# TECHNICZNE STANDARDY SYSTEMÓW INFORMACYJNYCH

Wersja 1.6

(z 10 grudnia 2025 r.)

Zatwierdzono:

Aleksander Wiliński
Elektronicznie podpisany przez Aleksander Wiliński
Data: 2025.12.10 13:15:54 +01'00'

Obowiązuje od:

1) 1 stycznia 2026 r. – w zakresie rozdziałów 6.2 oraz 6.3,
2) 1 września 2026 r. – w pozostałym zakresie.

Kamil Rafał Wąsowicz
Elektronicznie podpisany przez Kamil Rafał Wąsowicz
Data: 2025.12.10 11:23:16 +01'00'

Aleksander Wiliński
Elektronicznie podpisany przez Aleksander Wiliński
Data: 2025.12.10 10:54:54 +01'00'

## Metryka dokumentu:

| | |
|---|---|
| Nazwa dokumentu | TECHNICZNE STANDARDY SYSTEMÓW INFORMACYJNYCH |
| Nazwa pliku | OIRE_2025-12-10_TSSI.docx |
| Wersja dokumentu | 1.6 |
| Data opracowania | 2025-12-10 |
| Autor dokumentu | Projekt OIRE – CGI oraz PSE |
| Osoba weryfikująca | Projekt OIRE – Zespół IT (QC) |
| Zawartość dokumentu (krótki opis) | Wymagania techniczne dla systemów teleinformatycznych współpracujących z CSIRE wraz ze specyfikacją techniczną protokołu AS4. |
| Etap / Proces | Strumień 3: Budowa, testowanie i uruchomienie CSIRE/S3.4 Publikacja wymagań technicznych, w tym w zakresie oprogramowania, jakie muszą spełniać systemy informacyjne współpracujące z CSIRE. |

## Historia zmian dokumentu:

| L.p. | Wersja | Opis zmiany | Data przekazania | Opracowujący zmianę | Firma |
|---|---|---|---|---|---|
| 1. | 0.9 | Utworzenie dokumentu na bazie *Wstępnego projektu zmian Załącznika nr 5. do IRiESP-OIRE (wersja z dnia 12 października 2023)* | 2023-12-20 | Projekt OIRE – CGI oraz PSE | PSE S.A. |
| 2. | 1.0 | Poprawki redakcyjne<br>Dodanie odwołania do norm ISO<br>Aktualizacja wersji IRiESP-OIRE oraz TSKB<br>Aktualizacja algorytmów kryptograficznych<br>Aktualizacja informacji o identyfikacji stron<br>Dodanie wymagania w zakresie rejestracji zdarzeń (komunikaty).<br>Dodanie Załącznika 2 – Parametry PMode CSIRE | 2024-05-07 | Projekt OIRE – CGI oraz PSE | PSE S.A. |
| 3. | 1.1 | Poprawki redakcyjne<br>Aktualizacja wersji IRiESP-OIRE oraz TSKB<br>Korekta wartości: PMode[1].ReceptionAwareness.Retry<br>Dodanie nowych kolejek<br>Uspójnienie przykładów wywołań<br>Dodanie przykładu obsługi wielu Kontrahentów<br>Uszczegółowienie zakres logowanych informacji<br>Dodanie rozdziału "Przyszłe funkcje i zmiany” | 2024-06-18 | Projekt OIRE – CGI oraz PSE | PSE S.A. |
| 4. | 1.2 | Poprawki redakcyjne<br>Modyfikacja opisów oraz dodanie nowej kolejki | 2024-07-12 | Projekt OIRE – CGI oraz PSE | PSE S.A. |
| 5. | 1.3 | Poprawki redakcyjne<br>Dodanie wzorca One-Way/Pull<br>Dodanie potwierdzeń (as4 receipt)<br>Dodanie informacji o kodach ról rynkowych<br>Dodanie informacji o obsłudze idempotencji<br>Aktualizacja przykładowych komunikatów<br>Aktualizacja P-Mode<br>Aktualizacja kodów błędów | 2024-12-03 | Projekt OIRE – CGI oraz PSE | PSE S.A. |
| 6. | 1.4 | Poprawki redakcyjne<br>Aktualizacja wersji TSKB<br>Aktualizacja opisu PMode<br>Wprowadzenie anglojęzycznych opisów błędów EBMS oraz aktualizacja opisów<br>Poprawienie przykładu odpowiedzi na SendMessage z niezaprzeczalnością odbioru<br>Poprawienie kodów ról rynkowych<br>Dodanie rozdziału 10<br>Aktualizacja konfiguracji PMode w Załączniku 2 | 2024-12-23 | Projekt OIRE – CGI oraz PSE | PSE S.A. |

| | | | | | |
|---|---|---|---|---|---|
| 7. | 1.5 | Poprawki redakcyjne<br>Aktualizacja wersji TSKB<br>Zmiana kodu HTTP dla One-Way/Push MEP with Receipt<br>Aktualizacja informacji o certyfikatach<br>Aktualizacja rozdziału 10<br>Aktualizacja konfiguracji PMode w Załączniku 2 | 2025-11-21 | Projekt OIRE – CGI oraz PSE | PSE S.A. |
| 8. | 1.6 | Poprawki redakcyjne<br>Aktualizacja kodu błędu – literówka<br>Aktualizacja informacji o certyfikatach – wprowadzenie daty obowiązywania<br>Aktualizacja zaleceń w zakresie pobierania wiadomości | 2025-12-10 | Projekt OIRE – CGI oraz PSE | PSE S.A. |

# SPIS TREŚCI


1. WYKAZ DEFINICJI I SKRÓTÓW ..... 6
1.1. Wykaz definicji ..... 6
1.2. Lista skrótów ..... 8
1.3. Dokumenty powiązane ..... 10
2. WSTĘP ..... 11
3. CEL ..... 12
4. ZAKRES ..... 13
4.1. Podmioty ..... 13
4.2. Kompozycja dokumentu ..... 13
4.3. Język ..... 13
5. KOMUNIKACJA ..... 14
5.1. Struktura wiadomości ..... 14
5.2. Podstawowe informacje dotyczące wymiany danych ..... 15
5.2.1. Założenia odnośnie przekazywanych wiadomości biznesowych ..... 16
5.3. Parametry przetwarzania wiadomości ..... 17
5.3.1. Parametry PMode dostępne do konfiguracji dla systemów zewnętrznych ..... 17
5.3.2. Pozostałe PMode (z wartością stałą bądź nieobsługiwane) ..... 20
5.4. Wzorce wymiany komunikatów AS4 (MEP) ..... 24
5.4.1. One-Way/Push MEP ..... 25
5.4.2. Two-Way/Sync MEP ..... 28
5.4.3. One-Way/Pull MEP ..... 29
5.4.4. Wzorce komunikacji systemu CSIRE ..... 30
5.4.5. Wysłanie wiadomości do CSIRE ..... 30
5.4.6. Pobranie wiadomości z CSIRE ..... 34
5.4.7. Techniczne kody błędów na poziomie warstwy transportowej ..... 41
5.4.8. Techniczne kody błędów AS4 ..... 41
5.4.9. Kody SOAP Fault ..... 45
5.4.10. Przykład realizacji początkowych kroków procesu SWI z mapowaniem na wywołania interfejsu CSIRE ..... 49
6. BEZPIECZEŃSTWO ..... 51
6.1. Zabezpieczenie komunikacji w warstwie sieci ..... 51
6.2. Zabezpieczenie komunikacji w warstwie transportowej ..... 51
6.3. Zabezpieczenie komunikacji w warstwie komunikatu ..... 52
6.3.1. Podpisywanie wiadomości ..... 52
6.3.2. Szyfrowanie wiadomości ..... 53
6.4. Certyfikaty oraz Infrastruktura Klucza Publicznego (PKI) ..... 54
6.5. Wymiana certyfikatu ..... 54
7. KOMPRESJA ..... 55
8. IMPLEMENTACJA ROZWIĄZANIA ..... 56
8.1. Wprowadzenie ..... 56
8.2. Identyfikacja stron ..... 56
8.2.1. Identyfikacja OIRE ..... 56
8.2.2. Kody ról rynkowych ..... 57
8.2.3. Przykład wywołania SendMessage ..... 57
8.3. Dostarczenie wiadomości, powtórzenia, obsługa niedostępności ..... 58
8.4. Idempotencja ..... 59
8.5. Wymagania odnośnie środowisk systemów współpracujących z CSIRE ..... 59

8.6. Wymagania w zakresie rejestracji zdarzeń ..... 60
9. REKOMENDACJE W ZAKRESIE CERTYFIKACJI AS4 ..... 61
10. PRZYSZŁE FUNKCJE I ZMIANY ..... 62
10.1. Rozszerzenie zakresu implementacji Protokołu AS4 ..... 62
10.2. Udostępnianie komunikatów wejściowych poprzez CSIRE ..... 62
10.3. Wprowadzenie rozszerzenia umożliwiającego alternatywną obsługę wielu wartości OrganisationUser ..... 62
11. SPIS TABEL I RYSUNKÓW ..... 63
12. ODNIESIENIA ..... 64
13. ZAŁĄCZNIKI ..... 65
13.1. Załącznik 1 – WSDL ..... 65
13.2. Załącznik 2 – Parametry PMode CSIRE ..... 65

# 1. WYKAZ DEFINICJI I SKRÓTÓW

Niniejszy rozdział zawiera wykaz definicji pojęć oraz wykaz skrótów stosowanych w niniejszym dokumencie, a także spis dokumentów powiązanych z niniejszym dokumentem.

## 1.1. Wykaz definicji

| Definicja | Objaśnienie |
|---|---|
| Centralny System Informacji Rynku Energii | System informacyjny służący do przetwarzania informacji rynku energii na potrzeby realizacji procesów rynku energii elektrycznej oraz wymiany informacji pomiędzy Użytkownikami systemu elektroenergetycznego. |
| Kod EIC | Kod służący do identyfikacji podmiotów na europejskim rynku energii. Kody nadawane są przez Centralne Biuro Kodów EIC (ENTSO-E) i przez Lokalne Biura Kodów EIC w poszczególnych krajach. W Polsce Lokalne Biura Kodów EIC prowadzone są przez Polskie Sieci Elektroenergetyczne S.A. (numer identyfikacyjny 19) oraz Operatora Gazociągów Przesyłowych GAZ-SYSTEM S.A. (numer identyfikacyjny 53). |
| Kontrahent | Użytkownik profesjonalny lub Użytkownik uprawniony będący stroną Umowy CSIRE, bądź podmiot ubiegający się o jej zawarcie. |
| Message Consumer | Aplikacja biznesowa lub usługa pośrednicząca odpowiadająca w procesie za odbiór komunikatu. |
| Message Producer | Aplikacja biznesowa lub usługa pośrednicząca odpowiadająca w procesie za przygotowanie komunikatu. |
| Message Service Handler | Usługa umożliwiająca wymianę wiadomości pomiędzy partnerami biznesowymi |
| Nadawca fizyczny | Podmiot udostępniający Kontrahentowi system informacyjny oraz zapewniający jego obsługę w celu realizacji przez Kontrahenta procesów rynku energii lub wymiany informacji rynku energii. |
| Operator informacji rynku energii | Podmiot odpowiedzialny za zarządzanie i administrowanie Centralnym systemem informacji rynku energii oraz przetwarzanie zgromadzonych w nim informacji na potrzeby realizacji procesów rynku energii. |
| Organizacja | Reprezentacja podmiotu rynku energii w systemie CSIRE. |
| Portal Użytkownika profesjonalnego | Portal dedykowany dla Użytkowników profesjonalnych oraz Użytkowników uprawnionych. Umożliwia on realizację procesów rynku energii i wymianę informacji rynku energii za pośrednictwem CSIRE. |
| Protokół AS4 (Application Statement 4) | Standard opisujący 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. |
| Receiving MSH | Usługa pełniąca rolę punktu docelowego w wymianie wiadomości pomiędzy partnerami biznesowymi. |
| Sending MSH | Usługa pełniąca rolę punktu inicjującego wymianę wiadomości w imieniu partnera biznesowego inicjującego wymianę komunikatów. |

| Definicja | Objaśnienie |
|---|---|
| Użytkownik Organizacji | (ang. *OrganisationUser*) Użytkownik posiadający prawo do interakcji z CSIRE w kontekście danej Organizacji. |
| Użytkownik profesjonalny | Podmiot realizujący procesy rynku energii i wymianę informacji rynku energii za pośrednictwem CSIRE. |
| Użytkownik uprawniony | Podmiot realizujący wymianę informacji rynku energii za pośrednictwem CSIRE, niebędący Użytkownikiem profesjonalnym lub Użytkownik profesjonalny działający na podstawie upoważnienia Użytkownika KSE. |
| WS-Security | Standard OASIS określający mechanizm zabezpieczenia usług Web Service. |
| Wydanie 3.0 CSIRE | Wydanie CSIRE bazujące na TSKB z dnia 9 grudnia 2025 r. |

Tabela 1. Wykaz definicji

## 1.2. Lista skrótów

| Skrót | Rozwinięcie |
|---|---|
| **AS4** | Protokół AS4 (Application Statement 4) |
| **A2A** | *Administration-to-Administration* |
| **B2A** | *Business-to-Administration* |
| **B2B** | *Business-to-Business* |
| **CSIRE** | Centralny System Informacji Rynku Energii |
| **CSWI** | Centralny System Wymiany Informacji |
| **DNS** | *Domain Name System* |
| **ENTSOG** | *European Network of Transmission System Operators for Gas* |
| **FIFO** | *First In First Out* |
| **IRiESP – OIRE** | Instrukcja Ruchu i Eksploatacji Sieci Przesyłowej część „Sposób funkcjonowania Centralnego systemu informacji rynku energii oraz współpracy Operatora systemu przesyłowego elektroenergetycznego, działającego jako Operator informacji rynku energii, z Użytkownikami systemu elektroenergetycznego i innymi podmiotami zobowiązanymi lub uprawionymi do korzystania z Centralnego systemu informacji rynku energii” |
| **JSON** | *JavaScript Object Notation* |
| **MEP** | *Message Exchange Patterns* |
| **MIME** | *Multipurpose Internet Mail Extensions* |
| **MPC** | *Message Partition Channels* |
| **MSH** | *Message Service Handler* |
| **OIRE** | Operator informacji rynku energii |
| **OSD** | Operator systemu dystrybucyjnego |
| **PTPiREE** | Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej |
| **SE** | Sprzedawca |
| **SEu** | Sprzedawca z urzędu |
| **SEr** | Sprzedawca rezerwowy |
| **SOAP** | *Simple Object Access Protocol* |
| **SWI** | Standardy Wymiany Informacji |
| **TLS** | *Transport Layer Security* |
| **TSKB** | Techniczne Standardy Komunikacji Biznesowej |

| Skrót | Rozwinięcie |
|---|---|
| **UUID** | *Universally Unique Identifier* |
| **WSS** | *Web Services Security (WS-Security)* |
| **XML** | *Extensible Markup Language* |
| **XSD** | *XML Schema Definition* |

Tabela 2. Lista skrótów

## 1.3. Dokumenty powiązane

| Lp. | Nazwa dokumentu powiązanego | Wersja dokumentu | Używany skrót nazwy |
|---|---|---|---|
| 1. | Instrukcja Ruchu i Eksploatacji Sieci Przesyłowej – Sposób funkcjonowania Centralnego systemu informacji rynku energii oraz współpracy Operatora systemu przesyłowego elektroenergetycznego, działającego jako Operator informacji rynku energii, z Użytkownikami systemu elektroenergetycznego i innymi podmiotami zobowiązanymi lub uprawionymi do korzystania z Centralnego systemu informacji rynku energii. | IRiESP-OIRE (zatwierdzona 6.04.2023 r., z poźn. zm.) | IRiESP-OIRE |
| 2. | Techniczne standardy komunikacji biznesowej. | Techniczne standardy komunikacji biznesowej (wersja z dnia 9 grudnia 2025 r.) | TSKB |

Tabela 3. Dokumenty powiązane

# 2. WSTĘP

Protokół AS4 [AS4-Profile] określa otwarty standard bezpiecznego oraz niezawodnego przesyłania komunikatów poprzez sieć Internet z wykorzystaniem usługi sieciowych. Wykorzystuje powszechnie znane rozwiązania takie, jak SOAP, MIME oraz WS-Security. Zazwyczaj jest stosowany w modelach B2B, B2A oraz A2A.

Dzięki możliwości przesyłania różnych typów komunikatów takich, jak pliki: binarne, XML lub JSON, zapewnia wysoki poziom elastyczności.

Powyższe cechy oraz istnienie zarówno komercyjnych, jak i otwartych implementacji protokołu AS4 spowodowały, iż został on przyjęty przez Komisję Europejską do budowy komponentu eDelivery w ramach Digital Europe Programme.

Ponadto jest on wykorzystywany także przez podmioty skupione w ENTSOG w ramach rozwoju wewnątrzwspólnotowego rynku gazu.

AS4 został przyjęty przez PTPiREE jako standard wymiany komunikatów w projekcie budowy CSWI, a OIRE zaakceptował ten standard dla systemu CSIRE.

# 3. CEL

Niniejszy dokument opisuje wykorzystanie protokołu AS4 do wymiany danych z CSIRE. Przedstawione informacje będą służyć do przygotowania konfiguracji systemów informacyjnych Użytkowników profesjonalnych, Użytkowników uprawnionych oraz Nadawców fizycznych do współdziałania z OIRE w modelu B2B.

# 4. ZAKRES

## 4.1. Podmioty

Konfiguracja opisana w niniejszym standardzie dotyczy systemów informacyjnych Użytkowników profesjonalnych, Użytkowników uprawnionych oraz Nadawców fizycznych wymieniających dane z CSIRE. Kontrahenci korzystający z Nadawców fizycznych będą wykorzystywać ich kanały komunikacyjne oraz będą identyfikowani na podstawie zawartości komunikatów.

## 4.2. Kompozycja dokumentu

Standard techniczny wymiany informacji z wykorzystaniem protokołu AS4 opisany w niniejszym dokumencie zawiera informacje o zmianach lub wybranych opcjach w stosunku do norm pochodzących z zewnętrznych dokumentów.

Bazuje on na “AS4 Profile of ebMS 3.0 Version 1.0 OASIS Standard” [AS4-Profile], który wykorzystuje między innymi standard “OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features OASIS Standard” [ebMS3CORE]. Ponadto występują odwołania do dokumentów opracowanych w celu implementacji protokołu AS4 w konkretnych zastosowaniach tj. „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile] oraz “AS4 Interoperability Profile for Four-Corner Networks Version 1.0 Committee Specification 01” [BDX-AS4-v1.0].

Powyższe standardy OASIS zostały przyjęte jako standardy ISO: [ebMS3CORE] jako “Electronic business eXtensible Markup Language (ebXML) Part 1: Messaging service core specification” [ISO 15000-1:2021(E)] oraz [AS4-Profile] jako “Electronic business eXtensible Markup Language (ebXML) Part 2: Applicability Statement (AS) profile of ebXML messaging service” [ISO 15000-2:2021(E)].

## 4.3. Język

W wypadku części informacji pochodzących w zewnętrznych dokumentów, pozostawiono ich oryginalną wersję językową.

