie 4 lub 4 niniejszej instrukcji.
2. OSD weryfikuje, czy ZUD spełnił niezbędne warunki techniczne wymagane do rozpoczęcia wymiany danych oraz określa termin jej rozpoczęcia.
3. ZUD dostarcza do OSD certyfikat, którym będą podpisywane i szyfrowane komunikaty.
4. ZUD upewnia się, że certyfikat serwera OSD jest zaufany przez urząd certyfikacyjny (CA) przed wysłaniem danych.

3.3.2 Podłączenie do Serwisu eBOK.

1. ZUD otrzymuje dostęp do Serwisu eBOK na podstawie załączników nr 4 i 5 do umowy dystrybucyjnej

3.3.3 Podłączenie do Serwisu SFTP.

1. ZUD dostosowuje się do warunków technicznych określonych w punkcie 7.1 niniejszego dokumentu.
2. ZUD dostarcza do OSD swój klucz publiczny SSH, który będzie służył potwierdzeniu jego tożsamości.
3. W celu uzyskania pewności, iż klucz publiczny SSH został przekazany przez uprawniony podmiot, OSD dopuszcza następujące możliwości jego dostarczenia:
   a) osobisty, przez osobę wskazaną w Załączniku nr 4 do Umowy, legitymującą się ważnym dokumentem tożsamości, w siedzibie Spółki.
   b) pocztą tradycyjną, wysyłając klucz publiczny SSH na nośniku cyfrowym wraz ze stosownym oświadczeniem, podpisanym przez upoważnioną osobę.
   c) pocztą elektroniczną, wysyłając klucz publiczny SSH do autoryzacji ZUD w wymianie komunikatów na adres edifact@psgaz.pl. W celu dokonania weryfikacji czy otrzymany klucz SSH należy do uprawnionego ZUD, OSD wymaga elektronicznego podpisania przesłanego klucza, przez osobę wskazaną w Załączniku nr 4 do Umowy, jej kwalifikowanym podpisem cyfrowym.

4. ZUD zobowiązuje się do dostarczenia klucza SSH spełniającego wymagania podane w punkcie 7.1 oraz do niezwłocznego poinformowania OSD, jeżeli klucz SSH straci zaufanie (dostanie się w posiadanie nieuprawnionego podmiotu).

4 Protokół AS4.

4.1 Wprowadzenie i informacje ogólne.

Poniższy opis przedstawia wymagania techniczne umożliwiające zbudowanie komunikacji po protokole AS4 pomiędzy OSD a ZUD.

Zakłada się, że ZUD posiada wiedzę, umiejętności oraz zasoby niezbędne do zbudowania komunikacji z OSD po protokole AS4 wg. poniższej instrukcji.

4.1.1 Protokół Applicability Statement 4 (AS4).

Applicability Statement 4 (AS4) jest protokołem komunikacji opisującym bezpieczne oraz niezawodne przesyłanie komunikatów przez internet w komunikacji b2b (business-to-business). Protokół ten jest standardem od roku 2013, a jego celem jest rozwinięcie funkcjonalności poprzednich standardów AS, w szczególności popularnego AS2.

AS4 działa w oparciu o profil zgodności OASIS ebMS 3.0, łącząc trzy popularne i sprawdzone technologie:
- WS Security (Web Service Security)
- MIME (Multipurpose Internet Mail Extension)
- SOAP (Simple Objec Access Protocol)

Połączenie tych technologii umożliwia m.in. podpisywanie cyfrowe, szyfrowanie, przesyłanie załączników w dowolnym formacie, a w razie problemów w komunikacji obsługę komunikatów błędów. AS4 obsługuje wzorzec komunikacji *push* i *pull*.

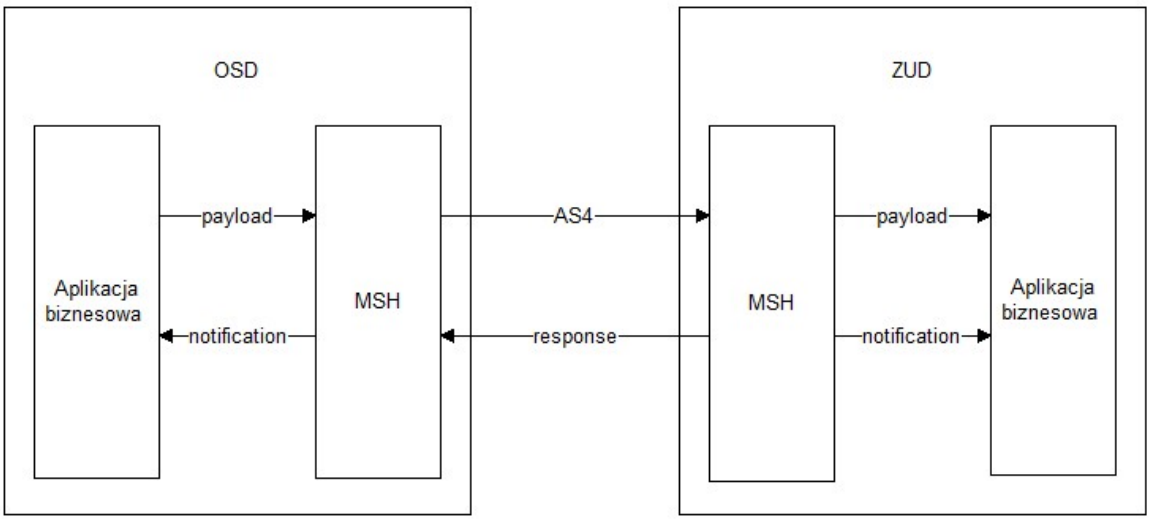
4.2 Komunikacja pomiędzy ZUD i OSD.

Po stronie OSD zdefiniowane zostaną dwa przepływy, jeden wysyłający dane do ZUD, drugi odbierający dane od ZUD. Adresy do komunikacji podane są w dalszej części dokumentacji.

4.2.1 Komunikacja OSD do ZUD.

Komunikacja OSD do ZUD odbywa się wg. wzorca one-way/push. W tym wzorcu partner inicjujący (MSH po stronie OSD) wysyła komunikat do partnera odbierającego (MSH po stronie ZUD) i synchronicznie otrzymuje odpowiedź.

Diagram poniżej przedstawia obrazowo sposób komunikacji OSD do ZUD za pomocą handlerów AS4 Messaging Service Handler (MSH). Na schemacie *payload* reprezentuje przesyłany komunikat.



4.2.1.1 Identyfikacja partnerów.

Identyfikacja partnerów ZUD, w stronę OSD -> ZUD odbywa się w polu PartyId, zgodnie ze zdefiniowanym w specyfikacji AS4 schematem.

