Komunikacja z Polską Spółką Gazownictwa Sp. z o.o. w oparciu o standard AS4

Nominacje oraz prognozy transportowe OSDW w standardzie EDIG@S v5.1

Perspektywa techniczna

REJESTR ZMIAN

Data	Wersja	Autor	Opis
16/09/2021	1.0	ICT	Wersja bazowa dokumentu
23/02/2022	1.1	ICT	Korekty redakcyjne
19/05/2022	1.2	ICT	Ustalenie maski dla atrybutu „identyfication” (XSD)
06/09/2022	1.3	ICT	Uszczegółowienie założeń (Rozdział 3)
29/09/2022	1.4	ICT	Zmiana maski dla atrybutu „identyfication” (XSD)

SPIS TREŚCI

1 WSTĘP

W dokumencie przedstawiona jest perspektywa techniczna związana z przyłączeniem nowego partnera biznesowego do usługi udostępnionej przez PSG pozwalającej na obsługę nominacji oraz prognoz transportowych OSDW przy użyciu protokołu ebMS3/AS4. W związku z zastosowaniem wspomnianego protokołu w procesie składania nominacji/prognoz będą miały również zastosowanie certyfikaty zabezpieczające komunikację na poziomie warstwy transportowej oraz komunikatu.

Nawiązanie połączenia z usługą będzie możliwe po uzgodnieniu między partnerami podstawowych informacji, tj.:

- danych związanych z warstwą sieciową – ma to na celu udrożnienie połączenia między serwerami przez sieć Internet (tzw. punkty styku oraz port, na którym działa usługa)
    - dla komunikacji wychodzącej od podmiotu przyłączanego w kierunku PSG
    - dla komunikacji przychodzącej do podmiotu przyłączanego a wychodzącej z PSG
- identyfikatora przyłączanego podmiotu (4 znakowy kod)
- certyfikatów, które będą używane w komunikacji na poziomie komunikatu oraz na poziomie warstwy transportowej

Usługa pozwala na wymianę dokumentów „Nomination_Document", „NominationResponse_Document" oraz „Acknowledgement_Document" w standardzie EDIG@S v5.1. Szczegółowe informacje dotyczące standardu EDIG@S znajdują się na stronie www.edigas.org.

2 PROTOKÓŁ AS4 – OGÓLNE INFORMACJE

Protokół AS4 (Applicability Statement 4) to standard umożliwiający bezpieczne i niezawodne przesyłanie komunikatów przez publiczną sieć Internet. Protokół ten bazuje na powszechnie znanych i sprawdzonych rozwiązaniach, takich jak protokoły HTTP, TLS, SOAP oraz usługach sieciowych (web service). Reprezentuje otwarty standard wymiany danych typu B2B opisany w specyfikacji OASIS ebMS 3.0. Elementami odpowiedzialnymi za bezpieczeństwo i wiarygodność przesyłanych danych są podpisy cyfrowe oraz mechanizmy szyfrujące (WS-Security).

Dokumentacja OASIS Protokołu AS4:

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/cs03/AS4-profile-v1.0-cs03.html

Komunikacja na poziomie protokołu AS4 w systemach przesyłowych gazu odbywa się zgodnie z profilem ENTSOG AS4 Profile. Profil ENTSOG AS4 jest (z pewnymi wyjątkami) uściśleniem standardu AS4 ebHandler Conformance Profile – jednego z profili Standardu AS4.

Dokumentacja Profilu ENTSOG AS4:

https://www.entsog.eu/interoperability-and-data-exchange-nc#as4-documents-for-implementation

3 SZCZEGÓŁY TECHNICZNE KOMUNIKACJI AS4

1. Wzorzec komunikacyjny AS4: one-way/push (w obu kierunkach)
2. Warstwa transportowa zabezpieczona protokołem TLSv1.2 (one-way authentication)
3. Sygnatura dla komunikatów
    a. Wymagana
    b. HashFunction: "http://www.w3.org/2001/04/xmlenc#sha256"
    c. Algorytm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
4. Szyfrowanie komunikatów
    a. Wymagane

    b. Algorytm: “http://www.w3.org/2009/xmlenc11#aes128-gcm”
    c. Dla komunikatów przychodzących do PSG akceptowalne są algorytmy szyfrujące klucz: rsa-oaep, rsa-oaep-mgf1p, rsa-1_5
    d. Dla komunikatów wychodzących z PSG algorytmem szyfrowania klucz jest rsa-1_5
5. Wymagana kompresja komunikatów (application/gzip)
6. Włączona opcja potwierdzania dostarczenia wiadomości
7. Sekcja PartyInfo
    a. PartyID (from/to): kod EIC
    b. Role (from/to): PSG przyjmuje rolę „ZSO” a podmiot przyłączany rolę „ZSH”
8. Sekcja CollaborationInfo
    a. AgreementRef: „http://entsog.eu/communication/agreements/<EIC_A>/<EIC_B>/<version>” (gdzie kody EIC są posortowane alfabetycznie, a wersja początkowo przyjmuje wartość 1)
    b. Service: “A06”
    c. Action: “http://docs.oasis-open.org/ebxml-msg/as4/200902/action”
9. Dla efektywnego procesu zaleca się walidację komunikatów przed ich wysłaniem do PSG
10. Komunikat wysłany w kierunku PSG powinien reprezentować pojedynczą nominację/prognozę
11. Punkty styku z siecią PSG
    - Środowisko PRD: b2b.psgaz.pl:6210/edigas/nominations
        - IP: 91.233.60.10
    - Środowisko TST: b2b-tst.psgaz.pl:6210/edigas/nominations
        - IP: 91.233.60.11

4 CERTYFIKATY

Użycie certyfikatów ma na celu podniesienie poziomu bezpieczeństwa w komunikacji między partnerami.

Certyfikaty używane przez PSG w opisywanej komunikacji zostały umieszczone w katalogu „certyfikaty”.

Rodzaje użytych certyfikatów:

- certyfikat do zabezpieczania łączności (poziom warstwy transportowej)
- certyfikat do podpisu i szyfrowania komunikatu (poziom komunikatu)

Ogólna specyfikacja certyfikatów:

- Wersja certyfikatu: V3
- Algorytm podpisu: sha256RSA
- Ważność certyfikatu: preferowane min 2 lata
- Klucz publiczny: RSA (2048 bit)

Certyfikaty PSG oraz partnerów PSG muszą być wymienione na nowe przed upływem terminu ważności podczas uzgodnionego okienka serwisowego.

5 SPECYFIKACJA KOMUNIKATÓW

Definicje XSD komunikatów znajdują się w dołączonym do specyfikacji katalogu „edigas_v5.1”.

Rodzaje obsługiwanych komunikatów:

1. NOMINT – Nomination_Document
2. NOMRES – NominationResponse_Document
3. ACKNOW – Acknowledgement_Document

6 PRZYKŁADOWE KOMUNIKATY

Przykłady komunikatów znajdują się w dołączonym do specyfikacji katalogu „komunikaty”.

Lista przykładowych komunikatów:

1. Nomination_Document (NOMINT)
2. NominationResponse_Document (NOMRES)
3. Acknowledgement_Document (ACKNOW)