# 5. KOMUNIKACJA

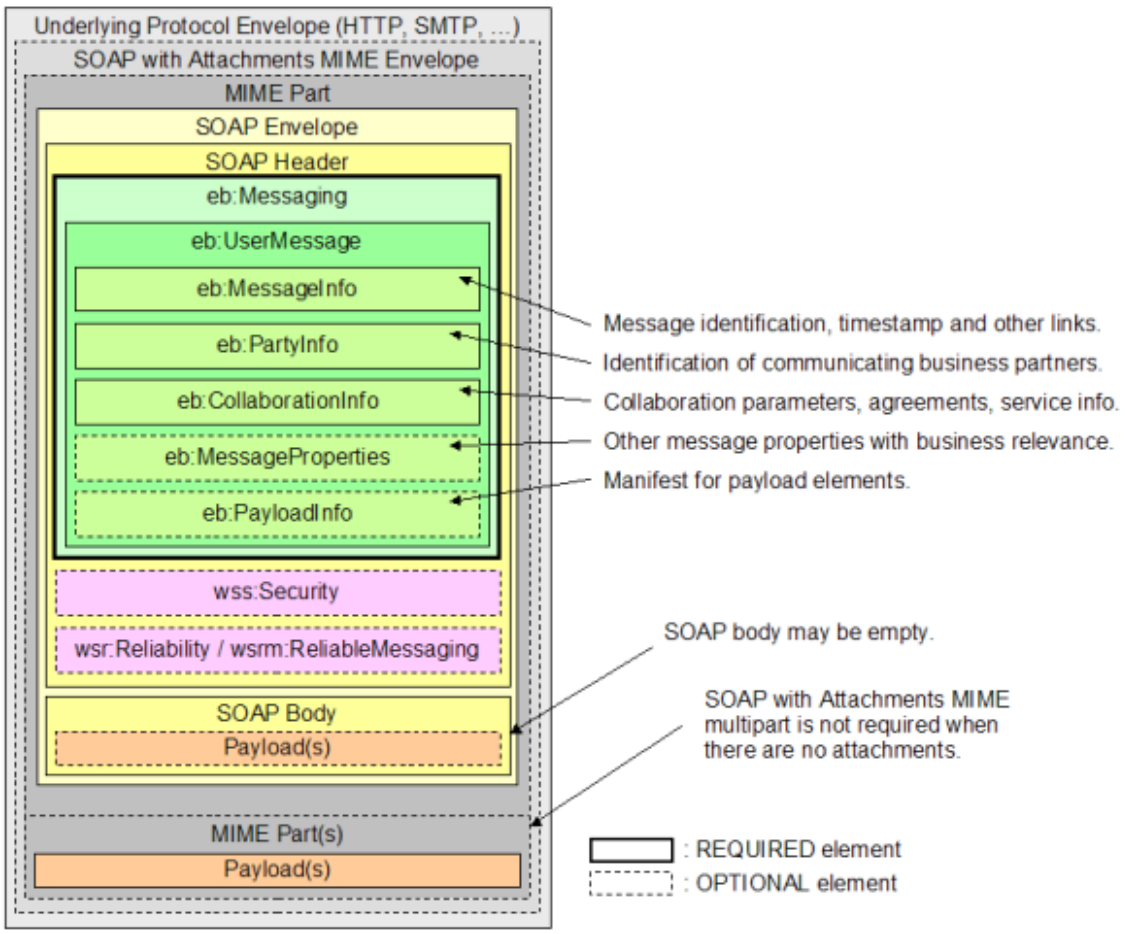
## 5.1. Struktura wiadomości

Standard wymiany komunikatów na potrzeby wymiany danych z CSIRE bazuje na wymianie komunikatów biznesowych poprzez wiadomości AS4.

Wiadomości AS4 powinny być budowane zgodnie z opisywanym przez OASIS standardem ebMS 3.0 [ebMS3CORE].

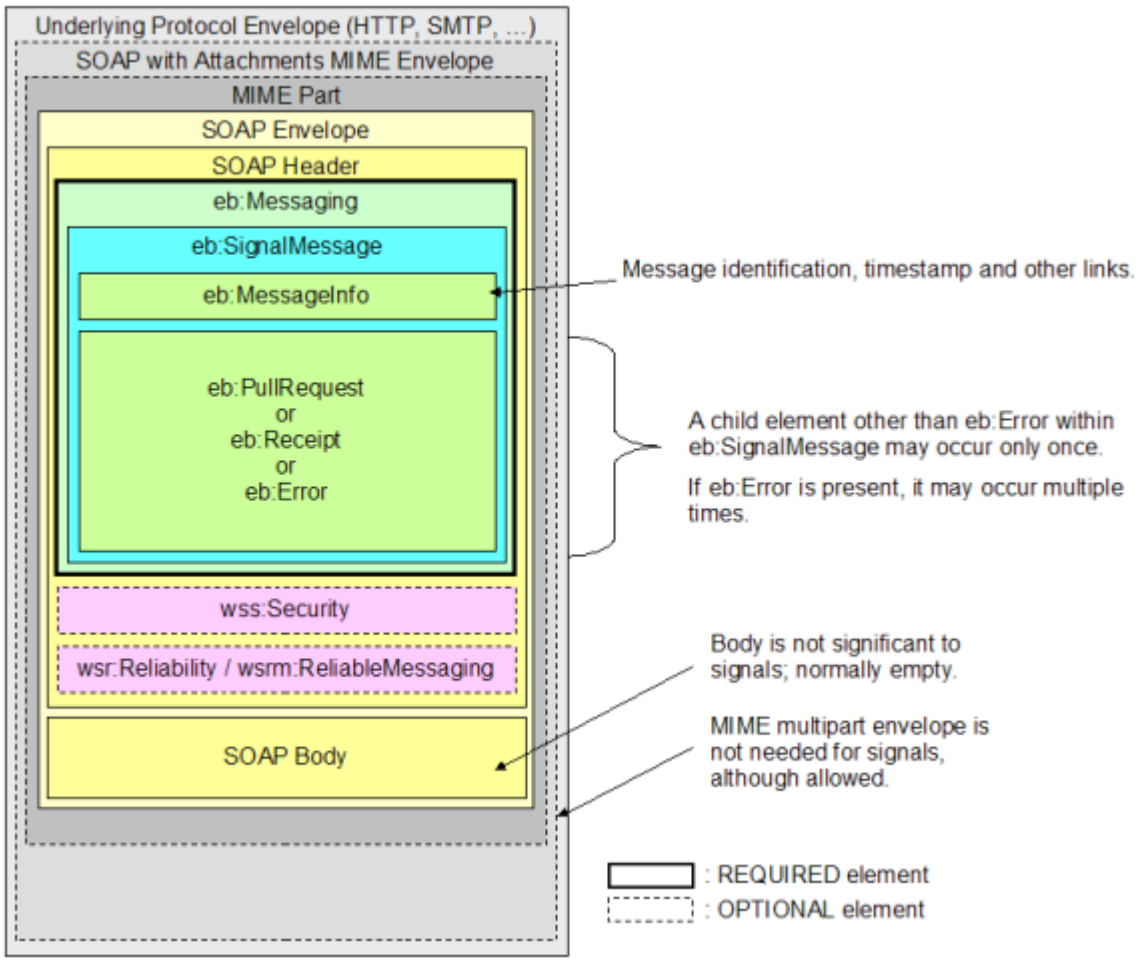
Struktura dwóch podstawowych wiadomości przekazywanych podczas transmisji pomiędzy MSH uczestniczącymi w wymianie danych, znajduje się na poniższych rysunkach.

Struktura wiadomości biznesowej




Rysunek 1 Struktura wiadomości (User Message Structure, [ebMS3CORE])

Struktura wiadomości sygnałowej




Rysunek 2 Struktura wiadomości sygnałowej (Signal Message Structure, [ebMS3CORE])

## 5.2. Podstawowe informacje dotyczące wymiany danych

Implementacja protokołu AS4 zakłada centralną rolę CSIRE w komunikacji między stronami rynku i wymusza inicjacje komunikacji z systemów zewnętrznych zarówno dla wiadomości wysyłanych do systemu, jak i wiadomości pobieranych z systemu CSIRE.

System CSIRE będzie zarówno producentem (*Message Producer*), jak i konsumentem (*Message Consumer*) wiadomości, przy czym sposób ich przekazania będzie różny zależnie od kierunku komunikacji.

System CSIRE w komunikacji z systemami zewnętrznymi będzie zawsze występował w roli Receiving MSH (czyli występować będzie w roli serwera usługi), zaś systemy zewnętrzne zawsze będą występować w roli Sending MSH (czyli będą występować w roli klientów usługi).

Oznacza to, iż wiadomości wysyłane do CSIRE będą przekazywane przez wywołanie AS4 pochodzące z systemów zewnętrznych wg. wzorca One-Way Push (opisany w 5.4.1), zaś wiadomości pochodzące z systemu CSIRE będą musiały być pobrane przez systemy zewnętrzne wg. wzorca Two-Way/Sync (opisany w 5.4.2).

Podstawowe założenia komunikacji z CSIRE:

- Wysyłanie wiadomości do systemu CSIRE odbywać się będzie poprzez wywołanie udostępnionej usługi (operacja SendMessage, patrz 5.4.4) odpowiadającej za przyjęcie i zarejestrowanie transakcji.
- Wiadomości wychodzące z CSIRE zostaną udostępnione do pobrania i to w gestii systemów zewnętrznych będzie pobranie ich z systemu CSIRE (za pomocą operacji PeekMessage patrz 5.4.5) i potwierdzenie ich poprawnego odebrania (za pomocą operacji DequeueMessage).
- Wywołanie operacji DequeueMessage zapewnia niezaprzeczalność dostarczenia wiadomości do systemu zewnętrznego (nie da się poprawnie wywołać operacji DequeueMessage bez poprawnego odczytania rezultatu operacji PeekMessage)

Dla systemów zewnętrznych komunikujących się z CSIRE oznacza to:

- Aktywna komunikacja z systemów zewnętrznych dla wiadomości wychodzących z CSIRE – konieczność cyklicznego odpytywania CSIRE poprzez wywołanie operacji PeekMessage.
- Systemy zewnętrzne zarządzają szybkością pobierania i przetwarzania wiadomości.
- Systemy zewnętrzne zarządzają kolejnością przetwarzania wiadomości (CSIRE wymusza pobranie w kolejności).
- WSDL opisujący WebService zawierający operacje SendMessage, PeekMessage oraz DequeueMessage znajduje się w Załączniku 1 – WSDL.

### 5.2.1. Założenia odnośnie przekazywanych wiadomości biznesowych

- Wiadomości biznesowe przekazywane w elemencie payload wiadomości AS4 UserMessage (niezależnie czy payload jest częścią wiadomości czy załącznikiem) powinny być poprawnymi komunikatami XML zgodnymi z WSDL z Załącznika 1 – WSDL oraz ze schematami XSD udostępnionymi w ramach TSKB.
- Schematy XSD są zgodne ze specyfikacją XML Schema 1.0.
- W ramach pojedynczego wysłania lub odebrania wiadomości z/do CSIRE przekazana może być jedna wiadomość biznesowa zgodna z XSD.
- Grupowanie (paczkowanie) np. dla profili dobowych zostanie uwzględnione w ramach schematów XSD (czyli np. jedna wiadomość, zgodna z XSD, będzie zawierać wiele profili dobowych).
- Wiadomości biznesowe mogą być przekazywane do CSIRE jako payload będący częścią wiadomości AS4 lub jako załącznik. W przypadku użycia kompresji payload musi być przekazany jako załącznik.
- CSIRE będzie udostępniać wiadomości w payload będącym częścią wiadomości AS4 z wyjątkiem sytuacji, gdy włączone zostanie użycie kompresji - wtedy wiadomości będą przekazywane w załączniku.
- W przypadku przekazania wiadomości jako załącznik powinien on zawierać pełną strukturę wywołania dla danej operacji SendMessage, PeekMessage lub DequeueMessage. Przykład dla operacji SendMessage można zobaczyć w rozdziale 5.4.5.2.2.

## 5.3. Parametry przetwarzania wiadomości

Każda wiadomość przekazana do systemu CSIRE musi zawierać w nagłówku sekcje CollaborationInfo zawierającą min. elementy AgreementRef, Service, Action (przykład wywołania z rozdziału 5.4.5.2.1). Elementy te służą do wskazania, który zestaw parametrów PMode z konfiguracji systemu CSIRE należy użyć do procesowania wiadomości. Sposób mapowania tych elementów na parametry PMode w systemie:

AgreementRef - PMode.Agreement

Service - PMode[1].BusinessInfo.Service

Action - PMode[1].BusinessInfo.Action

Dzięki temu strona wywołująca może poprzez odpowiednią konfiguracje PMode w systemie CSIRE oraz sekcje CollaborationInfo w wywołaniu używać różnych zestawów parametrów PMode dla różnych wywołań (np. używać kompresji tylko dla niektórych komunikatów).

Dla operacji PeekMessage (dla wzorca Two-Way/Sync) w systemie CSIRE może zostać utworzona para konfiguracji PMode z takimi samymi wartościami PMode.Agreement oraz PMode[1].BusinessInfo.Service i różnym PMode[1].BusinessInfo.Action:

- Konfiguracja z PMode[1].BusinessInfo.Action równym PeekMessage.request odpowiada za sposób obsługi wiadomości wejściowej do systemu CSIRE
- Konfiguracja z PMode[1].BusinessInfo.Action równym PeekMessage.reply odpowiada za sposób, w jaki wygenerowana będzie odpowiedź z systemu CSIRE.

Tabela 4 Przykład pary konfiguracji PMode dla operacji PeekMessage

| Pmode.Agreement | Pmode[1].BusinessInfo.Service | Pmode[1].BusinessInfo.Action | Pmode[1].PayloadService.CompressionType | Pmode[1].Security.X509.Encryption.Encrypt | Pmode[1].Security.X509.Sign |
|---|---|---|---|---|---|
| Agreement_1 | MarketMessaging | PeekMessage.request | | Yes | Yes |
| Agreement_1 | MarketMessaging | PeekMessage.reply | application/gzip | Yes | Yes |

W systemie CSIRE może istnieć wiele zestawów konfiguracji PMode dla operacji PeekMessage, tak by strona wywołująca mogła pobierać wiadomości z różnym zestawem funkcjonalności, np. pobierać wiadomości z niektórych kolejek jako skompresowany załącznik.

Dla operacji PeekMessage (dla wzorca One-Way/Pull) w systemie CSIRE powinna zostać utworzona konfiguracja zawierająca PMode[1].BusinessInfo.Service równe MarketMessaging oraz PMode[1].BusinessInfo.Action równe PeekMessage.

Dla PeekMessage używanego zgodnie z wzorcem One-Way/Pull w wywołaniu nie jest przekazywany element CollaborationInfo więc nie można wskazać oczekiwanego zestawu parametrów PMode – oznacza to iż dla tego przypadku może istnieć tylko jeden zestaw parametrów PMode.

Zestawienie obsługiwanych przez system CSIRE parametrów zawiera Załącznik 2 – Parametry PMode CSIRE.

### 5.3.1. Parametry PMode dostępne do konfiguracji dla systemów zewnętrznych

Poniżej w tabeli znajduje się lista parametrów określających tryb przetwarzania wiadomości (P-Mode) wykorzystywanych w niniejszej specyfikacji wraz z informacją o charakterze danego parametru.

168 Tabela 5 Parametry PMode dostępne do konfiguracji

| Lp. | PMode | Wymagalność | Opis | Wartość |
|---|---|---|---|---|
| 1. | PMode.ID | Obowiązkowy | Identyfikuje zestaw parametrów PMode. | Wygenerowany identyfikator UUID |
| 2. | PMode.Agreement | Obowiązkowy | Jest używany w połączeniu z PMode[1].BusinessInfo.Service i PMode[1].BusinessInfo.Action w celu jednoznacznej identyfikacji zestawu parametrów PMode na podstawie nagłówka komunikatu AS4 (atrybuty w CollaborationInfo ComplexElement). | Zgodnie z Załącznikiem 2 – Parametry PMode CSIRE.<br>Nie używany dla wzorca One-Way/Pull. |
| 3. | PMode.Initiator.Party | Obowiązkowy | Kwalifikuje stronę inicjującą MEP. | Stała wartość: Identyfikator Organizacji. |
| 4. | PMode.Initiator.Role | Obowiązkowy | Producent wiadomości pełni rolę inicjatora, czyli rolę strony wysyłającej pierwszą wiadomość wzorca MEP. | Stała wartość: Rola Organizacji na rynku. |
| 5. | PMode.Responder.Party | Obowiązkowy | Kwalifikuje stronę odbierającą MEP. | Stała wartość: Identyfikator Organizacji dla roli OIRE. |
| 6. | PMode.Responder.Role | Obowiązkowy | Rola odbiorcy wiadomości. | Stała wartość:<br>Rola Organizacji na rynku (OIRE). |
| 7. | PMode.MEP | Obowiązkowy | Wzorzec wymiany komunikatów (musi to być identyfikator URI), zob. także 5.4:<br>One-Way MEP reguluje wymianę pojedynczej jednostki wiadomości użytkownika, niezwiązanej z innymi wiadomościami użytkownika: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay.<br>Two-Way MEP zarządza wymianą dwóch jednostek wiadomości użytkownika w przeciwnych kierunkach: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/twoWay. | Możliwe wartości:<br>• One-Way/Push lub One-Way/Pull: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay<br>• Two-Way/Sync: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/twoWay |

| Lp. | PMode | Wymagalność | Opis | Wartość |
|---|---|---|---|---|
| 8. | PMode.MEPBinding | Obowiązkowy | Powiązanie kanału transportowego przypisane do MEP (push, pull, sync, push-and-push, push-and-pull, pull-and-push, pull-and-pull, …). CSIRE obsługuje tylko push i sync, musi być zgodny z PMode.MEP. | Stała wartość w zależności od MEP:<br>• One-Way/Push: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push<br>• One-Way/Pull: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/pull<br>• Two-Way/Sync: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/sync |
| 9. | PMode[1].BusinessInfo.Service | Obowiązkowy | Nazwa usługi, do której ma zostać dostarczona wiadomość Użytkownika. Jest używany w połączeniu z PMode.Agreement i PMode[1].BusinessInfo.Action w celu jednoznacznej identyfikacji zestawu parametrów PMode na podstawie nagłówka komunikatu AS4.<br><br>Jego zawartość musi być odwzorowana na element eb:Messaging/eb:UserMessage/eb:CollaborationInfo/eb:Service. | Stała wartość: MarketMessaging |
| 10. | PMode[1].BusinessInfo.Action | Obowiązkowy | Nazwa akcji, którą ma wywołać UserMessage. Jest używana w połączeniu z PMode.Agreement i PMode[1].BusinessInfo.Service do jednoznacznej identyfikacji zestawu parametrów PMode na podstawie nagłówka komunikatu AS4. Jest jedną ze stałych wartości dla CSIRE.<br><br>Jego zawartość powinna być odwzorowana na element eb:Messaging/eb:UserMessage/eb:CollaborationInfo/eb:Action. | Możliwe wartości zależą od wzorca MEP:<br>One-Way/Push:<br>• SendMessage<br>• DequeueMessage<br>Two-Way/Sync:<br>• PeekMessage.request<br>• PeekMessage.reply<br>One-Way/Pull:<br>• PeekMessage |
| 11. | PMode[1].PayloadService.CompressionType | Opcjonalny | Jeśli jest ustawiony, CSIRE zdekompresuje payload z żądania oraz skompresuje payload dla odpowiedzi zawierającej wiadomość biznesową. Dotyczy tylko payloadu w załączniku SOAP. | application/gzip |
| 12. | PMode[1].Security.X509.Sign | Obowiązkowy | Wartość logiczna wskazująca, czy wiadomości powinny być podpisywane. | Yes/No |

| Lp. | PMode | Wymagalność | Opis | Wartość |
|---|---|---|---|---|
| 13. | PMode[1].Security.X509.Encryption.Encrypt | Obowiązkowy | Parametr wskazujący (jeśli jest prawdziwy), że MSH zaszyfruje:<br>• Wszystkie części payloadu:<br>Każda treść SOAP również zostanie zaszyfrowana.<br>• Załączniki.<br>MSH nie zaszyfruje nagłówka.<br>Jeśli wymagana jest poufność danych w nagłówku, można to osiągnąć poprzez zabezpieczenie na poziomie transportu. | Yes/No |
| 14. | PMode[1].Security.SendReceipt | Opcjonalny | Parametr wskazujący czy wymagane jest potwierdzenie odbioru (patrz rozdział 5.4.1.1). | Yes/No |
| 15. | PMode[1].Security.SendReceipt.NonRepudiation | Opcjonalny | Parametr wskazujący czy wymagane jest niezaprzeczalne potwierdzenie odbioru, czy tylko potwierdzenie odbioru (patrz rozdział 5.4.1.1). | Yes/No<br>Obowiązuje gdy PMode[1].Security.SendReceipt = Yes |
| 16. | PMode[1].Security.SendReceipt.ReplyPattern | Opcjonalny | Wskazuje, czy potwierdzenie odbioru ma zostać wysłane:<br>- jako wywołanie zwrotne na oddzielnym połączeniu. (wartość „Callback”)<br>- synchronicznie w odpowiedzi HTTP lub kanale zwrotnym (wartość „Response”).<br>W przypadku braku PMode, można użyć dowolnego wzorca. | Stała wartość: Response<br>Obowiązuje gdy PMode[1].Security.SendReceipt = Yes |