Przykład poprawnie zdefiniowanych pól poniżej:

```
<eb:PartyInfo>
   <eb:From>
      <eb: PartyId type ="string">PSG</eb:PartyId>
      <eb:Role>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/initiator</eb:Role>
   </eb:From>
   <eb:To>
      <eb:PartyId type="string">ZTST</eb:PartyId>
      <eb:Role>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/responder</eb:Role>
   </eb:To>
</eb:PartyInfo>
```

W przykładzie dla konkretnego ZUD został przypisany identyfikator ‘ZTST’. Jest to wartość

przykładowa, poprawne identyfikatory ZUD zostaną przypisane partnerom w procesie przyłączania ZUD.

Identyfikacja odbywać się będzie również poprzez wartość pola <ZUD> w nagłówku komunikatu

4.2.1.2 Podpisywanie wiadomości.

W komunikacji między partnerami użyto następujących standardów podpisywania cyfrowego:

Signing digest algorithm	Sha256
Signature algorithm	Rsa-sha256
Signature canonicalization method	Exc-c14n – Exlusive

Weryfikacja podpisu elektronicznego w obie strony odbywać się będzie za pomocą Self Signed Certificate. W tym celu niezbędne jest, aby w procesie przyłączania ZUD do OSD podmioty umożliwiły sobie wymianę certyfikatu klucza użytego do podpisywania dokumentów.

OSD zastrzega sobie możliwość zmiany obsługiwanych algorytmów kryptograficznych na mocniejsze.

4.2.1.3 Szyfrowanie zawartości.

Szyfrowanie komunikatów po protokole AS4 odbywać się będzie z użyciem certyfikatu Self Signed Certificate udostępnionych stronom w procesie przyłączania.

W usłudze użyto następującego algorytmu szyfrowania:

Encryption algorithm	AES256-CBC

OSD zastrzega sobie możliwość zmiany obsługiwanych algorytmów kryptograficznych na mocniejsze.

4.2.1.4 Komunikat odpowiedzi.

MSH po stronie ZUD musi synchronicznie wysyłać komunikaty potwierdzenia odbioru lub komunikaty błędu (reciepe) zgodne ze standardem AS4, co jest niezbędne do zatwierdzenia transakcji po stronie OSD. Otrzymanie przez OSD potwierdzenia odbioru (bez komunikatu błędu) jest równoznaczne z dostarczeniem komunikatu przez OSD do ZUD. Usługa po stronie ZUD przy każdej transakcji dostanie także komunikat reciepe zgodny ze standardem AS4, zawierający potwierdzenie odbioru, lub z komunikatem błędu w przypadku wystąpienia błędów komunikacji.

Szczegółowa dokumentacja wymienionych funkcjonalności znajduje się pod adresem: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html

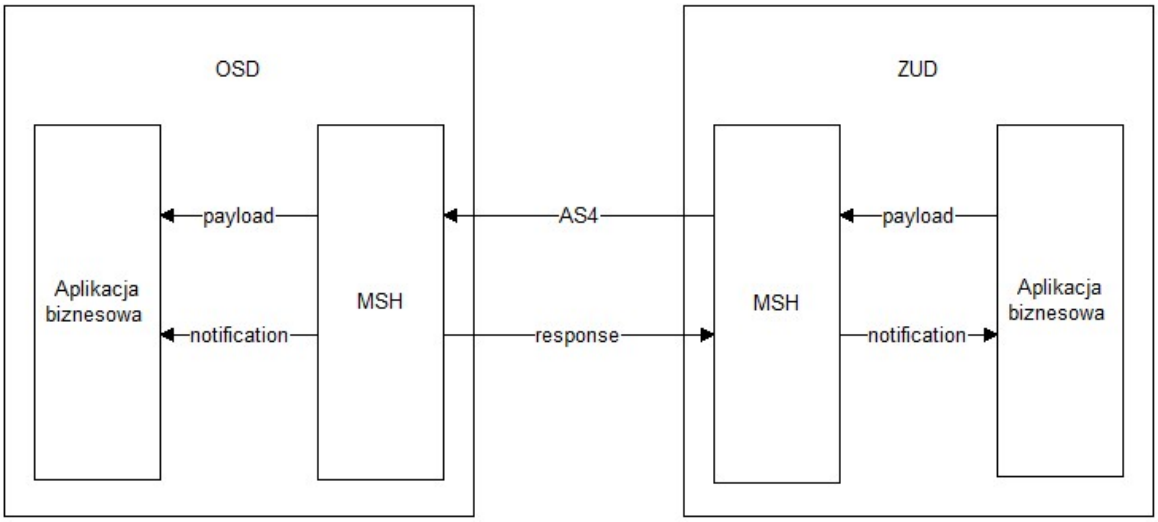
4.2.1.5 Adresy serwera ZUD.

W ramach komunikacji OSD do ZUD, żeby zestawić połączenie, ZUD musi podać swój adres usługi komunikacji po protokole AS4.

4.2.2 Komunikacja ZUD do OSD.

Komunikacja OSD do ZUD odbywa się wg. wzorca one-way/push. W tym wzorcu partner inicjujący (MSH po stronie OSD) wysyła komunikat do partnera odbierającego (MSH po stronie ZUD) i synchronicznie otrzymuje odpowiedź.

Diagram poniżej przedstawia obrazowo sposób komunikacji OSD do ZUD za pomocą handlerów AS4 Messaging Service Handler (MSH). Na schemacie *payload* reprezentuje przesyłany komunikat.



4.2.2.1 Identyfikacja partnerów.

Identyfikacja partnerów w stronę ZUD do OSD odbywa się poprzez pola *PartyId* oraz zdefiniowane wg. specyfikacji AS4 pola *Role*.

Przykład poprawnie zdefiniowanych pól poniżej:

```
<eb:PartyInfo>
   <eb:From>
      <eb:PartyId type="string">ZTST</eb:PartyId>
      <eb:Role>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/initiator</eb:Role>
   </eb:From>
   <eb:To>
      <eb:PartyId     type="string">PSG</eb:PartyId>
      <eb:Role>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/responder</eb:Role>
   </eb:To>
</eb:PartyInfo>
```

Powyżej dla ZUD został przypisany identyfikator ‘ZTST’. Jest to wartość przykładowa, poprawne identyfikatory ZUD zostaną przypisane partnerom w procesie przyłączania ZUD.

4.2.2.2 Podpisywanie wiadomości.

W komunikacji między partnerami użyto następujących standardów podpisywania cyfrowego:

Signing digest algorithm	Sha256

Signature algorithm	Rsa-sha256
Signature canonicalization method	Exc-c14n – Exlusive

Weryfikacja podpisu elektronicznego w obie strony odbywać się będzie za pomocą Self Signed Certificate. W tym celu niezbędne jest, aby w procesie przyłączania ZUD do OSD podmioty umożliwiły sobie wymianę certyfikatu klucza użytego do podpisywania dokumentów.

4.2.2.3 Szyfrowanie zawartości.

Szyfrowanie komunikatów po protokole AS4 odbywać się będzie z użyciem certyfikatu Self Signed Certificate udostępnianego stronom w procesie przyłączania.