## 5.3.2. Pozostałe PMode (z wartością stałą bądź nieobsługiwane)

Tabela 6 Parametry PMode ze stałą wartością bądź nieobsługiwane

| Lp. | PMode | Opis | Wartość |
|---|---|---|---|
| 1. | PMode[1].Protocol.SOAPVersion | Wersja SOAP, która ma być używana (1.1 lub 1.2). | Stała wartość 1.2 |
| 2. | PMode[1].Security.WSSVersion | Wartość reprezentuje wersję WS-Security, która ma być używana, i ma dwie możliwe wartości:<br>1.0<br>1.1 | Stała wartość 1.1 |
| 3. | PMode[1].Security.X509.Encryption.Certificate | Certyfikat publiczny do odszyfrowywania otrzymanych wiadomości. | Zarządzanie certyfikatami odbywa się z użyciem Portalu Użytkownika profesjonalnego. |
| 4. | PMode[1].Security.X509.Signature.Certificate | Certyfikat publiczny do weryfikacji otrzymanych podpisanych wiadomości. | Zarządzanie certyfikatami odbywa się z użyciem Portalu Użytkownika profesjonalnego. |

| Lp. | PMode | Opis | Wartość |
|---|---|---|---|
| 5. | PMode[1].Security.X509.Signature.HashFunction | Algorytm używany do obliczania skrótu podpisywanej wiadomości. Definicje tych wartości znajdują się w specyfikacji XML-DSIG-V1.0 [https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/] | http://www.w3.org/2001/04/xmlenc#sha256 |
| 6. | PMode[1].Security.X509.Signature.Algorithm | Identyfikuje algorytm obliczania wartości podpisu cyfrowego. | - (domyślnie) RSA-SHA256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)<br>- RSA-SHA384 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha384)<br>- RSA-SHA512 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha512) |
| 7. | PMode[1].Security.X509.Encryption.Algorithm | Algorytm szyfrowania, który ma być używany. | Patrz 6.3.2 |
| 8. | PMode[1].Security.X509.Encryption.MinimumStrength | Wartość całkowita określająca efektywną siłę, którą algorytm szyfrowania musi zapewnić w postaci efektywnych lub losowych bitów.<br>Wartość jest mniejsza niż długość klucza w bitach, gdy w kluczu używane są bity kontrolne.<br>Np. 8 bitów kontrolnych 64-bitowego klucza DES nie zostanie uwzględnionych w zliczaniu.<br>Ustawienie MinimumStrength na 56 jest wymagane, aby mieć minimalną siłę równą tej dostarczanej przez DES. | Stała wartość 128 |
| 9. | PMode[1].ErrorHandling.Report.AsResponse | Ten parametr typu boolean wskazuje, czy (jeśli „prawda”) błędy wygenerowane w wyniku odebrania błędnej wiadomości są przesyłane przez tylny kanał bazowego protokołu powiązanego z błędną wiadomością, czy nie. | Zawsze prawda. |
| 10. | PMode[1].ReceptionAwareness.Retry | Parametr logiczny wskazujący (jeśli to prawda), że kroki podjęte w celu zapewnienia odbioru wiadomości zostaną powtórzone, jeśli to konieczne. | Nie używany. |
| 11. | PMode.Initiator.Authorization.username | Opisuje informacje autoryzacyjne dla komunikatów wysyłanych przez inicjatora, które mają być przetwarzane po stronie odbiorcy. | Nieużywany. CSIRE nie oczekuje, że otrzyma nazwę użytkownika/hasło przez kanał AS4. |
| 12. | PMode.Initiator.Authorization.password | | |
| 13. | PMode.Responder.Authorization.username | Opisuje informacje autoryzacyjne dla wiadomości wysyłanych przez respondenta, które mają być przetwarzane po stronie inicjatora. | Nieużywany. CSIRE nie przewiduje wysyłania nazwy użytkownika/hasła kanałem AS4. |
| 14. | PMode.Responder.Authorization.password | | |

| Lp. | PMode | Opis | Wartość |
|---|---|---|---|
| 15. | PMode[1].Protocol.Address | Reprezentuje adres (adres URL punktu końcowego) odbiornika MSH (lub strony odbiorcy), do którego mają być wysyłane komunikaty. | Nieużywany.<br><br>Organizacje zawsze inicjują komunikację z CSIRE, dlatego konfiguracja adresu URL, na który organizacje mają otrzymywać wiadomości, nie jest wymagana. |
| 16. | PMode[1].BusinessInfo.PayloadProfile.maxSize | Ten parametr pozwala na określenie maksymalnego rozmiaru w kilobajtach dla całego payloadu, czyli dla sumy wszystkich części ładunku. | Nieużywany. Dla wszystkich wiadomości wymienianych z CSIRE stosowana jest stała wartość maksymalna wynosząca 100 MB. |
| 17. | PMode[1].BusinessInfo.Properties[] | Wartością tego parametru jest lista właściwości. Właściwość to struktura danych składająca się z czterech wartości: nazwy właściwości, której można użyć jako identyfikator właściwości (np. wymagana właściwość o nazwie „messagetype” może być zapisana jako: Właściwości[typ wiadomości].required="true"); opis właściwości; typ danych właściwości; i Wartość logiczna wskazująca, czy właściwość jest oczekiwana, czy opcjonalna w komunikacie użytkownika. Ten parametr steruje zawartością elementu eb:Messaging/eb:UserMessage/ eb:MessageProperties. | Nieużywany |
| 18. | PMode[1].BusinessInfo.PayloadProfile[] | Ten parametr pozwala na określenie ograniczenia lub profilu dla payloadu. | Nieużywany. |
| 19. | PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer | Parametr logiczny wskazujący (jeśli true ), że konsument (aplikacja/strona) komunikatu użytkownika pasującego do PMode powinien zostać powiadomiony, gdy wystąpi błąd w odbierającym MSH. | Nieużywany. |
| 20. | PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer | Parametr typu boolean wskazujący (jeśli true), że podczas przetwarzania komunikatu użytkownika do wysłania producent (aplikacja/strona) komunikatu użytkownika pasującego do PMode powinien zostać powiadomiony, gdy wystąpi błąd w wysyłającym MSH. | Nieużywany. |
| 21. | PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer | Parametr typu boolean wskazujący (jeśli jest prawdziwy), że błąd EBMS:0301 MissingReceipt musi zostać zwrócony przez wysyłający MSH do odbierającego MSH w przypadku, gdy nie zostanie zwrócony żaden AS4 Receipt. | Nieużywany |

| Lp. | PMode | Opis | Wartość |
|---|---|---|---|
| 22. | PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer | CSIRE zawsze zwraca wszelkie błędy, które wystąpiły podczas przetwarzania UserMessages, ponieważ jest to kluczowe dla rynków centralnych, wszystkie organizacje muszą wiedzieć, kiedy ich transakcja biznesowa nie została pomyślnie przetworzona i podjąć odpowiednie działania. | Nieużywany. |
| 23. | PMode[1].ErrorHandling.Report.ReceiverErrorsTo | Adres lub rozdzielona przecinkami lista adresów, na które mają być wysyłane błędy ebMS wygenerowane przez MSH, który odbiera błędny komunikat. np. Może to być adres MSH wysyłającego błędną wiadomość. | Nieużywany. |
| 24. | PMode[1].ErrorHandling.Report.SenderErrorsTo | Adres — lub rozdzielona przecinkami lista adresów — na który mają zostać wysłane błędy wygenerowane przez MSH, który próbował wysłać błędny komunikat. | Nieużywany. |
| 25. | PMode[1].Protocol.Address | Adres URL punktu końcowego odbiornika MSH (lub strony odbiorcy), do którego mają być wysyłane komunikaty w części PMode. | Nieużywany. |
| 26. | PMode[1].ReceptionAwareness | Parametr logiczny wskazujący (jeśli prawda), że należy podjąć kroki w celu zapewnienia odbioru wiadomości. | Nieużywany. |
| 27. | PMode[1].ReceptionAwareness.Retry.Parameters | Parametr określający wymagania dotyczące ponownych prób wywołania. | Nieużywany. |
| 28. | PMode[1].ReceptionAwareness.DuplicateDetection | Wykrywanie zduplikowanych wiadomości jest zawsze włączone w CSIRE i nie można nim sterować za pomocą parametrów. | Nieużywany. |
| 29. | PMode[1].ReceptionAwareness.DuplicateDetection.Parameters | Wykrywanie zduplikowanych wiadomości jest zawsze włączone w CSIRE i nie można nim sterować za pomocą parametrów. | Nieużywany. |

| Lp. | PMode | Opis | Wartość |
|---|---|---|---|
| 30. | PMode[1].Security.PModeAuthorize | Parametr logiczny wskazujący (jeśli true), że komunikat w MEP musi zostać autoryzowany do przetwarzania w trybie PMode. Jeśli parametr ma wartość true, oznacza to, że w tym celu należy użyć następujących elementów: PMode.Responder.Authorization. {username/password}, jeśli wiadomość jest wysyłana przez Respondera . PMode.Initiator.Authorization, jeśli wiadomość jest wysyłana przez Initiator . np. po ustawieniu na true dla komunikatu PushRequest wysłanego przez inicjatora, push będzie autoryzowany tylko przez MPC wskazany przez ten sygnał Push , jeśli: MPC jest taki sam , jak określono w nodze PMode dla przesyłanej wiadomości; I sygnał zawiera ważne dane uwierzytelniające (tj. nazwę użytkownika/hasło). | Nieużywany. |
| 31. | PMode[1].Security.UsernameToken. username | Nazwa użytkownika do uwzględnienia w tokenie nazwy użytkownika WSS . | Nieużywany. |
| 32. | PMode[1].Security.UsernameToken. password | Hasło do użycia wewnątrz tokena nazwy użytkownika WSS. | Nieużywany. |
| 33. | PMode[1].Security.UsernameToken. Digest | Wskazuje, czy skrót hasła zostanie uwzględniony w elemencie WSS UsernameToken. | Nieużywany. |
| 34. | PMode[1].Security.UsernameToken. Nonce | Wskazuje, czy element WSS UsernameToken będzie zawierał element Nonce. Nonce => liczba lub ciąg bitów używany tylko raz w inżynierii bezpieczeństwa. | Nieużywany. |
| 35. | PMode[1].Security.UsernameToken. Created | Wskazuje, czy element WSS UsernameToken będzie miał utworzony element sygnatury czasowej. | Nieużywany. |

## 5.4. Wzorce wymiany komunikatów AS4 (MEP)

W ramach rozwiązania stosowanego na potrzeby CSIRE, wykorzystywane będą dwa, spośród czterech dostępnych w ramach Protokołu AS4, wzorców wymiany wiadomości.

Każda interakcja pomiędzy stronami wymieniającymi komunikaty (OIRE, Użytkownicy profesjonalni, Użytkownicy uprawnieni), będzie wymagała zastosowania odpowiedniego wzorca (MEP).

Poniżej przedstawione zostaną poszczególne wzorce wymiany wiadomości.

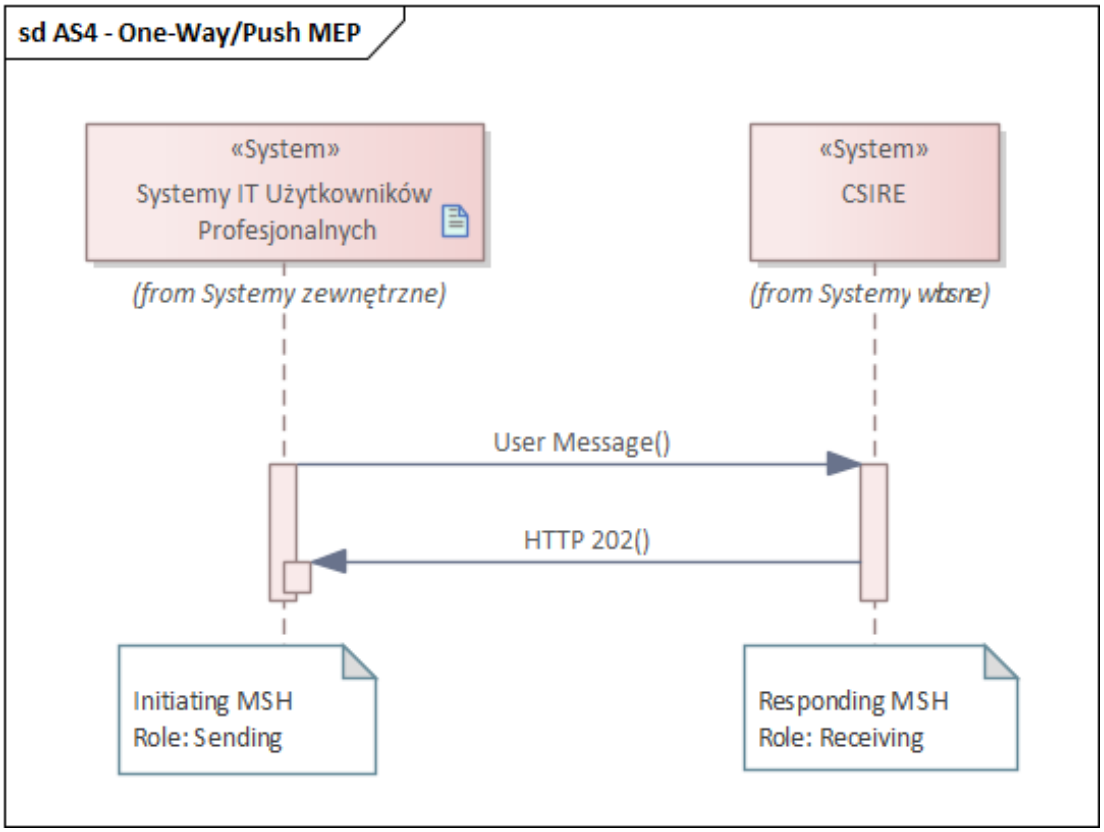
### 5.4.1. One-Way/Push MEP

Opis wzorca komunikacji można przedstawić za pomocą sekwencji następujących po sobie zdarzeń.

1. partner inicjujący (system zewnętrzny), wykorzystując Message Handler (*Initiating MSH*), wysyła wiadomość do partnera odbierającego (*Receiving MSH*).

2. w reakcji na przesłaną wiadomość, w sposób synchroniczny otrzymuje jedynie status odpowiedzi HTTP (202) oznaczający przyjęcie wiadomości do dalszego procesowania.

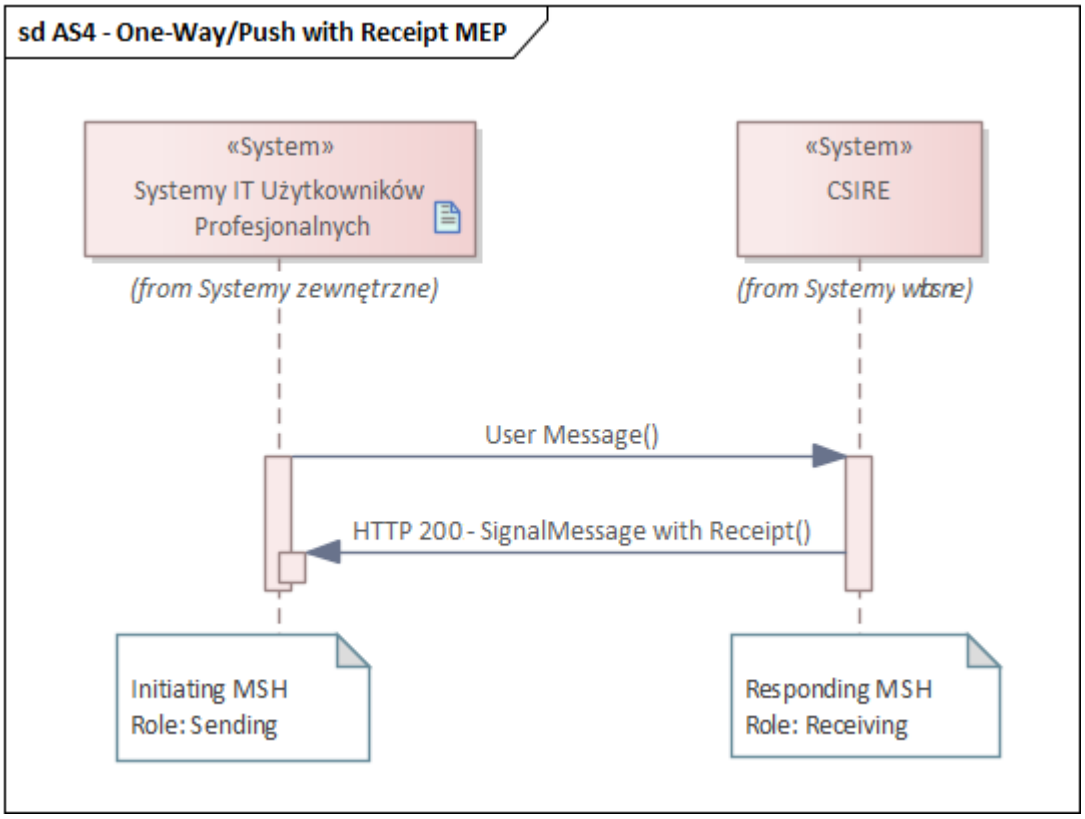
Wzorzec ten obrazuje następujący diagram:




Rysunek 3 One-Way/Push MEP

#### 5.4.1.1. Obsługa potwierdzeń - Receipts

System CSIRE może wysyłać element SignalMessage zawierający Receipt, aby potwierdzić odebranie wiadomości. Ta funkcjonalność jest dostępna dla operacji SendMessage i DequeueMessage, które są zrealizowane wg. wzorca One-Way/Push.




Rysunek 4 One-Way/Push MEP with Receipt

Receipt jest generowany jedynie w przypadku wiadomości poprawnej tzn. przyjętej do dalszego procesowania w CSIRE (brak błędu technicznego).

Wysyłanie Receipt jest kontrolowane za pomocą konfiguracji PMode: włączenie generowania Receipt wymaga ustawienia PMode[1].Security.SendReceipt = „Yes”.

Receipt może być generowany dla potwierdzenia odbioru lub dla niezaprzeczalności odbioru – kontrolowane jest to za pomocą PMode[1].Security.SendReceipt.NonRepudiation:

- PMode[1].Security.SendReceipt.NonRepudiation = „No” - Potwierdzenie jest wysyłane tylko dla potwierdzenia odbioru a element Receipt w odpowiedzi zawiera cały element UserMessage z wiadomości.
- PMode[1].Security.SendReceipt.NonRepudiation = „Yes” - Potwierdzenie jest wysyłane dla niezaprzeczalności i element Receipt w odpowiedzi zawiera element NonRepudiationInformation, a wewnątrz niego element Reference dla wszystkich części wiadomości w żądaniu:
  - W przypadku, gdy żądanie zostało podpisane cyfrowo: wszystkie elementy ds:Reference z Signature w żądaniu są kopiowane do odpowiedzi.
  - W przypadku, gdy żądanie nie zostało podpisane cyfrowo: element ds:Reference zostanie utworzony dla każdego elementu href eb:PartInfo w żądaniu.

#### 5.4.1.1.1. Przykład odpowiedzi na SendMessage z potwierdzeniem odbioru

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
    <env:Header>
```

```
         <ns2:Messaging xmlns:ns2="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/" xmlns:ns5="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns4="http://docs.oasis-open.org/ebxml-bp/ebbp-signals-2.0"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#" env:mustUnderstand="true">
              <ns2:SignalMessage>
                   <ns2:MessageInfo>
                        <ns2:Timestamp>2024-11-27T11:47:28.626Z</ns2:Timestamp>
                        <ns2:MessageId>4049956f-fd83-4a9a-81c4-d859a7ef0b07</ns2:MessageId>
                        <ns2:RefToMessageId>c4a8ecaf-0956-46a1-bf9c-
91b9ba2b888f</ns2:RefToMessageId>
                   </ns2:MessageInfo>
                   <ns2:Receipt>
                        <ns2:UserMessage>
                             <ns2:MessageInfo>
                                  <ns2:Timestamp>2024-11-27T12:47:27.000Z</ns2:Timestamp>
                                  <ns2:MessageId>c4a8ecaf-0956-46a1-bf9c-
91b9ba2b888f</ns2:MessageId>
                             </ns2:MessageInfo>
                             <ns2:PartyInfo>
                                  <ns2:From>
                                       <ns2:PartyId>Tu_wstaw_kod_EIC_Podmiotu</ns2:PartyId>
                                       <ns2:Role>Tu_wstaw_kod_roli_rynkowej_Podmiotu</ns2:Role>
                                  </ns2:From>
                                  <ns2:To>
                                       <ns2:PartyId>19VPL-348177312M</ns2:PartyId>
                                       <ns2:Role>MOP</ns2:Role>
                                  </ns2:To>
                             </ns2:PartyInfo>
                             <ns2:CollaborationInfo>

    <ns2:AgreementRef>urn:pl:oire:as4:agreement:SendMessage:SendReceipt</ns2:AgreementRef>
                                  <ns2:Service>MarketMessaging</ns2:Service>
                                  <ns2:Action>SendMessage</ns2:Action>
                                  <ns2:ConversationId>2011-921</ns2:ConversationId>
                             </ns2:CollaborationInfo>
                             <ns2:PayloadInfo>
                                  <ns2:PartInfo/>
                             </ns2:PayloadInfo>
                        </ns2:UserMessage>
                   </ns2:Receipt>
              </ns2:SignalMessage>
         </ns2:Messaging>
    </env:Header>
    <env:Body/>
</env:Envelope>
```

#### 5.4.1.1.2. Przykład odpowiedzi na SendMessage z niezaprzeczalnością odbioru

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
    <env:Header>
         <wsse:Security env:mustUnderstand="true" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
         <!-- !!! USUNIĘTO Z PRZYKŁADU!!! -->
         </wsse:Security>
         <ns2:Messaging env:mustUnderstand="true" xmlns:ns2="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/" xmlns:ns5="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns4="http://docs.oasis-open.org/ebxml-bp/ebbp-signals-2.0"
xmlns:ns3="http://www.w3.org/2000/09/xmlns3ig#">
              <ns2:SignalMessage>
                   <ns2:MessageInfo>
                        <ns2:Timestamp>2024-11-27T12:07:35.771Z</ns2:Timestamp>
                        <ns2:MessageId>443d67a6-4bde-4580-aac4-2f56ea4a3ebd</ns2:MessageId>
                        <ns2:RefToMessageId>df4e9164-ab55-4259-b1bf-
c23a91b90f1f</ns2:RefToMessageId>
                   </ns2:MessageInfo>
                   <ns2:Receipt>
                        <ns4:NonRepudiationInformation>
                             <ns4:MessagePartNRInformation>
                                  <ns3:Reference URI="#id-7B75DBBC5ED0DB848F1732709254837211">
                                       <ns3:Transforms>
                                            <ns3:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                       </ns3:Transforms>
                                       <ns3:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
```

```
     <ns3:DigestValue>H0iR5o4SLCEqRULs4kTuFuFHF2aP0y0iG1uZD+wKnuA=</ns3:DigestValue>
                                   </ns3:Reference>
                              </ns4:MessagePartNRInformation>
                              <ns4:MessagePartNRInformation>
                                   <ns3:Reference URI="#id-47C29F723C7122D486173434881372229">
                                        <ns3:Transforms>
                                             <ns3:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                        </ns3:Transforms>
                                        <ns3:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmlns3ig#sha256"/>

     <ns3:DigestValue>ZlgvaU55bGNVSE5MVjRsQ0UwZUM3YUVHUDI4=</ns3:DigestValue>
                                   </ns3:Reference>
                              </ns4:MessagePartNRInformation>
                         </ns4:NonRepudiationInformation>
                    </ns2:Receipt>
               </ns2:SignalMessage>
          </ns2:Messaging>
     </env:Header>
     <env:Body wsu:Id="id-f622ecd9-f4c8-450d-a16b-14ca437988a3" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"/>
</env:Envelope>
```

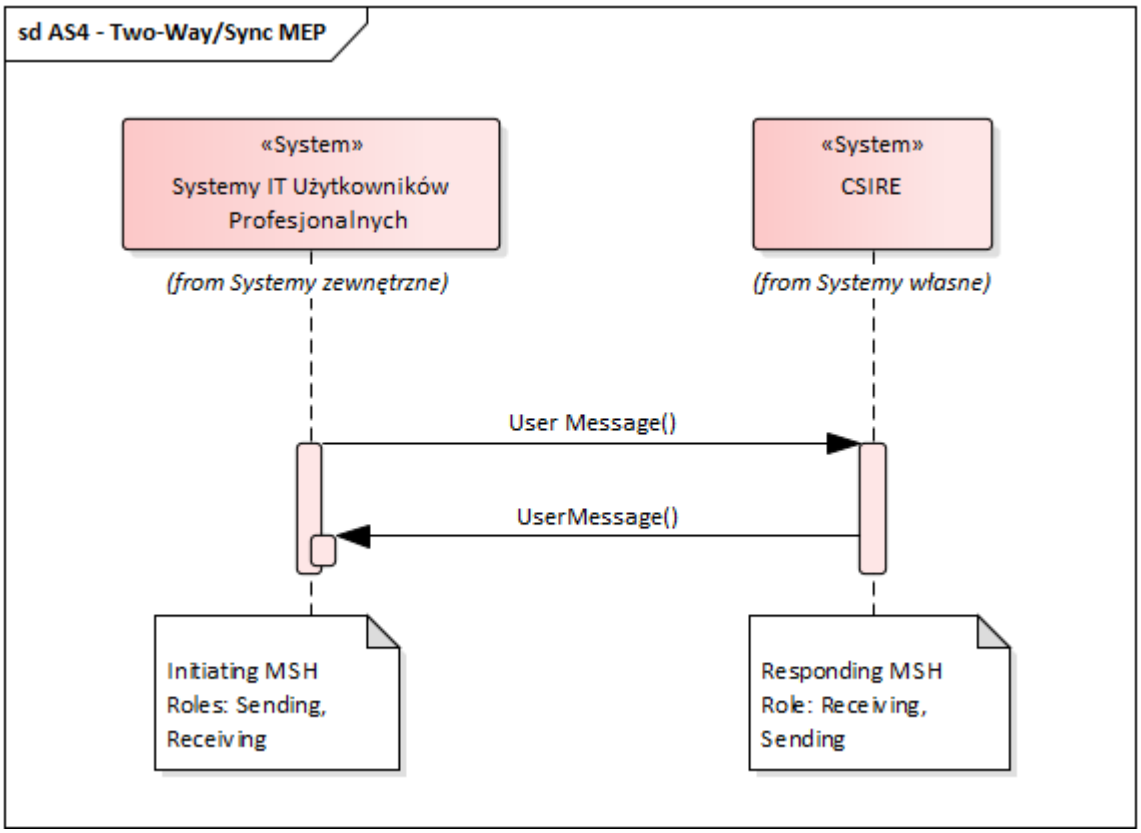
### 5.4.2. Two-Way/Sync MEP

Opis wzorca komunikacji można przedstawić za pomocą sekwencji następujących po sobie zdarzeń.

1. partner inicjujący (system zewnętrzny), wykorzystując Message Handler (*Initiating MSH*), wysyła wiadomość do partnera odbierającego (*Receiving MSH*).

2. odpytywany Message Handler (CSIRE) zwraca do partnera inicjującego synchronicznie odpowiedź na zadane żądanie.

Wzorzec ten obrazuje następujący diagram:




Rysunek 5 Two-Way/Sync MEP

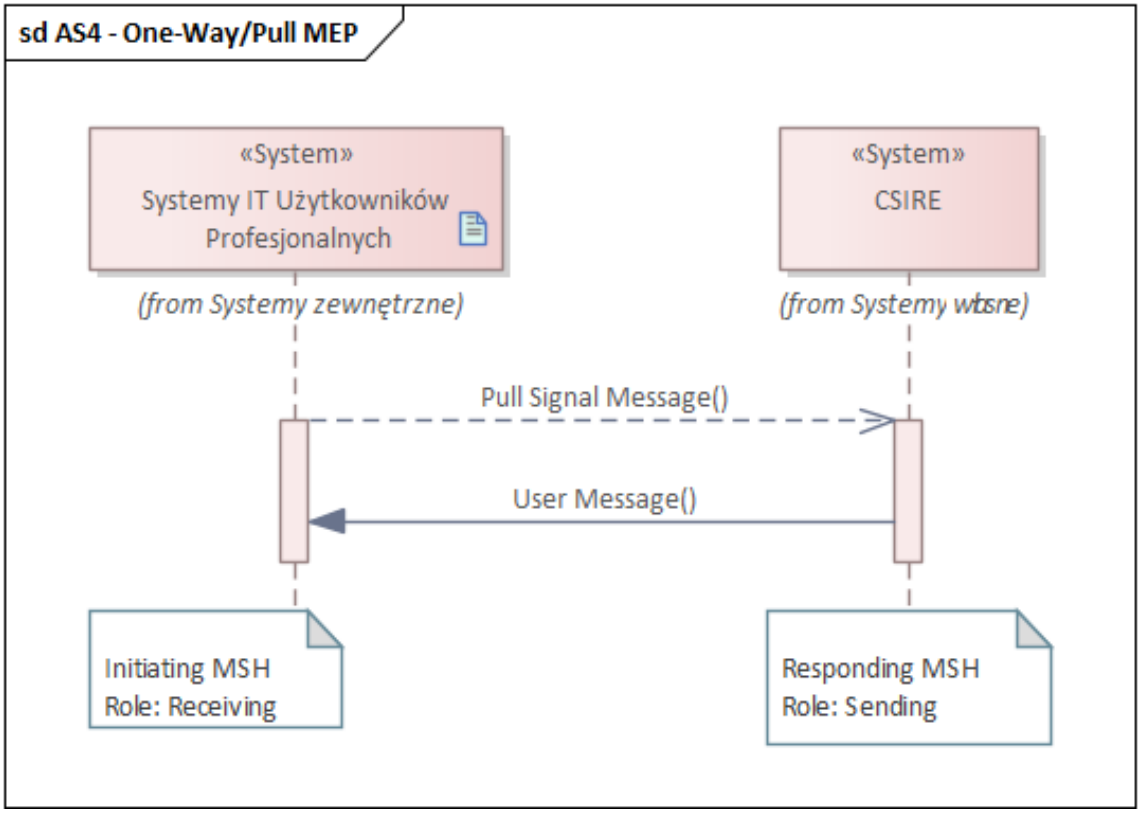
### 5.4.3. One-Way/Pull MEP

Opis wzorca komunikacji można przedstawić za pomocą sekwencji następujących po sobie zdarzeń.

1. partner inicjujący (system zewnętrzny), wykorzystując Message Handler (*Initiating MSH*), wysyła do partnera odbierającego (*Receiving MSH*) Signal Message zawierający element PullRequest.

2. odpytywany Message Handler (CSIRE) zwraca do partnera inicjującego synchronicznie odpowiedź na zadane żądanie.

Wzorzec ten obrazuje następujący diagram:




Rysunek 6 One-Way/Pull MEP

### 5.4.4. Wzorce komunikacji systemu CSIRE

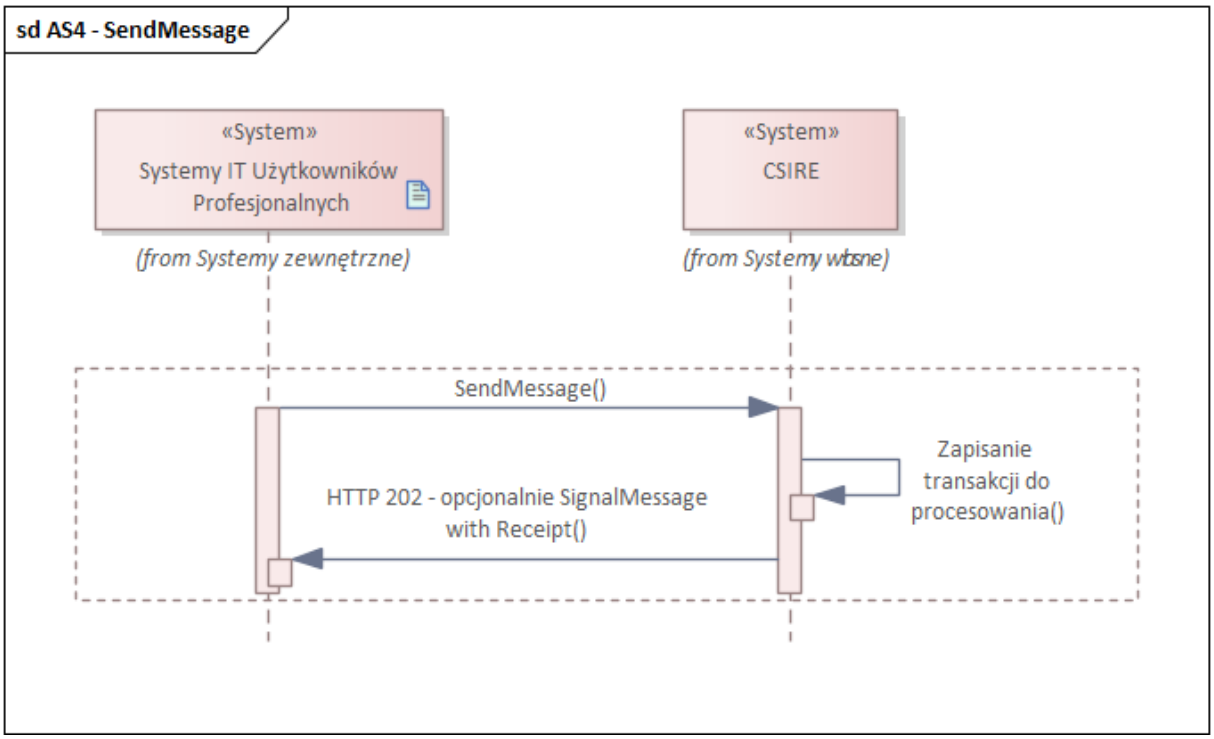
W następnych rozdziałach przedstawiono sposób komunikacji z systemem CSIRE przy wykorzystaniu mechanizmów AS4.

Dla przedstawionych operacji opisane są jedynie techniczne kody błędów tzn. takie które wynikają wprost z implementacji warstwy transportowej lub warstwy AS4. Dokument nie opisuje biznesowych kodów błędów pochodzących z TSKB – wiadomości zawierające takie kody biznesowe będą pobierane z użyciem operacji PeekMessage opisanej w rozdziałach 5.4.6.2. i 5.4.6.3. (analogicznie jak wszystkie inne wiadomości opisane w TSKB).

### 5.4.5. Wysłanie wiadomości do CSIRE

Aby wysłać wiadomość do CSIRE system zewnętrzny musi wywołać operację SendMessage, która będzie zrealizowana wg. wzorca One-Way Push.

W scenariuszu tym system zewnętrzny wysyła do CSIRE wiadomość i w sposób synchroniczny otrzymuje jedynie status odpowiedzi (HTTP 202) potwierdzający przyjęcie wiadomości do procesowania.




Rysunek 7 Operacja SendMessage

#### 5.4.5.1. Operacja SendMessage

- Jako wywołanie jest przesyłana wiadomość UserMessage (AS4) zawierająca payload zgodny z XSD (patrz 5.4.4.2).
- W przypadku przyjęcia wiadomości do procesowania zwracany jest kod HTTP 202, a wiadomość zapisywana jest w systemie do dalszego procesowania.
  Notyfikacje dotyczące przetwarzania (zgodne ze specyfikacją wiadomości opisaną w TSKB) zostaną wygenerowane przez CSIRE i będą pobierane z użyciem operacji PeekMessage, opisanej w rozdziałach 5.4. 6.2. i 5.4.6.3.
- W przypadku błędu przyjęcia wiadomości do procesowania zwracany jest komunikat zgodny z opisem w punktach 5.4.7 oraz 5.4.8

#### 5.4.5.2. Struktura wiadomości dla SendMessage

Struktura wiadomości UserMessage (AS4) przekazywanej w ramach operacji SendMessage

| Element | Kardynalność | Typ | Opis |
|---|---|---|---|
| SendMessageRequest | 1..1 | Complex Element | Główny element reprezentujący wywołanie SendMessage |
| MessageContainer | 1..1 | Complex Element | Element zawierający wiadomość przekazywaną w ramach operacji SendMessage |
| Payload | 1..1 | Complex Element | Zawiera wiadomość XML zgodną z schematem XSD opracowanym są na podstawie opisu komunikatów z TSKB i zgodnym ze specyfikacją XML Schema 1.0. |

#### 5.4.5.2.1. Przykład wywołania SendMessage

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
  <soapenv:Header>
    <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
soapenv:mustUnderstand="1">
      <eb:UserMessage>
        <eb:MessageInfo>
          <eb:Timestamp>2023-08-03T07:36:20.656Z</eb:Timestamp>
          <eb:MessageId>d7c3eccf-0781-4789-a456-035b39e8bb20</eb:MessageId>
        </eb:MessageInfo>
        <eb:PartyInfo>
          <eb:From>
            <eb:PartyId>ExampleParty1</eb:PartyId>
            <eb:Role>ExampleParty1RoleCode</eb:Role>
          </eb:From>
          <eb:To>
            <eb:PartyId>ExampleParty2</eb:PartyId>
            <eb:Role>ExampleParty2RoleCode</eb:Role>
          </eb:To>
        </eb:PartyInfo>
        <eb:CollaborationInfo>
          <eb:AgreementRef>SendMessageAgreementExample</eb:AgreementRef>
          <eb:Service>MarketMessaging</eb:Service>
          <eb:Action>SendMessage</eb:Action>
          <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
        </eb:CollaborationInfo>
      </eb:UserMessage>
    </eb:Messaging>
  </soapenv:Header>
  <soapenv:Body>
    <urn:SendMessageRequest>
      <urn:MessageContainer>
        <urn:Payload>
          ...
        </urn:Payload>
      </urn:MessageContainer>
    </urn:SendMessageRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

#### 5.4.5.2.2. Przykład wywołania SendMessage ze skompresowanym załącznikiem

Wywołanie na poziomie HTTP pokazujące sposób przekazania załącznika:

```
POST https://cmshostname.com/as4/PSE?organisationuser=SOMEUSER HTTP/1.1

Accept-Encoding: gzip,deflate
Content-Type: multipart/related; type="application/soap+xml"; start="<rootpart@soapui.org>";
boundary="----=_Part_9_1507953070.1700139714536"
MIME-Version: 1.0
Content-Length: 3850
Host: cmshostname.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.5.5 (Java/16.0.2)
------=_Part_9_1507953070.1700139714536
Content-Type: application/soap+xml; charset=UTF-8
Content-Transfer-Encoding: 8bit
Content-ID: <rootpart@soapui.org>

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
  xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
 <soap:Header>
  <eb:Messaging soap:mustUnderstand="true">
   <eb:UserMessage>
    <eb:MessageInfo>
     <eb:Timestamp>2023-11-16T07:56:03</eb:Timestamp>
     <eb:MessageId>31ad9125-2023-4293-af39-6c891a724c13</eb:MessageId>
    </eb:MessageInfo>
    <eb:PartyInfo>
     <eb:From>
```

```
        <eb:PartyId>ExampleParty1</eb:PartyId>
        <eb:Role> ExampleParty1RoleCode</eb:Role>
      </eb:From>
      <eb:To>
        <eb:PartyId>ExampleParty2
        </eb:PartyId>
        <eb:Role>ExampleParty2RoleCode</eb:Role>
      </eb:To>
     </eb:PartyInfo>
     <eb:CollaborationInfo>
      <eb:AgreementRef> SendMessageAgreementExample</eb:AgreementRef>
      <eb:Service>MarketMessaging</eb:Service>
      <eb:Action>SendMessage</eb:Action>
      <eb:ConversationId>2011-921</eb:ConversationId>
     </eb:CollaborationInfo>
     <eb:PayloadInfo>
      <eb:PartInfo href="cid:payload1_att.xml.gz">
       <eb:PartProperties>
        <eb:Property name="MimeType">application/xml</eb:Property>
        <eb:Property name="CharacterSet">utf-8</eb:Property>
        <eb:Property name="CompressionType">application/gzip</eb:Property>
       </eb:PartProperties>
      </eb:PartInfo>
     </eb:PayloadInfo>
    </eb:UserMessage>
  </eb:Messaging>
 </soap:Header>
 <soap:Body/>
</soap:Envelope>
------=_Part_9_1507953070.1700139714536
Content-Type: application/gzip; name=payload1_att.xml.gz
Content-Transfer-Encoding: binary
Content-ID: <payload1_att.xml.gz>
Content-Disposition: attachment; name="payload1_att.xml.gz"; filename="payload1_att.xml.gz"
---  BINARY COMPRESSED ATTACHMENT
```