W usłudze użyto następującego algorytmu szyfrowania:

Encryption algorithm	AES256-CBC

4.2.2.4 Komunikat odpowiedzi.

MSH po stronie OSD synchronicznie wysyła komunikaty potwierdzenia odbioru lub komunikaty błędu (reciepe) zgodne ze standardem AS4, co jest niezbędne do zatwierdzenia transakcji po stronie ZUD. Otrzymanie przez ZUD potwierdzenia odbioru (bez komunikatu błędu) jest równoznaczne z dostarczeniem komunikatu przez ZUD do OSD. Usługa po stronie OSD przy każdej transakcji dostanie także komunikat reciepe zgodny ze standardem AS4, zawierający potwierdzenie odbioru, lub z komunikatem błędu w przypadku wystąpienia błędów komunikacji.

Szczegółowa dokumentacja wymienionych funkcjonalności znajduje się pod adresem: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html

4.2.2.5 Adresy serwera.

Adres serwera odbierającego komunikaty EDIFACT po AS4 na środowisku produkcyjnym: *b2b.psgaz.pl:7443 TCP*

Adres serwera odbierającego komunikaty EDIFACT po AS4 na środowisku testowym: *b2b-tst.psgaz.pl:7443 TCP*

W ramach komunikacji OSD do ZUD, żeby zestawić połączenie, ZUD musi podać swój adres usługi komunikacji po protokole AS4.

4.2.3 XML/Edifact.

Wymiana danych pomiędzy OSD i ZUD będzie odbywać się w formacie XML/EDIFACT, dołączanym w formie załącznika do komunikatu w formacie AS4 (payload).

5 Protokół SOAP

5.1 Wprowadzenie i informacje ogólne.

Poniższy opis przedstawia wymagania techniczne umożliwiające zbudowanie komunikacji WebService XML z użyciem komunikatu SOAP, pomiędzy OSD a ZUD. Komunikaty wychodzące i przychodzące będą walidowane zgodnie z dołączonym do niniejszego dokumentu schematem WSDL.

Zakłada się, że ZUD posiada wiedzę, umiejętności oraz zasoby niezbędne do zbudowania komunikacji z OSD wg. poniższej instrukcji.

5.1.1 Komunikat SOAP

SOAP (Simple Object Access Protocol) jest popularnym protokołem komunikacyjnym opartym o XML. Pełna dokumentacja protokołu SOAP znajduje się na oficjalnej stronie W3C (World Wide Web Consortium) pod adresem: https://www.w3.org/TR/soap/ .

5.1.2 Schemat WSDL

WSDL (Web Services Description Language) jest popularnym, opartym o XML językiem definiowania usług internetowych. Pełna dokumantacja WSDL znajduje się na oficjalnej stronie W3C (World Wide Web Consortium) pod adresem: https://www.w3.org/TR/wsdl/ .

Poniżej znajdują się pliki schematu WSDL:

5.2 Komunikacja pomiędzy ZUD i OSD.

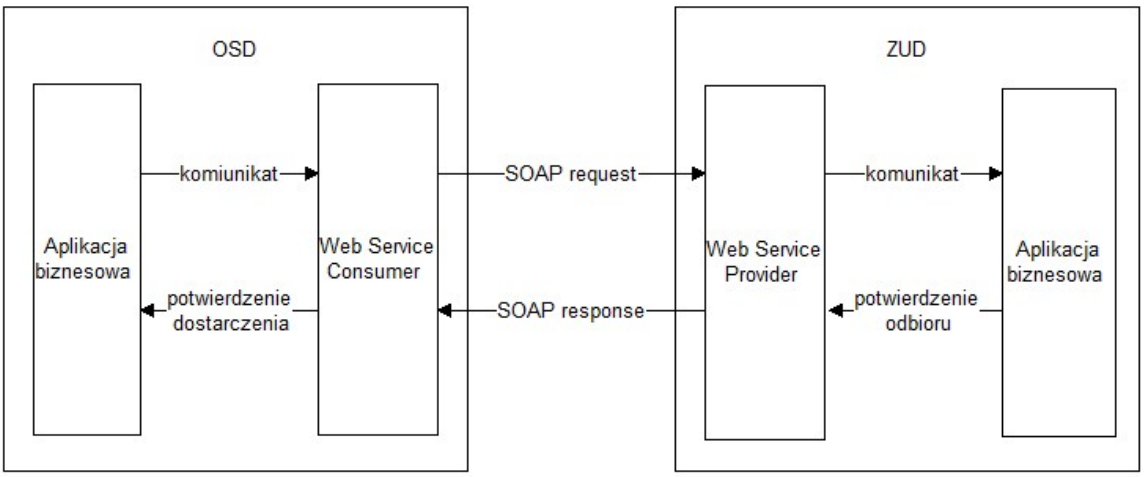
Po stronie OSD zdefiniowane zostaną dwa przepływy, jeden wysyłający dane do ZUD, drugi odbierający dane od ZUD. Adresy do komunikacji podane są w dalszej części dokumentacji.

Wg. przyjętego rozwiązania architektonicznego po każdej stronie komunikacji walidacja wiadomości odbywa się względem tego samego kontraktu WSDL, dołączonego do niniejszej dokumentacji w sekcji 5.1.2

5.2.1 Komunikacja OSD do ZUD.

Komunikacja OSD do ZUD odbywa się z użyciem technologii Web Service w oparciu o kontrakt WSDL dołączony do niniejszego dokumentu. Protokołem komunikacji, zgodnie ze standardem WS, jest SOAP.

Diagram poniżej przedstawia obrazowo sposób komunikacji OSD do ZUD za pomocą wywołania usługi Web Service. Szczegóły rozwiązania po stronie ZUD zależne będą od wybranego rozwiązania architektonicznego.



5.2.1.1 Identyfikacja partnerów.

Identyfikacja partnerów ZUD odbywa się po wartości CN (Common Name) certyfikatu, którego użyto do utworzenia połączenia szyfrowanego HTTPS.

5.2.1.2 Bezpieczeństwo

Przenoszenie komunikatów odbywać się będzie za pomocą szyfrowanej wersji protokołu HTTP – HTTPS, przy użyciu protokołu TLS w wersji 1.2. OSD korzysta z bazy certyfikatów zaufanych (truststore), w związku z czym konieczne jest udostępnienie certyfikatu ZUD w

trakcie procedury przyłączania w celu dodania certyfikatu do bazy certyfikatów zaufanych. Połączenia odbywające się z użyciem niezaufanych certyfikatów zostaną odrzucone.

5.2.1.3 Komunikat odpowiedzi.

Komunikaty odpowiedzi z OSD zgodne z wykorzystanym w komunikacji kontraktem WSDL zostaną wysłane dopiero w chwili potwierdzenia odebrania komunikatu od ZUD przez aplikację biznesową OSD.