Zdekompresowany, ze względu na czytelność, załącznik:

```
  <urn:SendMessageRequest xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:pl:oire:unk_2_1_1_1"
xmlns:urn2="urn:pl:oire:technical">
   <urn:MessageContainer>
    <urn:Payload>
      …
    </urn:Payload>
   </urn:MessageContainer>
  </urn:SendMessageRequest>
```

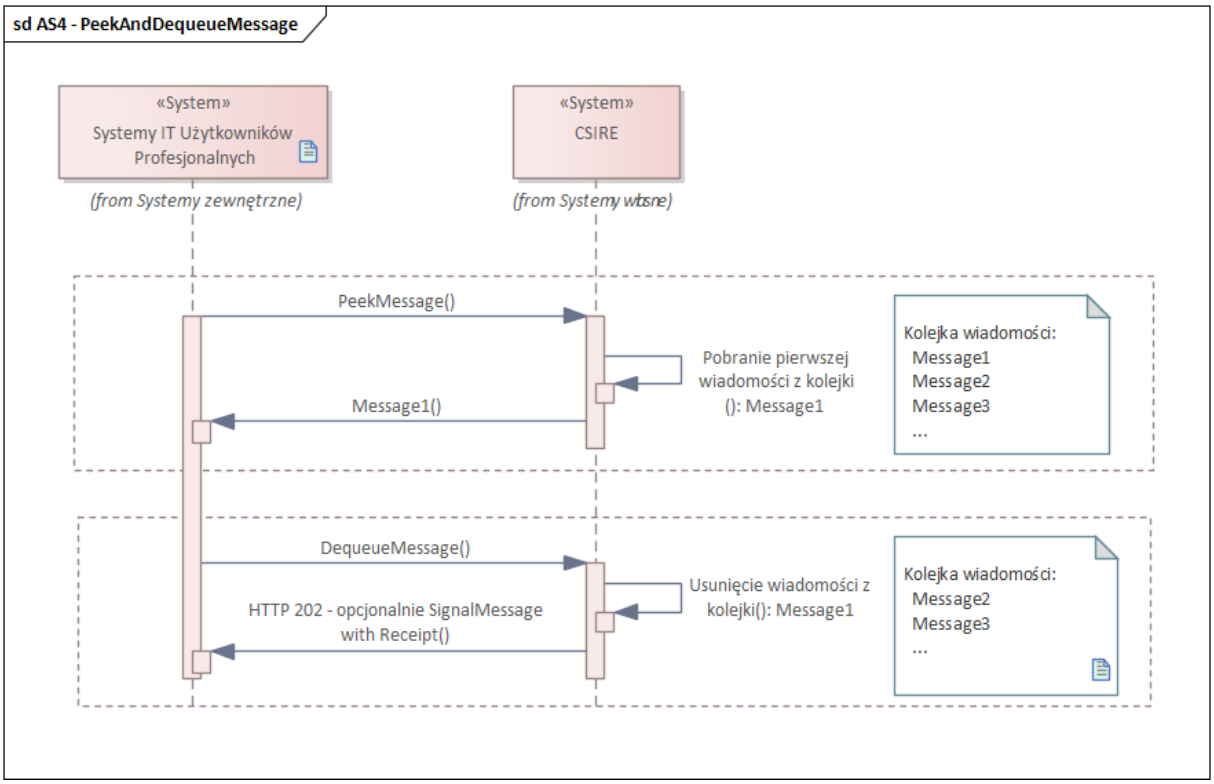
#### 5.4.5.2.3. Przykład odpowiedzi w przypadku błędu EBMS:0001

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                  xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
  <soapenv:Header>
    <eb:Messaging soapenv:mustUnderstand="1">
      <eb:SignalMessage>
        <eb:MessageInfo>
          <eb:Timestamp>2023-08-03T07:21:17.993Z</eb:Timestamp>
          <eb:MessageId>d7c3eccf-0781-4789-a456-035b39e8bb20</eb:MessageId>
        </eb:MessageInfo>
        <eb:Error origin="ebMS"
                  category="Content"
                  errorCode="EBMS:0001"
                  severity="failure"
                  refToMessageInError="d7c3eccf-0781-4789-a456-375b39e8bccf">
          <eb:Description>Value not recognized</eb:Description>
        </eb:Error>
      </eb:SignalMessage>
    </eb:Messaging>
  </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
```

### 5.4.6. Pobranie wiadomości z CSIRE

W celu zapewnienia niezaprzeczalności odebranie wiadomości z CSIRE zostało podzielone na dwie techniczne operacje:

- PeekMessage – zrealizowaną wg. wzorca Two-Way/Sync lub One-Way/Pull,
- DequeueMessage - zrealizowaną wg. wzorca One-Way/Push.

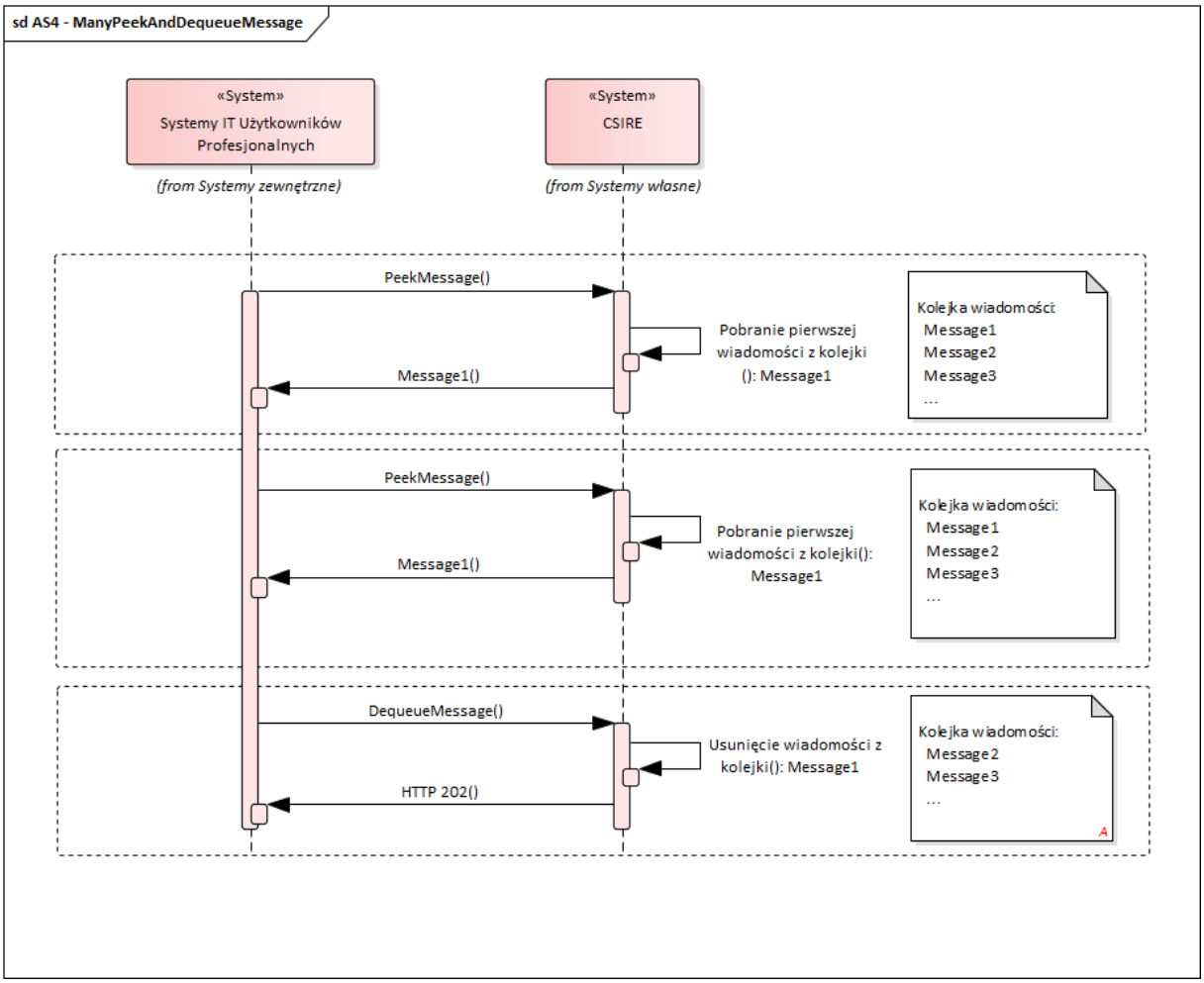



Rysunek 8 Operacje PeekMessage i DequeueMessage – prawidłowa sekwencja wywołań

Operacja PeekMessage służy do pobrania wiadomości z „kolejki” przez system zewnętrzny. Operacja ta zwraca pierwszą wiadomość w logicznej kolejce (zgodnie z FIFO), która nie została jeszcze usunięta. Należy pamiętać, że PeekMessage zwraca wiadomość, która może zostać przetworzona przez wywołującego PeekMessage, bez uprzedniego usunięcia tej wiadomości z kolejki (z użyciem operacji DequeueMessage opisanej niżej).

Obowiązkiem systemu informacyjnego Kontrahenta jest regularne przeglądanie, przetwarzanie i usuwanie wiadomości z kolejki. CSIRE będzie kontynuował przetwarzanie i przygotowywanie kolejnych wiadomości niezależnie od odbierania ich przez system informacyjny Kontrahenta. Wiadomości są dostarczane w kolejności, w jakiej CSIRE je utworzył.

Wielokrotne wywołanie operacji PeekMessage bez wywołania operacji DequeueMessage spowoduje zwrócenie tej samej wiadomości (patrz rysunek 7).




Rysunek 9 Pierwsze wywołanie PeekMessage bez DequeueMessage – nieprawidłowa sekwencja wywołań (jeśli nie chcemy ponownie pobrać tej samej wiadomości)

Do potwierdzenia poprawności pobrania wiadomości służy operacja DequeueMessage – po jej wykonaniu wiadomość jest usuwana z kolejki i system zewnętrzny będzie mógł przejść do pobierania następnej wiadomości.

Systemy zewnętrzne powinny cyklicznie odpytywać CSIRE (poprzez wywołanie operacji PeekMessage) odnośnie oczekujących wiadomości, w szczególności:

- W przypadku pobrania wiadomości z użyciem PeekMessage i technicznego potwierdzenia z użyciem DequeueMessage kolejne wywołanie PeekMessage powinno nastąpić niezwłocznie po wywołaniu DequeueMessage.
- W przypadku wywołania PeekMessage, dla którego CSIRE nie zwróciło wiadomości kolejne wywołanie PeekMessage powinno nastąpić po 15 sekundach.

#### 5.4.6.1. Kolejki wyjściowe z CSIRE

- Operacja PeekMessage (opisana w 5.4.6.2) umożliwia podanie nazwy kolejki (w elemencie MessageDomain), z której chcemy pobrać wiadomość.

- Jeśli w wywołaniu operacji PeekMessage podamy wiele nazw kolejek (wiele elementów MessageDomain) system CSIRE zwróci jedną, najstarszą wiadomość z kolejek przekazanych w wywołaniu.
- Jeśli w wywołaniu operacji PeekMessage nie podamy nazwy kolejki, system CSIRE zwróci jedną, najstarszą wiadomość ze wszystkich kolejek.
- Zdefiniowanie wielu kolejek wyjściowych umożliwia systemom zewnętrznych równoległe pobieranie z nich wiadomości.

| Nazwa kolejki | Przeznaczenie |
|---|---|
| AGREEMENTS | Wiadomości z grupy 1 procesów SWI |
| MPUPDATES | Wiadomości z grupy 2 procesów SWI |
| MPNOTIFICATIONS | Wiadomości z grupy 3 procesów SWI |
| MPREQUESTS | Wiadomości z grupy 4 procesów SWI |
| BRPCHANGE | Wiadomości z grupy 5 procesów SWI |
| DATALOAD | Wiadomości z grupy 6 procesów SWI bez profili dobowych (proces 6.1) |
| DAILYPROFILES | Wiadomości dotyczące zawierające profili dobowych (procesy 6.1, 7.1) |
| DATASHARE | Wiadomości z grupy 7 procesów SWI bez profili dobowych (proces 7.1) |
| CONNECTIONUPDATES | Wiadomości z grupy 8 procesów SWI |
| PARTIESINFOEXCHANGE | Wiadomości z grupy 9 procesów SWI |
| FACILITIESUPDATES | Wiadomości z grupy 10 procesów SWI |
| HISTORYDATALOAD | Wiadomości z grupy 11 procesów SWI |
| PROCESSINTERRUPTION | Wiadomości dotyczące przerwania realizacji procesów (macierz priorytetyzacji, timery oraz manualne) |
| SOFTVALIDATIONS | Wiadomości dotyczące „wyników walidacji miękkich” (pozostałe typu S) |

Tabela 7 Nazwy kolejek wyjściowych CSIRE

#### 5.4.6.2. Operacja PeekMessage

Operacja Peek Message może zostać wywołana zgodnie z wzorcem Two-Way/Sync lub One-Way/Pull

W przypadku użycia wzorca Two-Way/Sync:

- Wywołanie odpowiada wiadomości typu UserMessage (AS4) zawierającej payload zgodny z XSD (patrz 5.4.6.3)
- System zewnętrzny może w ramach wiadomości UserMessage wysłać informacje, z jakiej kolejki systemu CSIRE chce pobrać wiadomość (element Message Domain).
- Poprawne wywołanie skutkuje zwróceniem wiadomości typu UserMessage (AS4) zawierającej payload zgodny z XSD (patrz 5.4.6.3).
- Niepoprawne wywołanie skutkuje błędem zgodnym z punktami 5.4.7 oraz 5.4.8.

W przypadku użycia wzorca One-Way/Pull:

- Wywołanie nie zawiera wiadomości typu UserMessage (AS4)
- System zewnętrzny może wysłać informacje, z jakiej kolejki systemu CSIRE chce pobrać wiadomość poprzez użycie atrybutu MPC w SignalMessage.
- Możliwe jest pobranie wiadomości z wielu kolejek (ponieważ jest to również możliwe dla PeekMessage w ramach Two-Way/Sync). Zakładamy użycie średnika (;) jako separatora między nazwami kolejek podanymi w MPC.

- Jeśli wywołujący chce pobrać pierwszą dostępną wiadomość ze wszystkich kolejek powinien użyć domyślnej wartości kolejki *"http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC"* w polu MPC (zgodnie z "OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features" sekcja 3.4)
- Poprawne wywołanie skutkuje zwróceniem wiadomości typu UserMessage (AS4) zawierającej payload zgodny z XSD (patrz 5.4.6.3).
- Niepoprawne wywołanie skutkuje błędem zgodnym z punktami 5.4.7 oraz 5.4.8.
- Ponieważ wywołanie PeekMessage zgodnie z wzorcem One-Way/Pull nie zawiera elementu CollaborationInfo (zawierającego elementy Agreement, Service oraz Action wskazujące na zestaw parametrów PMode) system używa PMode skonfigurowanego dla:
  - PMode[1].BusinessInfo.Service = „MarketMessaging”
  - PMode[1].BusinessInfo.Action = „PeekMessage”

Jeśli zarówno wartość pola MPC (zgodnie z wzorcem One-Way/Pull), jak i payload w UserMessage (zgodnie z Two-Way/Sync) zostaną dostarczone w żądaniu PeekMessage, CSIRE odrzuci wiadomość z kodem błędu EBMS:0011 - ExternalPayloadError, ponieważ nadawca powinien jednoznacznie określić, z której kolejki chce pobrać wiadomość.

#### 5.4.6.3. Struktura wiadomości dla PeekMessage

Struktura wiadomości UserMessage (AS4) przekazywanej do systemu CSIRE jako wywołanie w przypadku użycia wzorca Two-Way/Sync:

| Element | Kardynalność | Typ | Opis |
|---|---|---|---|
| PeekMessageRequest | 1..1 | Complex Element | Główny element reprezentujący wywołanie PeekMessage |
| MessageDomains | 0..1 | Complex Element | Opcjonalny element zawierający liste kolejek z jakich należy pobrać wiadomość |
| MessageDomain | 1..n | xs:string max=100 | Element wskazujący z jakich kolejek z systemu CSIRE operacja PeekMessage ma pobrać pierwszą wiadomość |

Struktura wiadomości UserMessage (AS4) przekazywanej z CSIRE jako odpowiedź na wywołanie:

| Element | Kardynalność | Typ | Opis |
|---|---|---|---|
| PeekMessageResponse | 1..1 | Complex Element | Główny element reprezentujący odpowiedź na wywołanie PeekMessage |
| MessageContainer | 0..1 | Complex Element | Tylko dla wiadomości umieszczonych w kolejce |

| | | | |
|---|---|---|---|
| DocumentReferenceNumber | 1..1 | xs:string max=36 | Identyfikator DocumentReferenceNumber (i.e. UUID) wygenerowany przez CSIRE w celu zidentyfikowania transferu danych wiadomości, który powinien zostać wykorzystany do późniejszego Dequeue tej wiadomości |
| Payload | 1..1 | Complex Element | Zawiera komunikat XML zgodny ze schematem XSD opracowanym są na podstawie opisu komunikatów z TSKB i zgodnym ze specyfikacją XML Schema 1.0. |

#### 5.4.6.3.1. Przykład wywołania PeekMessage dla wzorca Two-Way/Sync

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
  <soapenv:Header>
    <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
soapenv:mustUnderstand="1">
      <eb:UserMessage>
        <eb:MessageInfo>
          <eb:Timestamp>2023-08-03T07:36:20.656Z</eb:Timestamp>
          <eb:MessageId>d7c3eccf-0781-4789-a456-035b39e8bb20</eb:MessageId>
        </eb:MessageInfo>
        <eb:PartyInfo>
          <eb:From>
            <eb:PartyId>ExampleParty1</eb:PartyId>
            <eb:Role>ExampleParty1RoleCode</eb:Role>
          </eb:From>
          <eb:To>
            <eb:PartyId>ExampleParty2</eb:PartyId>
            <eb:Role>ExampleParty2RoleCode</eb:Role>
          </eb:To>
        </eb:PartyInfo>
        <eb:CollaborationInfo>
          <eb:AgreementRef>PeekMessageAgreementExample</eb:AgreementRef>
          <eb:Service>MarketMessaging</eb:Service>
          <eb:Action>PeekMessage.request</eb:Action>
          <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
        </eb:CollaborationInfo>
      </eb:UserMessage>
    </eb:Messaging>
  </soapenv:Header>
  <soapenv:Body>
    <urn:PeekMessageRequest>
         <urn:MessageDomains>
            <urn:MessageDomain>DATALOAD</urn:MessageDomain>
         </urn:MessageDomains>
      </urn:PeekMessageRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

#### 5.4.6.3.1. Przykład wywołania PeekMessage dla wzorca One-Way/Pull

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
  <soapenv:Header>
    <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
soapenv:mustUnderstand="1">
      <eb:SignalMessage>
         <eb:MessageInfo>
         <eb:Timestamp>2024-02-19T11:30:11.320Z</eb3:Timestamp>
              <eb:MessageId>xxxx</eb:MessageId>.
         </eb:MessageInfo>
         <eb:PullRequest mpc="MPUPDATES;AGREEMENTS"/>
```

```
          </eb:SignalMessage>.
      </eb:Messaging>
  </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
```