W przypadku błędów komunikacji, identyfikacji, walidacji lub innych, zostanie odesłany komunikat soap fault z informacją o znanym powodzie wystąpienia błędu w treści komunikatu.

W przypadku braku odpowiedzi komunikatem odpowiedzi zgodnym ze kontraktem WSDL użytym w przetwarzaniu należy przyjąć, że strona OSD nie odebrała komunikatu.

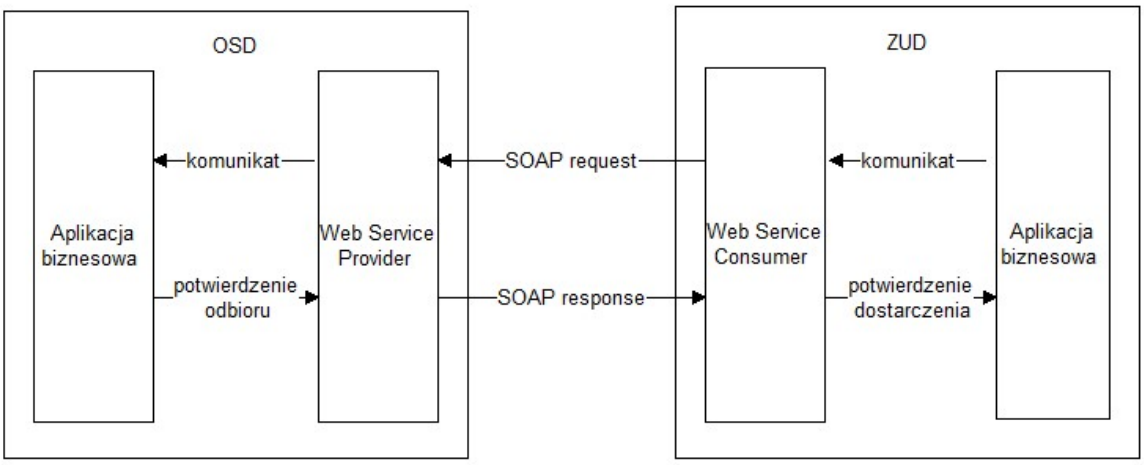
5.2.1.4 Adresy serwera.

W ramach komunikacji OSD do ZUD, żeby zestawić połączenie, ZUD powinien dostarczyć adres wystawionej usługi Web Service do komunikacji z OSD.

5.2.2 Komunikacja ZUD do OSD.

Komunikacja ZUD do OSD odbywa się z użyciem technologii Web Service w oparciu o kontrakt WSDL dołączony do niniejszego dokumentu. Protokołem komunikacji, zgodnie ze standardem WS, jest SOAP.

Diagram poniżej przedstawia obrazowo sposób komunikacji ZUD do OSD za pomocą wywołania usługi Web Service. Szczegóły rozwiązania po stronie ZUD zależne będą od wybranego rozwiązania architektonicznego.



5.2.2.1 Identyfikacja partnerów.

Połączenie między OSD-ZUD odbywa się w relacji jeden do wielu, wobec czego przyjmuje się, że identyfikacja OSD dla partnerów ZUD nie jest konieczna.

5.2.2.2 Bezpieczeństwo.

Przenoszenie komunikatów odbywać się będzie za pomocą szyfrowanej wersji protokołu HTTP – HTTPS, przy użyciu protokołu TLS w wersji 1.2. Zaleca się weryfikację po certifikacie klucza publicznego umieszczonego w bazie kluczy zaufanych (truststore). Udostępnienie certyfikatu OSD odbędzie się w trakcie procedury przyłączania partnera ZUD do komunikacji. Zaleca się odrzucanie komunikacji z użyciem certyfikatów niezaufanych z uwagi na wysokie ryzyko kompromitacji połączenia OSD-ZUD.

OSD zastrzega sobie możliwość zmiany obsługiwanych algorytmów kryptograficznych i protokołów komunikacyjnych na mocniejsze.

5.2.2.3 Komunikat odpowiedzi.

W przypadku odebrania komunikatu od ZUD i po dostarczeniu go do aplikacji biznesowej, OSD poinformuje partnera ZUD komunikatem Soap Response zgodnym ze schematem WSDL o poprawności odebrania komunikatu.

W przypadku błędów komunikacji OSD odeśle komunikat Soap Fault z informacją o znanym błędzie w treści komunikatu.

W przypadku braku odpowiedzi od OSD należy przyjąć, że komunikat nie został poprawnie dostarczony do OSD.

5.2.2.4 Adresy serwera.

W ramach komunikacji OSD do ZUD, żeby zestawić połączenie, ZUD powinien dostarczyć adres wystawionej usługi Web Service do komunikacji z OSD.

Adres serwera odbierającego komunikaty EDIFACT po AS4 na środowisku produkcyjnym: *b2b.psgaz.pl:7843 TCP*

Adres serwera odbierającego komunikaty EDIFACT po AS4 na środowisku testowym: *b2b-tst.psgaz.pl:7843 TCP*

6 Serwis eBOK.

6.1 Informacje wstępne.

Serwis eBOK (elektroniczne Biuro Obsługi Klienta) jest platformą udostępniającą wymianę informacji między innymi za pośrednictwem dokumentów PZD.
Aplikacja umożliwia w szczególności:

- zgłaszanie dokumentów PZD,
- monitorowanie przeprowadzanych procesów,
- korektę zgłoszonych dokumentów PZD gdy jest to wymagane,
- anulowanie procesu,
- wgląd do operatywnych danych pomiarowych z punktów wyjścia z systemu dystrybucyjnego, w których ZUD świadczy usługę sprzedaży paliwa gazowego

Instrukcja obsługi Serwisu eBOK Polskiej Spółki Gazownictwa znajduje się w *Załączniku nr 1* do niniejszej Instrukcji.

6.2 Dostęp do usługi.

Usługa jest dostępna pod adresem: https://ebok.psgaz.pl

6.3 Ograniczenia usługi.

Usługa dostępna jest wyłącznie dla:

- Wszystkich Punktów Wyjścia typu WR,
- Punktów Wyjścia typu WS z obszarów taryfowych Zabrze oraz Gdańsk

7 Serwis SFTP.

7.1 Opis wymagań technicznych:

a) Serwer dostępny jest pod adresem sftp.psgaz.pl i udostępnia możliwość wymiany danych za pomocą szyfrowanego protokołu SFTP (SSH File Transfer Protocol)

b) Usługa SFTP jest dostępna w sieci Internet pod adresem **sftp.psgaz.pl** i OSD zastrzega sobie możliwość zmiany adresu IP serwisu

c) Serwis wymaga szyfrowania za pomocą algorytmów uznanych powszechnie za bezpiecznie i OSD zastrzega sobie możliwość zmiany obsługiwanych algorytmów na mocniejsze

d) Usługa SFTP działa na porcie TCP 75

e) ZUD będzie miał założone konta w systemie OSD

f) Dla ZUD zostanie włączona możliwości logowania się z wykorzystaniem klucza SSH przekazanego przez ZUD.

g) Korzystając z usługi SFTP, ZUD może wykorzystywać klucz SSH-2 RSA o długości 4096 bitów lub klucz ED25519. OSD zastrzega sobie możliwość zmiany obsługiwanych algorytmów na mocniejsze.

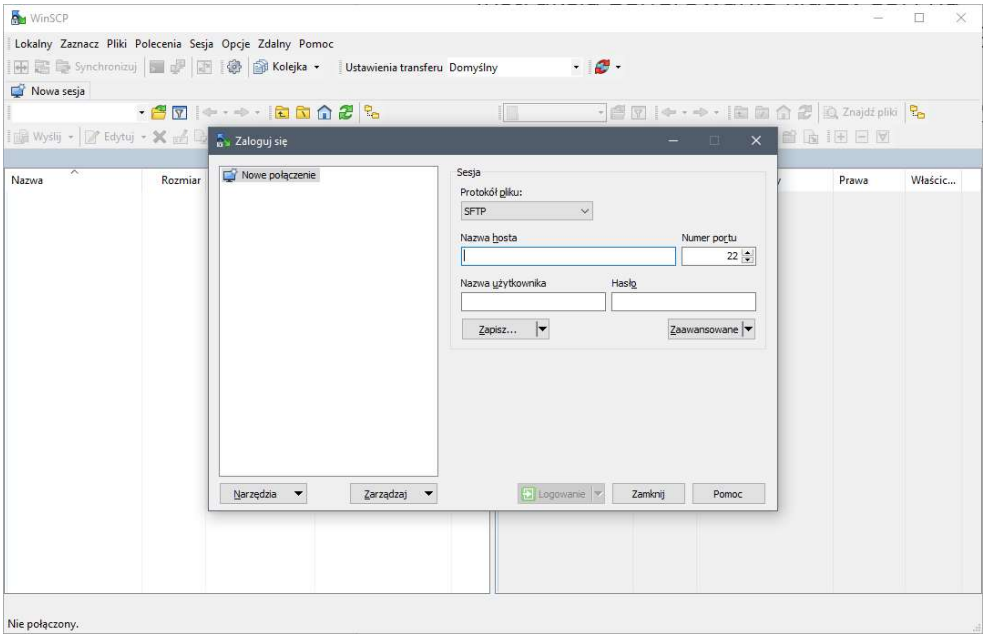
h) ZUD może korzystać z serwera SFTP za pomocą dowolnego klienta, na dowolnej platformie systemowej obsługującej oferowane przez serwer SFTP protokoły i algorytmy kryptograficzne. Zalecane jest korzystanie z klienta SFTP w jego aktualnej wersji (np. WinSCP https://winscp.net/ lub FileZilla https://filezilla-project.org/).

7.2 Instrukcja generowania kluczy SSH na potrzeby połączenia z serwerem SFTP.

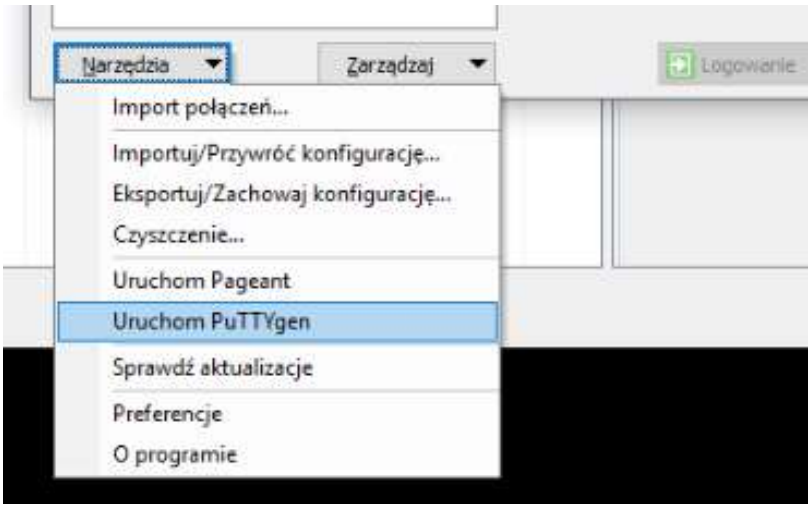
Opisano poniżej proces generowania kluczy prywatnego i publicznego niezbędnego do nawiązania szyfrowanego połączenia z serwem OSD. Opis bazuje na bezpłatnym kliencie WinSCP, którego można pobrać ze strony https://winscp.net/

a) Generowanie kluczy SSH

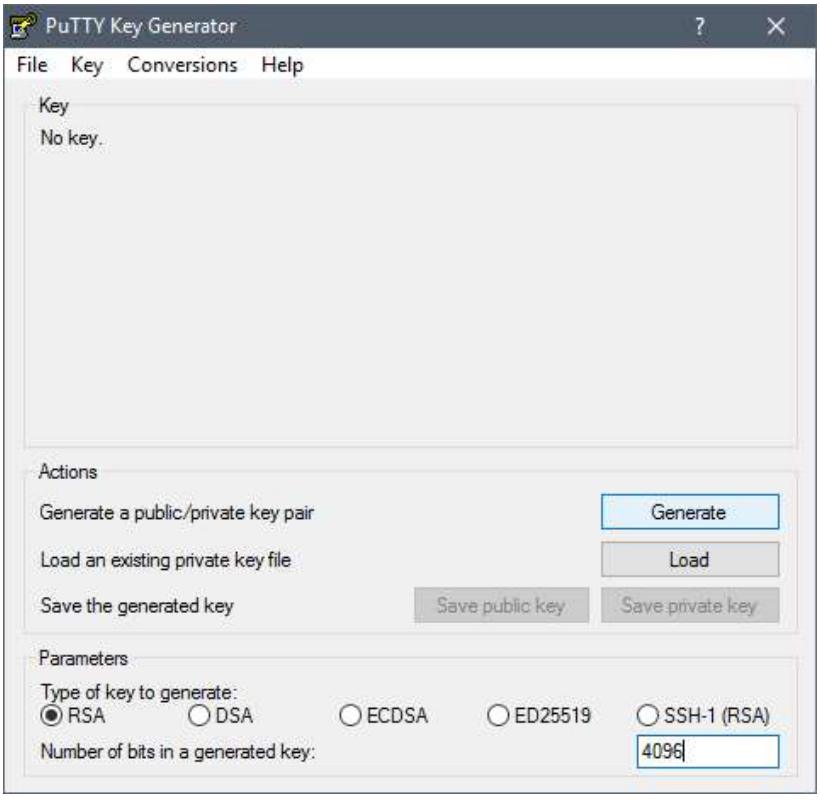
Pobieramy i instalujemy klienta WinSCP, następnie uruchamiamy go:



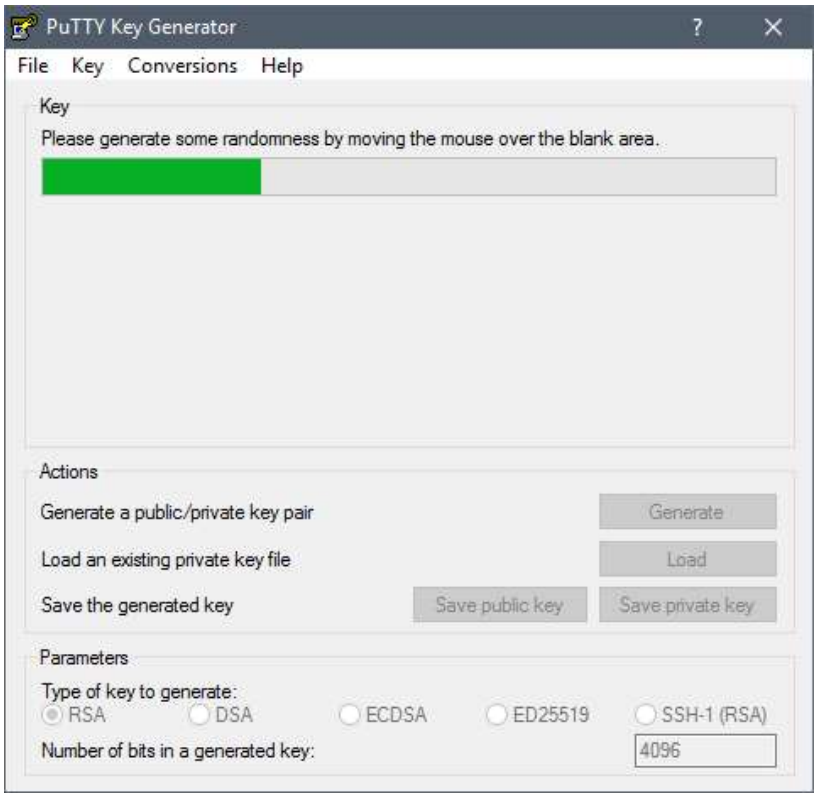
b) Generujemy parę kluczy: prywatny oraz publiczny – w tym celu rozwijamy menu *Narzędzia* widoczne w lewym dolnym rogu ekranu i wybieramy *Uruchom PuTTYgen*:



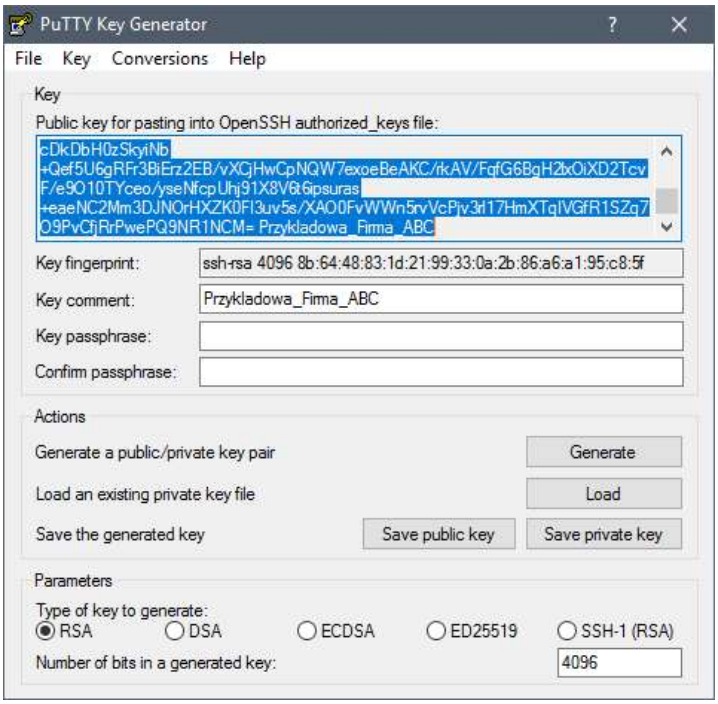
c) Zaznaczamy typ klucza RSA i ustawiamy jego długość na 4096 (jak na załączonym zrzucie ekranu), bądź wybieramy klucz ED25519. Następnie klikamy na przycisk ***Generate*:**



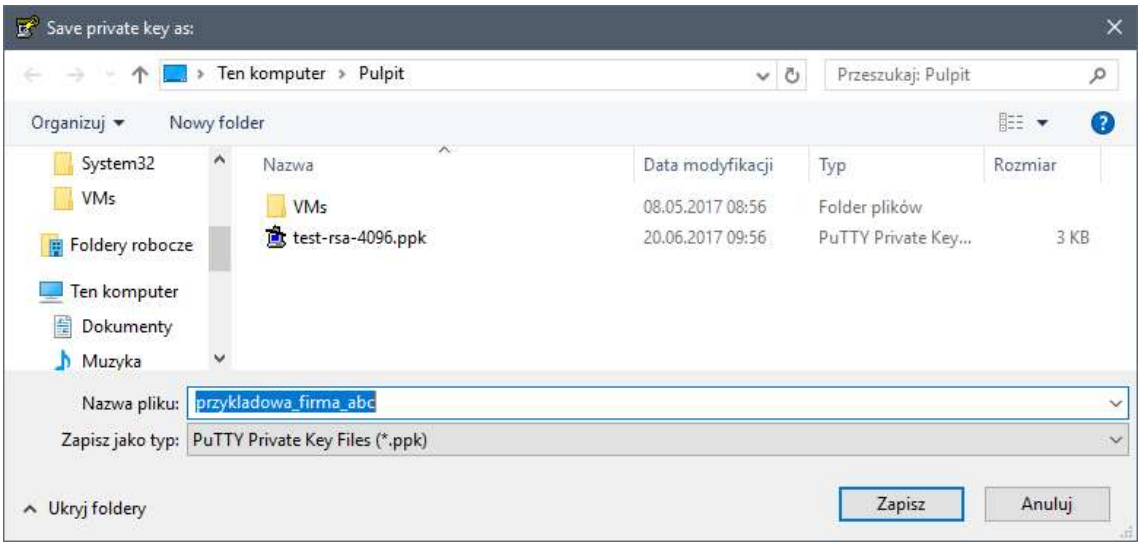
d) W trakcie generowania klucza poruszamy myszą nad oknem programu (zgodnie z komunikatem w aplikacji):



e) Po chwili klucz jest wygenerowany. Należy uzupełnić pole z komentarzem, umieszczając w nim nazwę firmy(ZUD):