#### 5.4.6.3.2. Przykład odpowiedzi PeekMessage

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
  <soapenv:Header>
    <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
soapenv:mustUnderstand="true">
      <eb:UserMessage>
        <eb:MessageInfo>
          <eb:Timestamp>2023-08-03T07:36:21.641Z</eb:Timestamp>
          <eb:MessageId>d7c3eccf-0781-4789-a456-375b39e8bccf</eb:MessageId>
        </eb:MessageInfo>
        <eb:PartyInfo>
          <eb:From>
            <eb:PartyId>ExampleParty2</eb:PartyId>
            <eb:Role>ExampleParty2RoleCode</eb:Role>
          </eb:From>
          <eb:To>
            <eb:PartyId>ExampleParty1</eb:PartyId>
            <eb:Role>ExampleParty1RoleCode</eb:Role>
          </eb:To>
        </eb:PartyInfo>
        <eb:CollaborationInfo>
          <eb:AgreementRef>PeekMessageAgreementExample</eb:AgreementRef>
          <eb:Service>MarketMessaging</eb:Service>
          <eb:Action>PeekMessage.reply</eb:Action>
          <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
        </eb:CollaborationInfo>
      </eb:UserMessage>
    </eb:Messaging>
  </soapenv:Header>
  <soapenv:Body>
    <urn:PeekMessageResponse>
      <urn:MessageContainer>
        <urn:DocumentReferenceNumber>cc3ae4a7-e93f-406a-99c8-
4bbc66ab5140</urn:DocumentReferenceNumber>
        <urn:Payload>
                  ...
        </urn:Payload>
      </urn:MessageContainer>
    </urn:PeekMessageResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

#### 5.4.6.3.3. Przykład odpowiedzi PeekMessage, gdy brak wiadomości w kolejce (EBMS:0006).

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <ns2:Messaging xmlns:ns2="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
                   xmlns:ns3="http://schemas.xmlsoap.org/soap/envelope/"
                   env:mustUnderstand="true">
      <ns2:SignalMessage>
        <ns2:MessageInfo>
          <ns2:Timestamp>2023-08-03T07:21:17.993Z</ns2:Timestamp>
          <ns2:MessageId>7d3e50b4-f372-4c48-865b-8193f3dd674c</ns2:MessageId>
          <ns2:RefToMessageId>10891C6e-8d0c-4701-9a1d-c84fd39d4832</ns2:RefToMessageId>
        </ns2:MessageInfo>
        <ns2:Error category="Communication"
                   errorCode="EBMS:0006"
                   origin="ebMS"
                   refToMessageInError="10891C6e-8d0c-4701-9a1d-c84fd39d4832"
                   severity="warning"
                   shortDescription="EmptyMessagePartitionChannel">
```