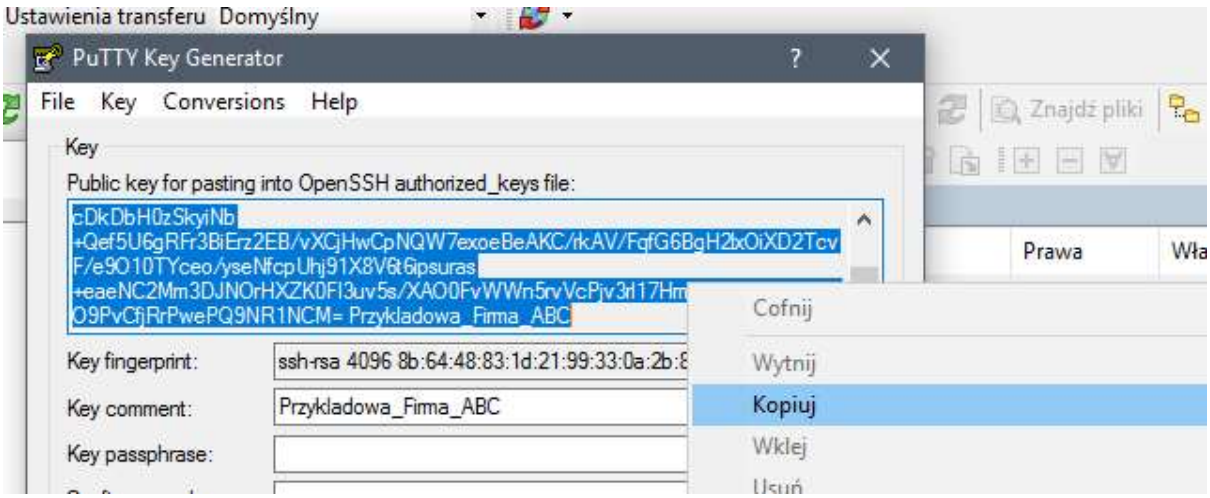


f) Następnie zapisujemy plik z kluczem prywatnym klikając na przycisk *Save private key*.



Uwaga! Należy zadbać o to, by miejsce jego zapisu nie było ogólnodostępne i plik nie dostał się w nieuprawnione ręce.

g) Zawartość klucza publicznego kopiujemy w całości i wysyłamy na adres e-mail: edifact@psgaz.pl lub dostarczamy za pomocą innych metod opisanych w punkcie „Podłączenie do Serwisu SFTP”.



Uwaga! Klucz rozpoczyna się od frazy *ssh-rsa* (dla kluczy RSA) lub *ssh-ed25519* (dla kluczy ED25519), a kończy się na podanej nazwie ZUD.

7.3 Definicja połączenia SFTP

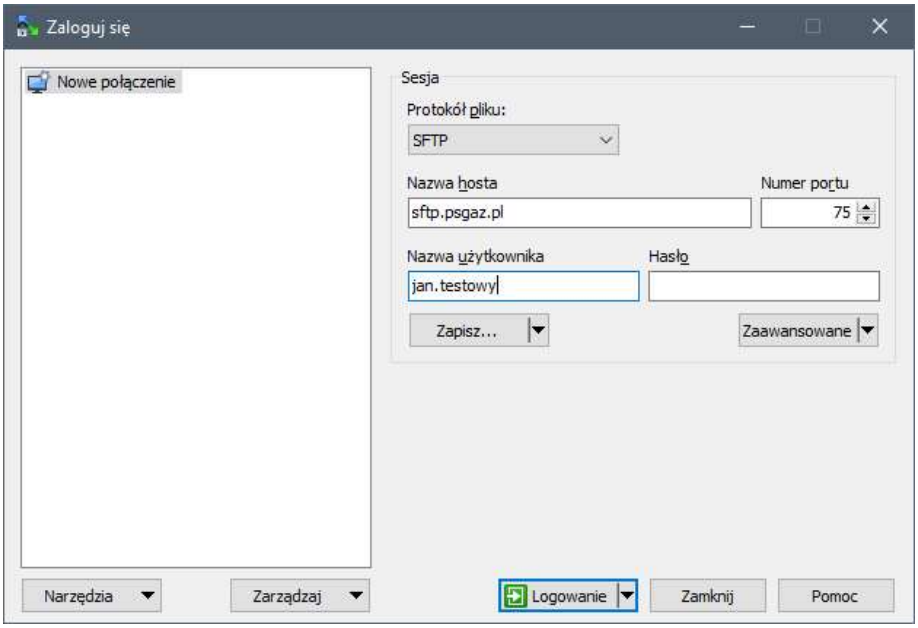
a) Uruchamiamy klienta WinSCP i uzupełniamy pola:

Protokół pliku – **SFTP**

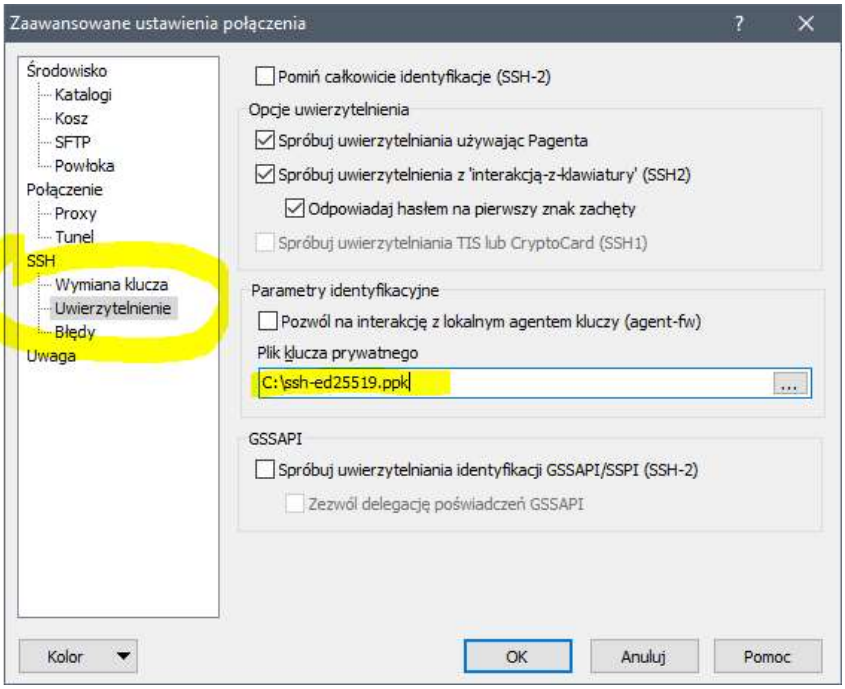
Nazwa hosta – **sftp.psgaz.pl**

Numer portu – **75**

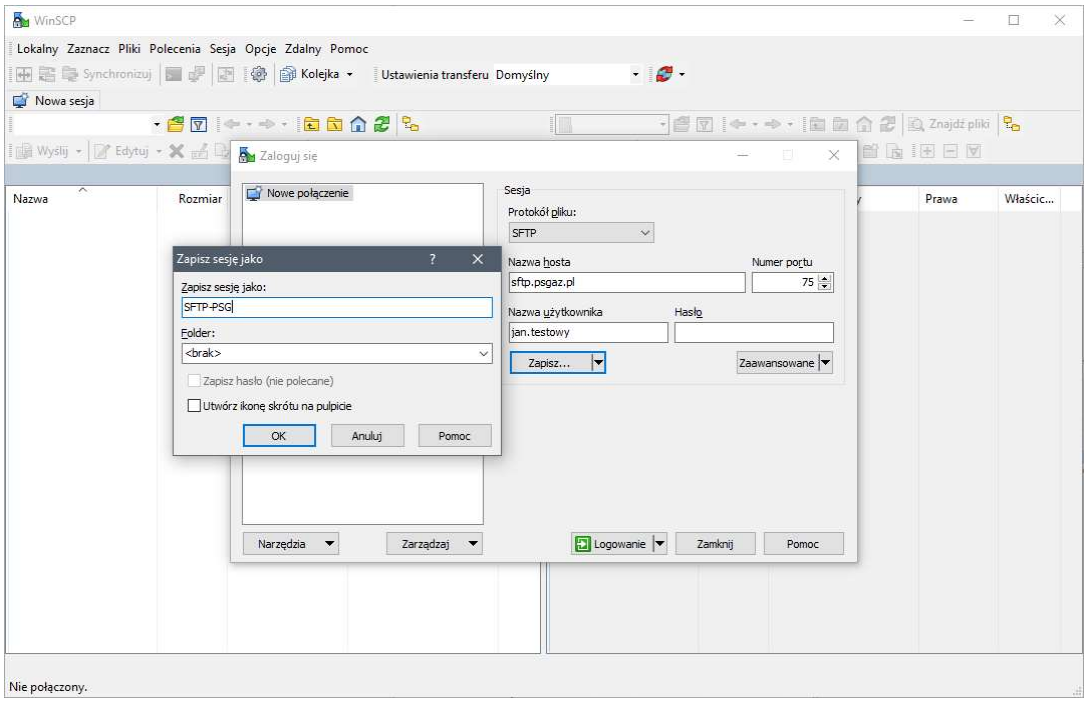
Nazwa użytkownika – zgodnie z informacją otrzymaną od OSD, następnie klikamy w przycisk *Zaawansowane*



b) W menu po lewej stronie wybieramy *SSH -> Uwierzytelnienie*. W polu *Plik klucza prywatnego*, wskazujemy położenie naszego pliku z kluczem:



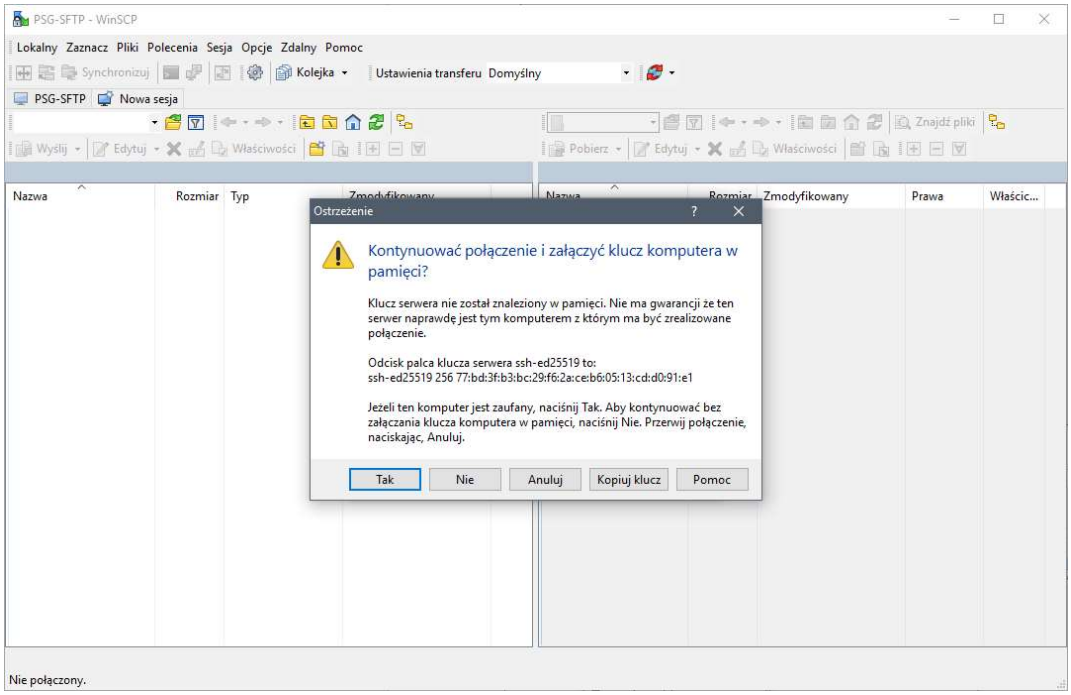
c) Zatwierdzamy ustawienia przyciskiem *OK* a następnie klikamy *Zapisz…,* by zapisać konfigurację naszego połączenia SFTP. Jako nazwę można podać np. SFTP-PSG:



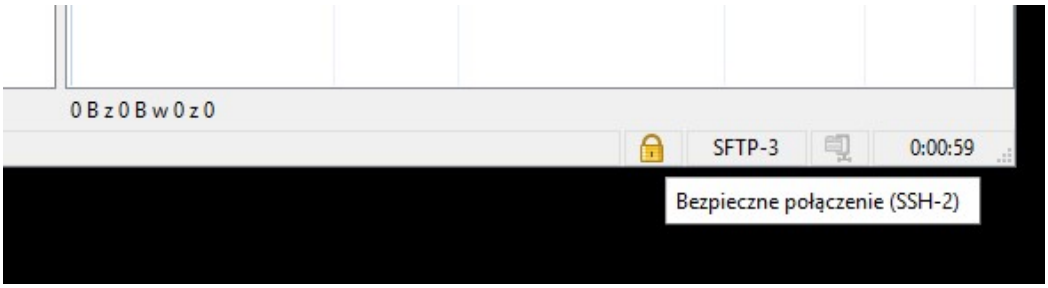
7.4 Nawiązywanie bezpiecznego połączenia

W celu nawiązania połączenia, klikamy na zdefiniowanej w punkcie c) powyżej nazwie połączenia.

W oknie z zapytaniem odpowiadamy twierdząco:



d) Po chwili mamy nawiązane bezpieczne, szyfrowane połączenie:



8 Dane kontaktowe

W przypadku problemów z działaniem poszczególnych usług (SFTP, EDI, eBOK) prosimy o zgłaszanie awarii na adres: edifact@psgaz.pl

9 Karta zmiany

Lp.	Data zmiany	Ogólny opis zakresu zmiany

10 Załączniki

Załącznik nr 1: Instrukcja obsługi Serwisu EBOK Polskiej Spółki Gazownictwa