```
          <ns2:Description xml:lang="En">The Message queue is empty</ns2:Description>
          <ns2:ErrorDetail>The Message queue is empty</ns2:ErrorDetail>
        </ns2:Error>
      </ns2:SignalMessage>
    </ns2:Messaging>
  </env:Header>
  <env:Body/>
</env:Envelope>
```

#### 5.4.6.4. Operacja DequeueMessage

- Zrealizowaną jako wzorzec One-Way Push.
- Wywołanie odpowiada wiadomości typu UserMessage (AS4) zawierającej payload zgodny z XSD (patrz 5.4.5.5).
- Poprawne wywołanie skutkuje zwróceniem kodu HTTP 202.
- W przypadku błędu zwracany jest komunikat zgodny z opisem w punktach 5.4.7 oraz 5.4.8.

#### 5.4.6.5. Struktura wiadomości dla DequeueMessage

Struktura wiadomości UserMessage (AS4) przekazywanej do systemu CSIRE jako wywołanie:

| Element | Kardynalność | Typ | Opis |
|---|---|---|---|
| DequeueMessageRequest | 1..1 | Complex Element | Główny element reprezentujący wywołanie DequeueMessage |
| DocumentReferenceNumber | 1..1 | xs:string max=36 | UUID - DocumentReferenceNumber w komunikacie z poprzednio podglądniętego komunikatu (patrz PeekMessage). |

##### 5.4.6.5.1. Przykład wywołania DequeueMessage

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
  <soapenv:Header>
    <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
soapenv:mustUnderstand="1">
      <eb:UserMessage>
        <eb:MessageInfo>
          <eb:Timestamp>2023-08-03T07:36:20.656Z</eb:Timestamp>
          <eb:MessageId>d7c3eccf-0781-4789-a456-035b39e8bb20</eb:MessageId>
        </eb:MessageInfo>
        <eb:PartyInfo>
          <eb:From>
            <eb:PartyId>ExampleParty1</eb:PartyId>
            <eb:Role>ExampleParty1RoleCode</eb:Role>
          </eb:From>
          <eb:To>
            <eb:PartyId>ExampleParty2</eb:PartyId>
            <eb:Role>ExampleParty2RoleCode</eb:Role>
          </eb:To>
        </eb:PartyInfo>
        <eb:CollaborationInfo>
          <eb:AgreementRef>DequeueMessageAgreementExample</eb:AgreementRef>
          <eb:Service>MarketMessaging</eb:Service>
          <eb:Action>DequeueMessage</eb:Action>
          <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
        </eb:CollaborationInfo>
      </eb:UserMessage>
```

```
    </eb:Messaging>
  </soapenv:Header>
  <soapenv:Body>
    <urn:DequeueMessageRequest>
       <urn:DocumentReferenceNumber>cc3ae4a7-e93f-406a-99c8-
4bbc66ab5140</urn:DocumentReferenceNumber>
    </urn:DequeueMessageRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

### 5.4.7. Techniczne kody błędów na poziomie warstwy transportowej

| HTTP status | Kategoria | Znaczenie | Sugerowany sposób obsługi |
|---|---|---|---|
| 500 | Server | Błąd wewnętrzny systemu CSIRE | Ponowienie wywołania w późniejszym terminie. Kontakt z operatorem systemu w przypadku, gdyby problem nie ustąpił. |
| 404 | Client | Nieznana operacja | Sprawdzenie i poprawienie nazwy operacji przed ponowieniem wysyłki |
| 408 | Client | Timeout | Ponowienie wywołania w późniejszym terminie. Kontakt z operatorem systemu w przypadku, gdyby problem nie ustąpił. |
| 401 | Bezpieczeństwo | Odmowa dostępu | Odmowa dostępu — uwierzytelnianie użytkownika nie powiodło się lub nie zostało dostarczone w celu potwierdzenia tożsamości. |
| 413 | Client | Zbyt duża wiadomość | Proszę zweryfikować powód zbyt dużego rozmiaru wiadomości (np. zbyt wiele profili dobowych w ramach jednej wiadomości). Wiadomość powinna zostać podzielona na mniejsze części które powinny zostać wysłane ponownie. |
| 400 | Client | Błędne wywołanie | Błędne wywołanie – proszę sprawdzić dokładny opis błędu i poprawić wiadomość |

Tabela 8 Techniczne kody błędów

### 5.4.8. Techniczne kody błędów AS4

Kanał AS4 zawsze zwraca błędy jako ebMS SignalMessages (ze statusem HTTP: 4xx lub 5xx) z wyjątkiem EBMS:0006 (Pusty kanał partycji wiadomości) dla którego zwracany jest status HTTP 200.

| Kod błędu | Krótki opis (EN) | Ważność | Znaczenie | Sugerowany sposób obsługi |
|---|---|---|---|---|
| EBMS:0001 | ValueNotRecognized | Błąd | Dokument komunikatu jest dobrze sformułowany, a schemat prawidłowy, niemniej jednak jakiś element/atrybut zawiera wartość, której nie można rozpoznać i dlatego MSH nie może go użyć. | Popraw wiadomość i wyślij ponownie. |
| EBMS:0002 | FeatureNotSupported | Ostrzeżenie | Chociaż dokument komunikatu jest prawidłowo sformułowany, a schemat prawidłowy, niektórych wartości elementu/atrybutu nie można przetworzyć zgodnie z oczekiwaniami, ponieważ powiązana funkcja nie jest obsługiwana przez MSH. | Usuń nieobsługiwane wartości z wiadomości i wyślij poprawioną wiadomość. |
| EBMS:0003 | ValueInconsistent | Błąd | Chociaż dokument komunikatu jest dobrze sformułowany, a schemat prawidłowy, wartość niektórych elementów/atrybutów jest niespójna albo z treścią innego elementu/atrybutu, albo z trybem przetwarzania MSH, albo z wymaganiami normatywnymi specyfikacji ebMS. | Sprawdź, czy poprawić komunikat lub zmienić konfigurację PMode. Po poprawieniu wyślij ponownie wiadomość. |
| EBMS:0004 | Other | Błąd | | Sprawdź element ErrorDetail w Error, aby dowiedzieć się, co poszło nie tak. W przypadku, gdy payload nie jest prawidłowo sformułowany/schemat jest nieprawidłowy, payload musi zostać poprawiony przed próbą ponownego wysłania. |

| Kod błędu | Krótki opis (EN) | Ważność | Znaczenie | Sugerowany sposób obsługi |
|---|---|---|---|---|
| EBMS:0005 | ConnectionFailure | Błąd | MSH doświadcza tymczasowej lub trwałej awarii podczas próby otwarcia połączenia transportowego ze zdalnym MSH. | Odczekaj co najmniej 5 minut przed ponowną próbą. Spróbuj ponownie maksymalnie 3 razy, zanim skontaktujesz się z działem pomocy technicznej w celu uzyskania pomocy. |
| EBMS:0006 | EmptyMessagePartitionChannel | Ostrzeżenie | W kolejce wiadomości nie ma dostępnych wiadomości. *Zwracany ze statusem HTTP 200 | Ponów wywołanie po określonym czasie. |
| EBMS:0007 | MimeInconsistency | Błąd | Użycie MIME nie jest zgodne z wymaganym użyciem w tej specyfikacji. | Popraw załącznik i wyślij ponownie. |
| EBMS:0008 | FeatureNotSupported | Błąd | Chociaż dokument komunikatu jest dobrze sformułowany, a schemat prawidłowy, obecność lub brak niektórych elementów/atrybutów nie jest zgodna z możliwościami MSH w odniesieniu do obsługiwanych funkcji. | Popraw wiadomość i wyślij ponownie. |
| EBMS:0009 | InvalidHeader | Błąd | Nagłówek ebMS jest albo źle sformułowany jako dokument XML, albo nie jest zgodny z regułami pakowania ebMS. | Popraw wiadomość i wyślij ponownie. |
| EBMS:0010 | ProcessingModeMismatch | Błąd | Nagłówek ebMS lub inny nagłówek (np. niezawodność, bezpieczeństwo) oczekiwany przez MSH nie jest zgodny z oczekiwaną treścią na podstawie powiązanego trybu PMode. | Sprawdź, czy poprawić komunikat lub zmienić konfigurację PMode. Po poprawieniu wyślij ponownie wiadomość. |

| Kod błędu | Krótki opis (EN) | Ważność | Znaczenie | Sugerowany sposób obsługi |
|---|---|---|---|---|
| EBMS:0011 | ExternalPayloadError | Błąd | MSH nie jest w stanie rozpoznać odniesienia do zewnętrznego payloadu (tj. części, która nie jest zawarta w komunikacie ebMS, identyfikowanym przez identyfikator URI PartInfo/href). | Popraw załącznik lub nagłówek SOAP w wiadomości i wyślij ponownie. |
| EBMS:0101 | FailedAuthentication | Błąd | Podpis w nagłówku Security przeznaczony dla aktora SOAP „ebms” nie mógł zostać zweryfikowany przez moduł Security. | Sprawdź, czy publiczny certyfikat skonfigurowany w CSIRE jest nadal poprawny. Jeśli nie, popraw certyfikat publiczny. |
| EBMS:0102 | FailedDecryption | Błąd | Zaszyfrowane dane odnoszące się do nagłówka Security przeznaczonego dla aktora SOAP „ebms” nie mogły zostać odszyfrowane przez moduł zabezpieczeń. | Sprawdź, czy wiadomość jest zaszyfrowana popranych kluczem. |
| EBMS:0103 | PolicyNoncompliance | Błąd | Metody zabezpieczeń, parametry, zakres lub inne wymagania lub umowy na poziomie polityki bezpieczeństwa nie zostały spełnione. | Popraw wiadomość i wyślij ponownie. |

819

820 Tabela 9 Techniczne kody błędów AS4

### 5.4.9. Kody SOAP Fault

Kanał AS4 zwraca błędy jako elementy ebMS SignalMessages, które mogą również zawierać element SOAP Fault zawierający szczegółowe informacje na temat przyczyny błędu– poniżej wyszczególniono kody błędów zawracane w SOAP Fault wraz ze znaczeniem oraz sugerowanym sposobem obsługi.

| Error code | Type | SOAP Code | Message | Znaczenie | Sugerowany sposób obsługi |
|---|---|---|---|---|---|
| MHB.MHD.000 | System | Receiver | General Failure | Błąd ogólny | Ponownie wyślij wiadomość, używając nowych identyfikatorów wiadomości i transakcji, jeśli problem nadal występuje, skontaktuj się z Operatorem Rynku. |
| MHB.MHD.001 | Syntax | Sender | Message validation failed | Walidacja wiadomości nie powiodła się | Wyślij ponownie poprawioną wiadomość (błąd jest generowany w wypadku XML (payload) niezgodnego ze schematem XSD). |
| MHB.MHD.002 | System | Receiver | System configuration error | Błąd konfiguracji systemu | Wyślij wiadomość ponownie, jeśli problem będzie się powtarzał, skontaktuj się z Operatorem Rynku. |
| MHB.MHD.003 | Security | Sender | User not authorized for system function (e.g. not found, no rights for the operation or message type, user blocked or inactive) | Użytkownik nieuprawniony do funkcji systemu (np. nie znaleziono, brak uprawnień do operacji lub typu komunikatu, użytkownik zablokowany lub nieaktywny) | Sprawdź autoryzację i skontaktuj się z OIRE w przypadku pytań. Wyślij wiadomość ponownie po skorygowaniu autoryzacji. |
| MHB.MHD.004 | Security | Sender | Unknown request | Nieznane żądanie | Wyślij ponownie poprawioną wiadomość (błąd jest generowany w wypadku braku rozpoznania payloadu np. ze względu jego brak lub gdy podano nieznany namespace). |
| MHB.MHD.005 | System | Receiver | Back-end timeout | Timeout po stronie backend serwera | Wyślij wiadomość ponownie, jeśli błąd będzie się powtarzał, skontaktuj się z OIRE. System uniemożliwi dwukrotne przetworzenie wiadomości z tym samym identyfikatorem transakcji. Jeśli więc ponowne wysłanie spowoduje błąd MHB.MHD.006, system już przetworzył (lub nadal przetwarza) pierwszą wiadomość. |

| Error code | Type | SOAP Code | Message | Znaczenie | Sugerowany sposób obsługi |
|---|---|---|---|---|---|
| MHB.MHD.006 | Syntax | Sender | The provided Ids are not unique or have been used before | Podane identyfikatory nie są unikalne lub zostały już wcześniej użyte | Popraw identyfikator komunikatu lub którykolwiek z identyfikatorów transakcji, ponieważ nie są one unikalne i zostały już użyte. Popraw komunikat biznesowy i wyślij go ponownie (błąd jest generowany w sytuacji gdy komunikat XML zawiera MessageId zapisany w CSIRE). |
| MHB.MHD.007 | System | Sender | Unknown or invalid message reference (e.g. cannot dequeue the current message in the MessageQueue if message reference provided does not match the message reference that has been peeked before (i.e. current message)) | Nieprawiłdowa wartość DocumentReferenceNumber (np. w przypadku gdy nie można wywołać operacji DequeueMessage) | Numer DocumentReferenceNumber podany w żądaniu operacji DequeueMessage nie pasuje do dostępnego komunikatu w kolejce komunikatów. Popraw wywołanie i wyślij komunikat ponownie. |
| MHB.MHD.008 | Security | Sender | Message content unsecure | Niebezpieczna treść wiadomości | Treść wiadomości zawiera niebezpieczne elementy (np. SQL injection lub cross-site scripting). Wiadomość musi zostać dostosowana, zanim będzie mogła zostać zaakceptowana przez system. |
| MHB.MHD.009 | Security | Sender | User not authorized for organisation (e.g. System User neither matches PhysicalSender nor (one of) the delegated Organisation(s)) | Użytkownik nieautoryzowany dla organizacji (np. użytkownik systemu nie pasuje do PhysicalSender ani żadnej z delegowanych organizacji) | Sprawdź nagłówek wiadomości, konfigurację autoryzacji i delegacji oraz skontaktuj się z OIRE w przypadku pytań. Wyślij wiadomość ponownie po wprowadzeniu poprawek. |
| MHB.MHD.010 | Syntax | Sender | Unknown TenantCode in URL | Nieznany kod TenantCode w adresie URL | Popraw TenantCode w adresie URL i wyślij wiadomość ponownie. |
| MHB.MHD.011 | Syntax | Sender | Unknown System Function | Nieznana funkcja systemu | Nie można znaleźć funkcji systemowej opartej na treści wiadomości.<br><br>Skontaktuj się z OIRE (sprawdź, czy pola (np. BusinessProcess), które łączą się z funkcją systemową CSIRE, są prawidłowe). |

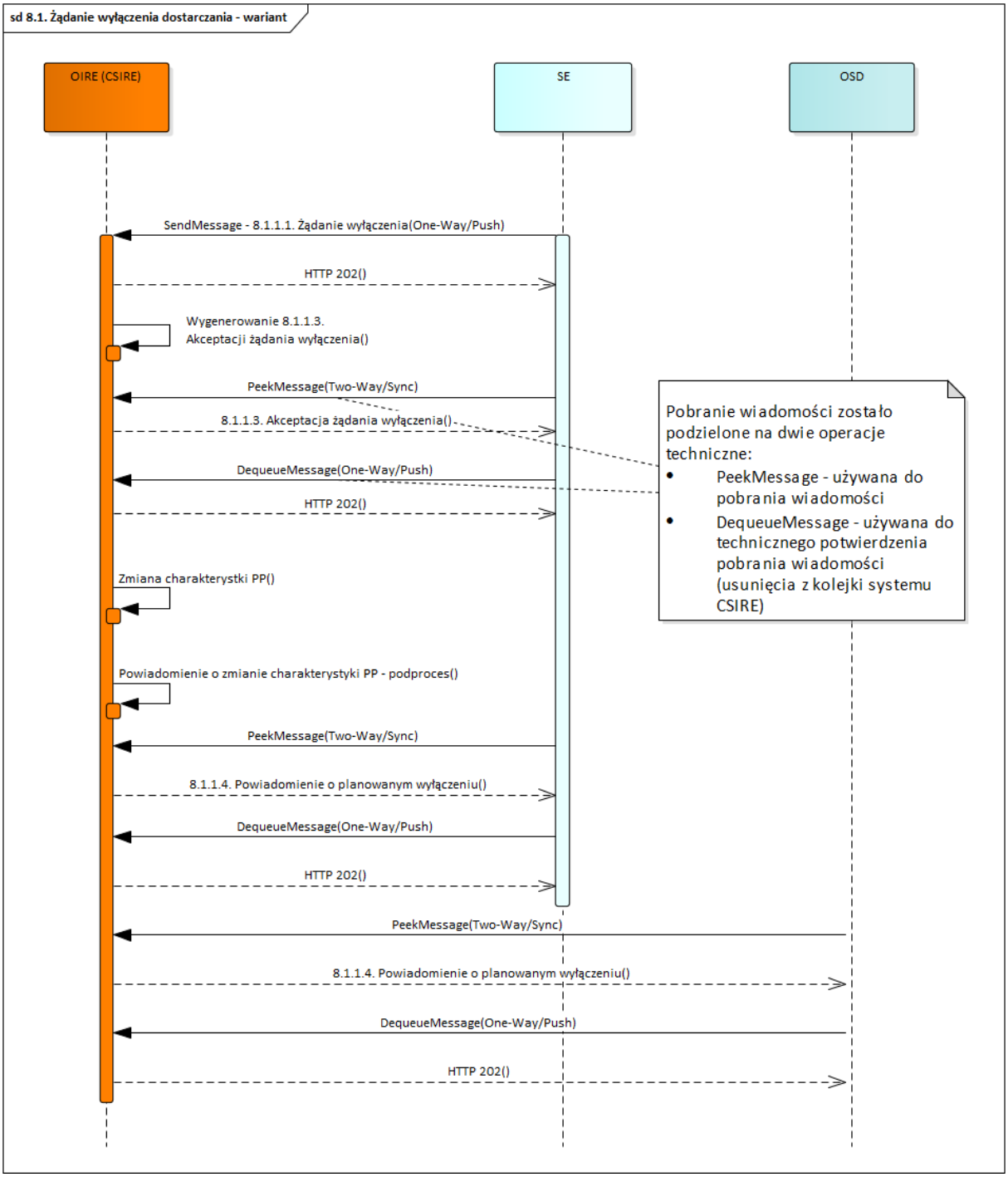
| Error code | Type | SOAP Code | Message | Znaczenie | Sugerowany sposób obsługi |
|---|---|---|---|---|---|
| [**Błąd nie może wystąpić w bieżącej implementacji AS4]**<br><br>*MHB.MHD.012* | *System* | *Sender* | *Number of messages exceeds maximum of <system_configured_maximum>* | *Liczba wiadomości przekracza maksymalną skonfigurowaną wartość.* | *Liczba wiadomości do przejrzenia w żądaniu PeekMessage jest większa niż dozwolona. Zmniejsz liczbę, aby mieściła się w dozwolonym zakresie i wyślij wiadomość ponownie.* |
| MHB.MHD.013 | Security | Sender | XML Signature verification failed | Weryfikacja podpisu XML nie powiodła się | Sprawdź, czy wszystkie elementy podpisu zostały dostarczone zgodnie ze specyfikacją (patrz sekcja 0) i w razie potrzeby wprowadź poprawki przed ponownym wysłaniem wiadomości. |
| MHB.MHD.014 | Throttling | Sender | Number of Organisation requests exceeded maximum allowed (throttling) | Liczba żądań dla organizacji przekroczyła maksymalny dozwolony limit | Funkcja systemu jest chroniona za pomocą ograniczania, zezwalając tylko na określoną liczbę żądań z organizacji wysyłającej w określonym przedziale czasu. Zmniejszenie liczby wysyłanych żądań do dozwolonego limitu. |
| MHB.MHD.015 | Security | Sender | Decryption Failed | Deszyfrowanie nie powiodło się | Sprawdzić, czy wszystkie elementy szyfrowania zostały dostarczone zgodnie ze specyfikacją i w razie potrzeby wprowadzić poprawki przed ponownym wysłaniem wiadomości. |
| MHB.MHD.016 | System | Sender | Peeking concurrently on identical MessageDomain is not allowed | Jednoczesne wywołanie PeekMessge na tej samej kolejce (MessageDomain) jest niedozwolone | Poczekaj przed kolejnym wywołaniem PeekMessage dla tej samej kolejki (MessageDomain) na odpwiedź z poprzedniego wywołania |
| MHB.MHD.017 | System | Sender | Dequeueing concurrently on identical DocumentReferenceNumber is not allowed | Jednoczesne wywołanie DequeueMessage dla identycznych numerów DocumentReferenceNumber jest niedozwolone. | Jednoczesne wywołanie DequeueMessage dla identycznych numerów DocumentReferenceNumber jest niedozwolone. |
| MHB.MHD.018 | Security | Sender | Unsupported security algorithm used: '<algorithm>' | Użyto nieobsługiwanego algorytmu zabezpieczeń | Wskazany algorytm nie może być używany jako algorytm podpisywania i/lub szyfrowania. Zmień algorytm na taki, który jest dozwolony. |

Tabela 10 Kody SOAP Fault

Przykład odpowiedzi zawierającej SOAP Fault:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope">
     <SOAP-ENV:Header>
          <ns2:Messaging SOAP-ENV:mustUnderstand="true" xmlns:ns2="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
xmlns:ns3="http://schemas.xmlsoap.org/soap/envelope/">
               <ns2:SignalMessage>
                    <ns2:MessageInfo>
                         <ns2:Timestamp>2024-12-19T14:12:35.127Z</ns2:Timestamp>
                         <ns2:MessageId>dbf573ee-7556-410d-84c7-bb1f0b09e264</ns2:MessageId>
                    </ns2:MessageInfo>
                    <ns2:Error category="Content" errorCode="EBMS:0001" origin="ebMS"
severity="failure" shortDescription="ValueNotRecognized">
                         <ns2:Description xml:lang="En">Unknown config version or Unknown
TenantCode in URL</ns2:Description>
                         <ns2:ErrorDetail/>
                    </ns2:Error>
               </ns2:SignalMessage>
          </ns2:Messaging>
     </SOAP-ENV:Header>
     <SOAP-ENV:Body>
          <SOAP-ENV:Fault>
               <SOAP-ENV:Code>
                    <SOAP-ENV:Value>SOAP-ENV:Sender</SOAP-ENV:Value>
               </SOAP-ENV:Code>
               <SOAP-ENV:Reason>
                    <SOAP-ENV:Text xml:lang="en">Unknown TenantCode in URL</SOAP-ENV:Text>
               </SOAP-ENV:Reason>
               <SOAP-ENV:Detail>
                    <urn:CMSFault xmlns:urn="urn:cms:b2b:v01">
                         <urn:ErrorCode>MHB.MHD.010</urn:ErrorCode>
                         <urn:ErrorIdentification>1734617555126</urn:ErrorIdentification>
                    </urn:CMSFault>
               </SOAP-ENV:Detail>
          </SOAP-ENV:Fault>
     </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

## 5.4.10. Przykład realizacji początkowych kroków procesu SWI z mapowaniem na wywołania interfejsu CSIRE




Rysunek 10 Diagram sekwencji wywołań systemu CSIRE dla początkowych kroków procesu 8.1. Żądanie wyłączenia dostarczania" dla "poprawnego" przebiegu.

Na powyższym diagramie przedstawiono sekwencję wywołań dla pierwszych kroków procesu „8.1. Żądanie wyłączenia dostarczania" z SWI przy założeniu rozpoczęcia procesu przez SE/SEu i poprawnej komunikacji z systemem CSIRE (brak błędów technicznych i biznesowych).

- Pierwsze wywołanie rozpoczynające proces to wywołanie operacji SendMessage przez SE. Jako payload wiadomości przekazywany jest komunikat „8.1.1.1. Żądanie wyłączenia” zgodny z TSKB. Odpowiedź HTTP 202 oznacza przyjęcie wiadomości do procesowania.
- Po odebraniu wiadomości system CSIRE w ramach procesu 8.1 wygeneruje wiadomość „8.1.1.3. Akceptacja żądania wyłączenia” zgodną z TSKB. Ta wiadomość będzie czekać na pobranie przez SE, który uprzednio wywołał operację SendMessage.
- SE z użyciem operacji PeekMessage pobiera wiadomość „8.1.1.3. Akceptacja żądania wyłączenia” a następnie potwierdza odebranie wywołując operacje DequeueMessage (odpowiedź HTTP 202 oznacza poprawne zdjęcie wiadomości z kolejki)
- System CSIRE po zmianie charakterystyki PP wygeneruje wiadomości „8.1.1.4. Powiadomienie o planowanym wyłączeniu”, zgodne z TSKB, do SE oraz odpowiedniego OSD.
- Zarówno SEr/SEu jak i OSD pobiorą wiadomość „8.1.1.4. Powiadomienie o planowanym wyłączeniu” z użyciem operacji PeekMessage oraz potwierdzą odebranie z użyciem operacji DequeueMessage.

# 6. BEZPIECZEŃSTWO

Rozdział ten opisuje zagadnienia konfiguracji zabezpieczeń dla wykorzystania Profilu AS4 zdefiniowanego w dokumencie „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile], w sposób zgodny z wymaganiami określonymi dla ENTSOG AS4 ebHandler oraz uwzględniający bieżące rekomendacje obowiązujące w PSE w zakresie stosowania zabezpieczeń kryptograficznych. Wymienione niżej wymagania konfiguracji zabezpieczeń stanowią aktualizację treści sekcji 2.3.4 „Security” dokumentu „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile].

## 6.1. Zabezpieczenie komunikacji w warstwie sieci

Dla zabezpieczenia komunikacji sieciowej pomiędzy partnerami zastosowanie mają zasady zawarte w rozdziale 2.3.4.1 „Network Layer Security” dokumentu „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile].

Dodatkowo, statyczne adresy (lub statyczne zakresy adresów) ustalone i zakomunikowane zgodnie z tymi zasadami powinny być użyte do ograniczenia swobody przepływów wiadomości przychodzących lub wychodzących, za pomocą urządzeń brzegowych sieci typu „firewall” lub urządzeń terminujących połączenia TLS, tylko z zarejestrowanymi uprzednio partnerami.

## 6.2. Zabezpieczenie komunikacji w warstwie transportowej

W celu zapewnienia poufności przesyłanych informacji w warstwie transportowej, spełnione muszą być warunki opisane w rozdziale 2.3.4.2 „Transport Layer Security” dokumentu „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile]. Zastosowanie mają zatem parametry opisane w rozdziale 2.2.6.1 „Transport Layer Security” tego dokumentu, z dodatkowymi zastrzeżeniami wymienionymi poniżej:

1. Wymagane jest użycie protokołu TLS w wersji 1.2 lub 1.3 (rekomendowana). Obsługa protokołów SSL 2.x, 3.x oraz TLS w wersjach 1.0, 1.1 musi być wyłączona.
2. W przypadku użycia TLS w wersji 1.3 strony komunikacji muszą wspierać obsługę zestawów algorytmów kryptograficznych TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256.
3. W przypadku użycia TLS w wersji 1.2 strony komunikacji muszą wspierać obsługę zestawów algorytmów kryptograficznych ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-POLY1305, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES256-GCM-SHA384, DHE-RSA-CHACHA20-POLY1305
4. Obsługa zestawów algorytmów kryptograficznych innych, niż wymienione powyżej musi być wyłączona.
5. Obustronne uwierzytelnianie mTLS musi być stosowane. W tym celu dopuszcza się wykorzystanie odpowiednich certyfikatów wydanych dla nazw DNS urządzeń występujących w podwójnej roli serwera i klienta TLS.
6. Certyfikaty wykorzystywane przez odrębne komponenty infrastruktury zapewniające obsługę komunikacji TLS muszą spełniać wszystkie warunki określone w punkcie 6.4 „Certyfikaty oraz Infrastruktura Klucza Publicznego (PKI)”.
7. Rekomendowane jest aby certyfikat na potrzeby zestawiania komunikacji mTLS był typu rozszerzonej walidacji EV (*ang. Extended Validation*), jednakże w ramach

Wydania 3.0 CSIRE dopuszczalne jest wykorzystanie certyfikatu typu walidacji organizacji OV (*ang. Organization Validation*). Certyfikat typu rozszerzonej walidacji EV musi być zaimplementowany od 20 września 2027.

## 6.3. Zabezpieczenie komunikacji w warstwie komunikatu

Lista wspieranych algorytmów podpisywania i szyfrowania komunikatów przedstawiona w poniższych rozdziałach może być rozszerzona w kolejnych wersjach niniejszego dokumentu.

Od 20 września 2027 podpisywanie oraz szyfrowanie komunikatów musi być realizowane z wykorzystaniem oddzielnych certyfikatów dedykowanych dla każdej z tych metod zabezpieczania (do powyższej daty dopuszczalne jest stosowanie jednego certyfikatu).

Do Wydania 3.0 CISRE (włącznie) dopuszczalne jest stosowanie certyfikatów S/MIME (*ang. Secure/Multipurpose Internet Mail Extensions).*

### 6.3.1. Podpisywanie wiadomości

CSIRE umożliwia podpisywanie wiadomości zarówno w przychodzących (żądanie), jak i wychodzących (odpowiedź/powiadomienie) wiadomościach. Podpis konfigurowany jest za pomocą parametru PMode PMode[1].Security.X509.Sign (patrz także 5.3.1).

CSIRE wspiera następujące standardy i specyfikacje w odniesieniu do WS-Security i podpisów XML:

- BasicSecurityProfile-v1.1
- XML-DSIG-V1.0 (prefiks DS)
- WSS-SOAP-Message-Security-V1.1.1 (prefiks WSSE)
- WSS-WSU-V1.0 (prefiks WSU)

Parametry/warianty dostępne do podpisywania wiadomości:

- Algorytmy podpisu dostępne w CSIRE:
  - (default) RSA-SHA256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)
  - RSA-SHA384 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha384)
  - RSA-SHA512 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha512)
- Funkcje skrótu dostępne w CSIRE:
  - SHA-1 (http://www.w3.org/2000/09/xmldsig#sha1)
  - (default) SHA-256 (http://www.w3.org/2001/04/xmlenc#sha256)
  - SHA-384 (http://www.w3.org/2001/04/xmldsig-more#sha384)
  - SHA-512 (http://www.w3.org/2001/04/xmlenc#sha512)
- Rekomendowane jest aby certyfikat do podpisu wiadomości posiadał wartość atrybutu użycia klucza (ang. *key usage*): niezaprzeczalność (ang. *non-repudiation lub ang. content commitment*).

### 6.3.2. Szyfrowanie wiadomości

CSIRE umożliwia szyfrowanie wiadomości XML zarówno w przychodzących (żądanie), jak i wychodzących (odpowiedź/powiadomienie) wiadomościach, przy czym można skonfigurować dla każdego kierunku, czy szyfrowanie XML powinno być zapewnione w wiadomościach, czy nie.

Wiadomości wejściowe:

- brak konfiguracji dla szyfrowania dla wiadomości wejściowych.
- CSIRE sprawdza wiadomość, czy jakikolwiek element zawiera znacznik EncryptedData i wtedy odszyfrowuje wiadomość.

Wiadomości wyjściowe:

- CSIRE używa parametru PMode PMode[1].Security.X509.Encryption.Encrypt (patrz sekcja 5.3.1) do kontrolowania, czy wiadomości wychodzące mają być szyfrowane przy użyciu publicznego certyfikatu przechowywanego dla organizacji.

Parametry i opcje używane do szyfrowania wiadomości:

- Typ identyfikatora klucza: Metoda, za pomocą której certyfikat jest identyfikowany po stronie odbiorcy.

  CSIRE stosuje następujący typ: Binary security token

  Binary security token direct reference: Certyfikat podpisujący jest konwertowany na BinarySecurityToken i wstawiany do nagłówka bezpieczeństwa. Odniesienie do binarnego tokenu bezpieczeństwa jest również wstawiane do wsse:SecurityReferenceToken. Oznacza to, że cały certyfikat podpisu jest przekazywany do odbiorcy.

- Algorytm szyfrowania klucza: Algorytm asymetryczny używany do szyfrowania klucza symetrycznego (np. AES).

- Rekomendowane jest aby certyfikat do szyfrowania wiadomości posiadał wartość atrybutu użycia klucza (*ang. key usage*): szyfrowanie klucza (*ang. key encipherment*), szyfrowanie danych (*ang. data encipherment*)
- Wybór dostępny na liście jest kontrolowany przez WS-Security Framework.

  Algorytmy szyfrowania klucza dostępne w CSIRE:

  - (default) RSA-OAEP including MGF1 with SHA1 (http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p)
  - RSA-v1.5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5)
  - RSA-OAEP (http://www.w3.org/2009/xmlenc11#rsa-oaep)

- Algorytm szyfrowania: Algorytm stosowany do szyfrowania payload przy użyciu klucza symetrycznego wiadomości.

  CSIRE udostępnia poniższe algorytmy:

  - (default) AES128-GCM (http://www.w3.org/2009/xmlenc11#aes128-gcm)

- AES192-GCM (http://www.w3.org/2009/xmlenc11#aes192-gcm)
- AES256-GCM (http://www.w3.org/2009/xmlenc11#aes256-gcm)

Zachowane ze względu na kompatybilność wsteczną – niezalecane:

- AES-128-CBC (http://www.w3.org/2001/04/xmlenc#aes128-cbc)
- AES-192-CBC (http://www.w3.org/2001/04/xmlenc#aes192-cbc)
- AES-256-CBC (http://www.w3.org/2001/04/xmlenc#aes256-cbc)

## 6.4. Certyfikaty oraz Infrastruktura Klucza Publicznego (PKI)

Dla certyfikatów cyfrowych wykorzystywanych do zabezpieczenia komunikacji w warstwie komunikatu oraz certyfikatów cyfrowych wykorzystywanych do zabezpieczenia komunikacji w warstwie transportowej, stosuje się zasady opisane w rozdziale 2.3.4.4 „Certificates and Public Key Infrastructure" dokumentu „ENTSOG AS4 Profile 3.6" [EG-AS4-Profile], z zastrzeżeniem poniższych wyjątków i dodatkowych warunków:

1. Wybór Urzędu Certyfikacji PKI wydającego certyfikaty nie podlega przeglądowi przez ENTSOG.
2. Kody EIC nie są wymagane w żadnym polu w certyfikacie np. CommonName
3. Certyfikaty przeznaczone do wykorzystania produkcyjnego muszą być wydane przez powszechnie zaufane Centrum Certyfikacji PKI, spełniające warunki dla kwalifikowanych podmiotów świadczących usługi zaufania, zgodnie z przepisami rozporządzenia eIDAS i zarejestrowane na liście zaufania opublikowanej w witrynie „EU Trust Services Dashboard" Komisji Europejskiej, lub posiadające pieczęć AICPA/CICA WebTrust.
4. Nie dopuszcza się stosowania tych samych certyfikatów w środowiskach produkcyjnych i środowiskach testowych.
5. Informacje o statusie odwołania wykorzystywanych certyfikatów, muszą być udostępniane w sposób niezawodny pod dostępnym dla stron uczestniczących w komunikacji adresem wskazanych w atrybutach CDP (CRL Distribution Point) lub AIA OCSP certyfikatu pod rygorem odrzucenia weryfikowanych tymi certyfikatami połączeń lub wiadomości.

## 6.5. Wymiana certyfikatu

Procedura manualna – użytkownik pełniący rolę ABIRE dla danego Kontrahenta będzie samodzielnie konfigurować certyfikat z użyciem Portalu Użytkownika profesjonalnego (proces zarządzania certyfikatami danego Kontrahenta jest w jego zakresie odpowiedzialności).

# 7. KOMPRESJA

Payload komunikatów AS4, wysyłany w ramach SendMessage, musi być skompresowany, aby umożliwić wydajne przesyłanie danych. Analogicznie dane odbierane przez system zewnętrzny z użyciem PeekMessage również muszą być skompresowane.

W przypadkach, gdy będzie to wydajnościowo uzasadnione, duże narzuty na kompresję/dekompresję, względem uzyskanych z tego tytułu korzyści, dopuszcza się możliwość przesyłania komunikatów bez kompresji.

Stosowanie kompresji musi być zgodne z opisem profilu AS4 (patrz sekcja 3.1 w “AS4 Profile of ebMS 3.0 Version 1.0 OASIS Standard” [AS4-Profile]).

Kompresować można tylko payload podany jako załącznik SOAP, kompresja wiadomości przekazana w ramach treści wiadomości SOAP jest niedozwolona. Skompresowany załącznik SOAP musi być zgodny ze specyfikacją protokołu SOAP z załącznikami „SOAP Messages with Attachments” [SOAPATTACH].

Wpieranym algorytmem kompresji jest GZIP („GZIP file format specification version 4.3” [RFC1952]) – dane muszą być skompresowane przed dodaniem jako załącznik SOAP, zaś typ skompresowanego załącznika musi być ustawiony jako „application/gzip”.

# 8. IMPLEMENTACJA ROZWIĄZANIA

## 8.1. Wprowadzenie

Wiele z parametrów przetwarzania (P-Mode'ów) definiuje w sposób jednoznaczny techniczne ustawienia i wymagania dotyczące implementacji, niemniej jednak istnieją parametry które wymagają konfiguracji i muszą być zaimplementowane zgodnie z wytycznymi i wskazówkami biznesowymi opisanymi poniżej.

## 8.2. Identyfikacja stron

Jednym z podstawowych warunków poprawnej wymiany wiadomości pomiędzy stronami, w ramach opisanego w tym dokumencie profilu, jest możliwość jednoznacznej identyfikacji podmiotów uczestniczących w komunikacji. Wobec powyższego, obligatoryjnym warunkiem do zapewnienia poprawnej komunikacji jest stosowanie przez strony kodów EIC jako identyfikatorów stron komunikacji.

Kod EIC musi być używany w dwóch parametrach trybów przetwarzania wiadomości. Mowa tutaj o wartościach dla PMode.Initiator.Party, oraz PMode.Responder.Party.

Identyfikatory EIC stron komunikacji AS4 pozwalają na jednoznaczną identyfikację Kontrahenta.

Partnerem komunikacyjnym może być zarówno Kontrahent, jak i podmiot zewnętrzny (np. Nadawca fizyczny), świadczący usługi komunikacyjne B2B na rzecz różnych Kontrahentów. W wymianie wiadomości, wykorzystywany kod EIC zawsze będzie kodem Kontrahenta.

Podmiot zewnętrzny świadczący usługi komunikacyjne B2B na rzecz innych podmiotów (np. Nadawca fizyczny) będzie identyfikowany na podstawie tożsamości systemu w CSIRE.

Poza kodem EIC przekazywanym w konfiguracji AS4 PMode oraz nagłówkami komunikatów AS4, do identyfikacji stron wymagane są dodatkowe kroki:

- Tożsamość systemu musi zostać utworzona w CSIRE dla każdej Organizacji.
- Tożsamość systemu wymaga rejestracji certyfikatu klienta, który należy również dostarczyć przy każdym żądaniu do CSIRE (wzajemny TLS), patrz także sekcja 6.4.
- Dla każdej Organizacji należy utworzyć w systemie Użytkownika Organizacji z unikalną nazwą użytkownika.
- Aby korzystać z kanału CSIRE AS4, Użytkownik Organizacji musi posiadać uprawnienia do operacji Systemu: SendMessage, PeekMessage i DequeueMessage (patrz także punkt 5.4).

W wypadku Kontrahenta posiadającego więcej niż jedną rolę rynkową w CSIRE tworzona jest taka liczba Organizacji ile jest par: kod EIC oraz rola rynkowa z uwzględnieniem powyższych uwarunkowań.

### 8.2.1. Identyfikacja OIRE

OIRE identyfikują wartości podane w poniższej tabeli.

| EIC Code | EIC Name | Display Name | EIC Parent | VAT Code | Function |
|---|---|---|---|---|---|
| 19VPL-348177312M | Centralny System Inf. Rynku Energii / Operator Inf. Rynku Energii | PL_DATA_HUB | | | IT-system |

Tabela 10 Kod EIC OIRE

### 8.2.2. Kody ról rynkowych

Kontrahentów identyfikują kody ról rynkowych podane w poniższej tabeli.

| Rola rynkowa | Kod roli rynkowej |
|---|---|
| Operator – OSD | DSO |
| Operator – OSP | TSO |
| Sprzedawca | SE |
| POB | BRP |
| Użytkownik Uprawniony | AUS |
| OIRE | MOP |

Tabela 11 Role rynkowe

### 8.2.3. Przykład wywołania SendMessage

Dla Kontrahenta A (ExampleParty1=Kod EIC Kontrahenta A; ExampleParty1RoleCode= Kod roli rynkowej Kontrahenta A).

Dla Kontrahenta B (ExampleParty1=Kod EIC Kontrahenta B; ExampleParty1RoleCode= Kod roli rynkowej Kontrahenta B).

Dla kolejnych Kontrahentów identycznie.

OIRE to zawsze (ExampleParty2=Kod EIC OIRE; ExampleParty2RoleCode= Kod roli rynkowej OIRE).

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
<soap:Header>
 <eb:Messaging soap:mustUnderstand="true">
  <eb:UserMessage>
   <eb:MessageInfo>
     <eb:Timestamp> 2024-05-25T00:00:00+02:00</eb:Timestamp>
     <eb:MessageId>181c3aa2-53b8-4eb5-a521-d6236cfae85f</eb:MessageId>
   </eb:MessageInfo>
   <eb:PartyInfo>
     <eb:From>
       <eb:PartyId>ExampleParty1</eb:PartyId>
       <eb:Role>ExampleParty1RoleCode</eb:Role>
     </eb:From>
     <eb:To>
       <eb:PartyId>ExampleParty2</eb:PartyId>
       <eb:Role>ExampleParty2RoleCode</eb:Role>
     </eb:To>
   </eb:PartyInfo>
   <eb:CollaborationInfo>
     <eb:AgreementRef>urn:pl:oire:as4:agreement:SendMessage</eb:AgreementRef>
     <eb:Service>MarketMessaging</eb:Service>
     <eb:Action>SendMessage</eb:Action>
     <eb:ConversationId>2011-921</eb:ConversationId>
   </eb:CollaborationInfo>
   <eb:PayloadInfo>
    <eb:PartInfo/>
   </eb:PayloadInfo>
  </eb:UserMessage>
 </eb:Messaging>
```

```
</soap:Header>
<soap:Body>
  <urn:SendMessageRequest xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:pl:oire:unk_2_1_1_1:v1"
xmlns:urn2="urn:pl:oire:technical:v1">
  <urn:MessageContainer>
    <urn:Payload>
      <urn1:MeteringPointCreationNotification>
        <urn1:Header>
          <urn2:MessageId>5c9b488f-4af2-4d02-14fd-583e9090dbd9</urn2:MessageId>
          <urn2:MessageType>2.1_1</urn2:MessageType>
          <urn2:MessageTypeResponsibleOrganization>x</urn2:MessageTypeResponsibleOrganization>
          <urn2:MessageTimestamp>2024-05-25T00:00:00+02:00</urn2:MessageTimestamp>
          <urn2:PhysicalSenderId>ExampleParty1</urn2:PhysicalSenderId>
          <urn2:PhysicalSenderIdResponsibleOrganization>x
          </urn2:PhysicalSenderIdResponsibleOrganization>
          <urn2:JuridicalSenderId>ExampleParty1</urn2:JuridicalSenderId>
          <urn2:JuridicalSenderIdResponsibleOrganization>x
          </urn2:JuridicalSenderIdResponsibleOrganization>
          <urn2:PhysicalRecipientId>ExampleParty2/CSIRE</urn2:PhysicalRecipientId>
          <urn2:PhysicalRecipientIdResponsibleOrganization>x
          </urn2:PhysicalRecipientIdResponsibleOrganization>
          <urn2:JuridicalRecipientId>ExampleParty2</urn2:JuridicalRecipientId>
          <urn2:JuridicalRecipientIdResponsibleOrganization>x
          </urn2:JuridicalRecipientIdResponsibleOrganization>
        </urn1:Header>
 . . . . . .
      </urn1:MeteringPointCreationNotification>
    </urn:Payload>
  </urn:MessageContainer>
  </urn:SendMessageRequest>
</soap:Body>
</soap:Envelope>
```

## 8.3. Dostarczenie wiadomości, powtórzenia, obsługa niedostępności

Systemy zewnętrzne komunikujące się z CSIRE powinny zapewnić, by każda wiadomość została dostarczona. W przypadku wystąpienia problemu komunikacyjnego podczas pierwszej próby, należy wymusić po stronie wysyłającego implementację ponownej wysyłki wiadomości.

Jednocześnie należy dopilnować, by żaden system zewnętrzny nie wygenerował zbyt dużego ruchu sieciowego, poprzez nieustanne podejmowane próby ponownego wysłania wiadomości, która nie może być z powodów technicznych dostarczona (patrz kody błędów opisane w 5.4.7 i 5.4.8).

Rekomenduje się, by parametr dotyczący maksymalnej liczby powtórzeń (ang. *max retries*) był ustawiony na wartość nie mniejszą niż 2 i nie większą niż 5.

Jednocześnie okres, po którym podjęta zostanie kolejna próba dostarczenia wiadomości (ang. *retry period*), nie powinien być mniejszy niż 5000 millisekund.

Dodatkowym zaleceniem dla systemów zewnętrznych jest zwiększanie tego okresu po każdej ponowionej próbie.

W przypadku nieudanego wywołania operacji DequeueMessage z błędem: *MHB.MHD.007 „Unknown or invalid message reference”* (pomimo kilkukrotnego ponowienia zgodnie z rekomendacjami powyżej) zaleca się kontynuacje procesu pobierania wiadomości z kolejki, czyli:

- Wywołania operacji PeekMessage,
- następnie wywołania operacji DequeueMessage dla nowo pobranej wiadomości.

Błąd wywołania DequeueMessage: *MHB.MHD.007 „Unknown or invalid message reference”* oznacza, iż wiadomości o podanym identyfikatorze została już uprzednio usunięta (przez inne wywołanie DequeueMessage lub z Portalu Użytkownika profesjonalnego) lub nigdy nie było jej w CSIRE, więc dalsze ponawianie zawsze zwróci ten sam błąd.

W wypadku problemów w komunikacji, których nie można obsłużyć za pomocą powyżej opisanych mechanizmów, wykorzystywane są metody opisane w rozdziale „Procedury awaryjne stosowane w przypadku awarii CSIRE" IRiESP-OIRE.

Systemy zewnętrzne powinny mieć możliwość kolejkowania wiadomości, których nie udało się dostarczyć do CSIRE (np. z powodu niedostępności) tak, by możliwe było ponowne ich wysłanie po ustąpieniu niedostępności.

Kolejkowanie wiadomości powinno być zrealizowane w taki sposób, aby zapewnić persystencje wiadomości, odporność na awarie (wyłączenie) oraz możliwość ponowienia zgodnie z oryginalną kolejnością.

System informacyjny podmiotu zewnętrznego powinien posiadać funkcjonalność ręcznego (tj. inicjowanego przez jego użytkownika) oraz automatycznego (tj. realizowanego wg. zdefiniowanych reguł) wznowienia wysyłania komunikatów po przywróceniu komunikacji z CSIRE.

## 8.4. Idempotencja

Identyfikatory wiadomości przesyłane do CSIRE przez uczestników rynku w wiadomościach biznesowych (payload) muszą być unikalne. W przypadku, gdy podany identyfikator komunikatu lub identyfikator transakcji nie jest unikalny, CSIRE odrzuca żądanie, odpowiadając komunikatem EBMS:0004.

Możliwe jest jednak, że wiadomość wysłana przez CSIRE do systemu informacyjnego Kontrahenta nie została odebrana lub nie została prawidłowo przetworzona przez jego system informacyjny. W takim przypadku system informacyjny Kontrahenta powinien mieć możliwość odebrania oryginalnej odpowiedzi, aby umożliwić jej prawidłowe przetworzenie.

Dla powyższego scenariusza CSIRE wspiera idempotencję: wysyłając to samo żądanie (wiadomość biznesowa (payload) z tym samym MessageId) Kontrahent otrzyma odpowiedź na oryginalną, pierwotną, wiadomość. Oznacza to również, że wiadomość ponowiona nie będzie dalej przetwarzana (tj. nie zostanie wykonany żaden proces biznesowy, gdyż proces biznesowy został uruchomiony dla pierwotnej wiadomości).

Idempotencja działa tylko przez ograniczony czas (określony poprzez wartość globalnego parametru ustawianego w CSIRE) od przekazania pierwotnej wiadomości, po jego przekroczeniu CSIRE odpowie komunikatem o błędzie EBMS:0004.

*Decyzja o wykorzystaniu niniejszej funkcjonalności oraz okresu jej działania zostanie podjęta na podstawie doświadczeń z testów i pilotażu.*

## 8.5. Wymagania odnośnie środowisk systemów współpracujących z CSIRE

Każdy podmiot, który zamierza korzystać z systemu informacyjnego współdziałającego z CSIRE, musi dysponować środowiskiem produkcyjnym oraz środowiskami nieprodukcyjnymi:

- certyfikacyjnym,
- pilotażowym.

Muszą być one oddzielone od środowiska produkcyjnego. Służą testowaniu współpracy systemów oraz zapewnienia kompatybilności.

Środowisko nieprodukcyjne powinno odzwierciedlać środowisko produkcyjne w zakresie architektury oraz wersji komponentów.

W środowisku nieprodukcyjnym powinny obowiązywać identyczne zasady zarządzania dostępem, jak w środowisku produkcyjnym.

OIRE przewiduje weryfikację i przyłączenie do CSIRE co najwyżej jednego środowiska certyfikacyjnego, jednego środowiska testowego, jednego środowiska pilotażowego oraz jednego środowiska produkcyjnego dla każdego Kontrahenta.

Środowisko certyfikacyjne musi być przygotowane do korzystania ze sztucznie wygenerowanych danych certyfikacyjnych (testowych).

Środowisko pilotażowe musi być przygotowane do korzystania z danych sztucznie wygenerowanych (testowych), zanonimizowanych danych odpowiadających danym produkcyjnym lub danych produkcyjnych.

## 8.6. Wymagania w zakresie rejestracji zdarzeń

Systemy informacyjne współpracujące z CSIRE rejestrują w dziennikach (logach) zdarzenia dotyczące komunikacji w zakresie metadanych (bez treści komunikatów) na potrzeby analizy wymiany informacji.

Zdarzenia muszą być przechowywane przez okres co najmniej dwóch lat.

Dzienniki zdarzeń muszą zawierać co najmniej następujące informacje:

- źródło danych (Message Producer),
- datę zdarzenia,
- użytkownika (właściciela procesu na poziomie systemu operacyjnego),
- znak czasu (Timestamp) ,
- adresy IP: źródłowy (Message Producer) oraz docelowy (CSIRE),
- użyta operacja (SendMessage, PeekMessage, DequeMessage),
- status odpowiedzi serwera (techniczne kody błędów opisane w 5.4.7 i 5.4.8).

# 9. REKOMENDACJE W ZAKRESIE CERTYFIKACJI AS4

W celu ograniczenia ryzyk związanych z integracją systemów Użytkowników profesjonalnych oraz Użytkowników uprawnionych z systemem CSIRE, rekomendujemy wykorzystanie implementacji AS4, które przeszły testy interoperacyjności wykonywane m. in. przez Drummond Group.

Aktualna lista zweryfikowanych rozwiązań znajduje się w: https://www.drummondgroup.com/certified-products-2/b2b-interoperability/#appst

# 10.PRZYSZŁE FUNKCJE I ZMIANY

Zakres, daty wprowadzenia oraz udostępnienia zmian zostaną podane dedykowanymi komunikatami.

Co do zasady przyszłe funkcje i zmiany powinny zachowywać zgodność wstecz (ang. *backward compatibility).*

## 10.1. Rozszerzenie zakresu implementacji Protokołu AS4

Nowe funkcjonalności mają objąć zakres potwierdzeń oraz niezaprzeczalności.

## 10.2. Udostępnianie komunikatów wejściowych poprzez CSIRE

Funkcjonalność ma umożliwiać udostępnienie przez API CSIRE komunikatów wejściowych (np. na podstawie ich UUID) wprowadzonych do OIRE, przez kanał komunikacji inny niż CSIRE AS4 (Portal Użytkownika profesjonalnego).

Zakłada się, iż głównym przypadkiem użycia będzie incydentalny dostęp do danych historycznych.

Funkcjonalność jest przewidywana do udostępnienia w ramach Wydania 3.0 CSIRE.

## 10.3. Wprowadzenie rozszerzenia umożliwiającego alternatywną obsługę wielu wartości OrganisationUser

W celu obsługi wiele ról rynkowych przez jeden system teleinformatyczny współpracujący z CSIRE wymagane jest wskazywanie różnych wartości OrganisationUser w adresie URL CSIRE.

Ponieważ dla niektórych systemów teleinformatycznych współpracujących z CSIRE powyższe rozwiązanie wprowadza perturbacje zostanie opracowana alternatywna metoda obsługi wielu ról rynkowych.

Funkcjonalność jest przewidywana do udostępnienia w ramach Wydania 3.0 CSIRE.

# 11.SPIS TABEL I RYSUNKÓW

Tabela 1. Wykaz definicji ..... 7
Tabela 2. Lista skrótów ..... 9
Tabela 3. Dokumenty powiązane ..... 10
Tabela 4 Przykład pary konfiguracji PMode dla operacji PeekMessage ..... 17
Tabela 5 Parametry PMode dostępne do konfiguracji ..... 18
Tabela 6 Parametry PMode ze stałą wartością bądź nieobsługiwane ..... 20
Tabela 7 Nazwy kolejek wyjściowych CSIRE ..... 36
Tabela 8 Techniczne kody błędów ..... 41
Tabela 9 Techniczne kody błędów AS4 ..... 44
Tabela 10 Kody SOAP Fault ..... 47
Tabela 11 Role rynkowe ..... 57
Tabela 12 Odniesienia ..... 64

Rysunek 1 Struktura wiadomości (User Message Structure, [ebMS3CORE]) ..... 14
Rysunek 2 Struktura wiadomości sygnałowej (Signal Message Structure, [ebMS3CORE]) ..... 15
Rysunek 3 One-Way/Push MEP ..... 25
Rysunek 4 One-Way/Push MEP with Receipt ..... 26
Rysunek 5 Two-Way/Sync MEP ..... 29
Rysunek 6 One-Way/Pull MEP ..... 30
Rysunek 7 Operacja SendMessage ..... 31
Rysunek 8 Operacje PeekMessage i DequeueMessage – prawidłowa sekwencja wywołań ..... 34
Rysunek 9 Pierwsze wywołanie PeekMessage bez DequeueMessage – nieprawidłowa sekwencja wywołań (jeśli nie chcemy ponownie pobrać tej samej wiadomości) ..... 35
Rysunek 10 Diagram sekwencji wywołań systemu CSIRE dla początkowych kroków procesu 8.1. Żądanie wyłączenia dostarczania" dla "poprawnego" przebiegu. ..... 49

# 12. ODNIESIENIA

1339

| Nazwa | Źródło |
|---|---|
| [AS4-Profile] | AS4 Profile of ebMS 3.0 Version 1.0 OASIS Standard 23 January 2013<br>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html |
| [BDX-AS4-v1.0] | AS4 Interoperability Profile for Four-Corner Networks Version 1.0 Committee Specification 01 12 November 2021<br>https://docs.oasis-open.org/bdxr/bdx-as4/v1.0/cs01/bdx-as4-v1.0-cs01.html |
| [ebMS3CORE] | OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features OASIS Standard 1 October 2007<br>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.html |
| [EG-AS4-Profile] | ENTSOG AS4 Profile Version 3.6 – 2018-03-27<br>https://www.entsog.eu/sites/default/files/2019-05/INT0488-161115%20AS4%20Usage%20Profile_Rev_3.6_clean_final.pdf |
| [ISO 15000-1:2021(E)] | ISO 15000-1:2021 Electronic business eXtensible Markup Language (ebXML) Part 1: Messaging service core specification<br>Publication date : 2021-02<br>https://www.iso.org/standard/79108.html |
| [ISO 15000-2:2021(E)] | ISO 15000-2:2021 Electronic business eXtensible Markup Language (ebXML) Part 2: Applicability Statement (AS) profile of ebXML messaging service<br>Publication date : 2021-02<br>https://www.iso.org/standard/79109.html |
| [SOAP12] | SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) W3C Recommendation 27 April 2007<br>https://www.w3.org/TR/soap12/ |
| [SOAPATTACH] | SOAP Messages with Attachments: W3C Note 11 December 2000<br>https://www.w3.org/TR/SOAP-attachments/ |
| [XMLDSIG] | XML-Signature Syntax and Processing (Second Edition). W3C Recommendation. 10 June 2008.<br>http://www.w3.org/TR/xmldsig-core/ |
| [WSS10] | Web Services Security: SOAP Message Security 1.0, 2004<br>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf |
| [WSS11] | Web Services Security: SOAP Message Security 1.1. OASIS Standard incorporating Approved Errata. 1 November 2006<br>http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SOAPMessageSecurity.pdf |

1340 Tabela 12 Odniesienia

1341

# 13.ZAŁĄCZNIKI

## 13.1. Załącznik 1 – WSDL

## 13.2. Załącznik 2 – Parametry PMode CSIRE