

TECHNICZNE STANDARDY SYSTEMÓW INFORMACYJNYCH

Wersja 1.2
(z 12 lipca 2024 r.)

Zatwierdzono:

Obowiązuje od 01.08.2024 r.

Metryka dokumentu:

Nazwa dokumentu	TECHNICZNE STANDARDY SYSTEMÓW INFORMACYJNYCH
Nazwa pliku	OIRE_2024-07-12_TSSI.docx
Wersja dokumentu	1.2
Data opracowania	2024-07-12
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 <i>Wstępnego projektu zmian Załącznika nr 5. do IRIESP-OIRE (wersja z dnia 12 października 2023)</i>	2023-12-20	Projekt OIRE – CGI oraz PSE	PSE S.A.
2.	1.0	Poprawki redakcyjne	2024-05-07	Projekt OIRE – CGI oraz PSE	PSE S.A.
3.	1.0	Dodanie odwołania do norm ISO	2024-05-07	Projekt OIRE – CGI oraz PSE	PSE S.A.
4.	1.0	Aktualizacja wersji IRIESP-OIRE oraz TSKB	2024-05-07	Projekt OIRE – CGI oraz PSE	PSE S.A.
5.	1.0	Aktualizacja algorytmów kryptograficznych	2024-05-07	Projekt OIRE – CGI oraz PSE	PSE S.A.
6.	1.0	Aktualizacja informacji o identyfikacji stron	2024-05-07	Projekt OIRE – CGI oraz PSE	PSE S.A.
7.	1.0	Dodanie wymagania w zakresie rejestracji zdarzeń (komunikaty).	2024-05-07	Projekt OIRE – CGI oraz PSE	PSE S.A.
8.	1.0	Dodanie Załącznika 2 – Parametry PMode CSIRE	2024-05-07	Projekt OIRE – CGI oraz PSE	PSE S.A.
9.	1.1	Poprawki redakcyjne Aktualizacja wersji IRIESP-OIRE oraz TSKB Korekta wartości: PMode[1].ReceptionAwareness.Retry Dodanie nowych kolejek Uspójnienie przykładów wywołań Dodanie przykładu obsługi wielu Kontrahentów Uszczegółowienie zakres logowanych informacji Dodanie rozdziału "Przyszłe funkcje i zmiany"	2024-06-18	Projekt OIRE – CGI oraz PSE	PSE S.A.
10.	1.2	Poprawki redakcyjne Modyfikacja opisów oraz dodanie nowej kolejki	2024-07-12	Projekt OIRE – CGI oraz PSE	PSE S.A.

SPIS TREŚCI

1. WYKAZ DEFINICJI I SKRÓTÓW	5
1.1. Wykaz definicji	5
1.2. Lista skrótów	7
1.3. Dokumenty powiązane	9
2. WSTĘP	10
3. CEL	11
4. ZAKRES	12
4.1. Podmioty	12
4.2. Kompozycja dokumentu	12
4.3. Język	12
5. KOMUNIKACJA	13
5.1. Struktura wiadomości	13
5.2. Podstawowe informacje dotyczące wymiany danych	14
5.2.1. Założenia odnośnie przekazywanych wiadomości biznesowych	15
5.3. Parametry przetwarzania wiadomości	16
5.3.1. Parametry PMode dostępne do konfiguracji dla systemów zewnętrznych	16
5.3.2. Pozostałe PMode (z wartością stałą bądź nieobsługiwane)	19
5.4. Wzorce wymiany komunikatów AS4 (MEP)	24
5.4.1. One-Way/Push MEP	25
5.4.2. Two-Way/Sync MEP	25
5.4.3. Wzorce komunikacji systemu CSIRE	26
5.4.4. Wysłanie wiadomości do CSIRE	26
5.4.5. Pobranie wiadomości z CSIRE	30
5.4.6. Techniczne kody błędów na poziomie warstwy transportowej	36
5.4.7. Techniczne kody błędów AS4	37
5.4.8. Przykład realizacji początkowych kroków procesu SWI z mapowaniem na wywołania interfejsu CSIRE	40
6. BEZPIECZEŃSTWO	42
6.1. Zabezpieczenie komunikacji w warstwie sieci	42
6.2. Zabezpieczenie komunikacji w warstwie transportowej	42
6.3. Zabezpieczenie komunikacji w warstwie komunikatu	43
6.3.1. Podpisywanie wiadomości	43
6.3.2. Szyfrowanie wiadomości	43
6.4. Certyfikaty oraz Infrastruktura Klucza Publicznego (PKI)	44
6.5. Wymiana Certyfikatu	45
7. KOMPRESJA	46
8. IMPLEMENTACJA ROZWIĄZANIA	47
8.1. Wprowadzenie	47
8.2. Identyfikacja stron	47
8.2.1. Identyfikacja i rola rynkowa OIRE	47
8.2.2. Przykład wywołania SendMessage	48
8.3. Dostarczenie wiadomości, powtórzenia, obsługa niedostępności	49
8.4. Wymagania odnośnie środowisk systemów współpracujących z CSIRE	49
8.5. Wymagania w zakresie rejestracji zdarzeń	50
9. REKOMENDACJE W ZAKRESIE CERTYFIKACJI AS4	51
10. PRZYSZŁE FUNKCJE I ZMIANY	52

10.1. Obsługa operacji PeekMessage z wykorzystaniem wzorca One-Way/Pull	52
10.2. Zmiana statusu HTTP z 4xx na 2xx	52
11. SPIS TABEL I RYSUNKÓW	53
12. ODNIESIENIA.....	54
13. ZAŁĄCZNIKI	55
13.1. Załącznik 1 – WSDL.....	55
13.2. Załącznik 2 – Parametry PMode CSIRE.....	55

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	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.

Tabela 1. Wykaz definicji

1.2. Lista skrótów

Skrót	Rozwinięcie
AS4	Protokół AS4 (Application Statement 4)
A2A	<i>Administration-to-Administration</i>
B2A	<i>Business-to-Administration</i>
B2B	<i>Business-to-Business</i>
CSIRE	Centralny System Informacji Rynku Energii
CSWI	Centralny System Wymiany Informacji
DNS	<i>Domain Name System</i>
ENTSOG	<i>European Network of Transmission System Operators for Gas</i>
FIFO	<i>First In First Out</i>
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 uprawnionymi do korzystania z Centralnego systemu informacji rynku energii”
JSON	<i>JavaScript Object Notation</i>
MEP	<i>Message Exchange Patterns</i>
MIME	<i>Multipurpose Internet Mail Extensions</i>
MPC	<i>Message Partition Channels</i>
MSH	<i>Message Service Handler</i>
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	<i>Simple Object Access Protocol</i>
SWI	Standardy Wymiany Informacji
TLS	<i>Transport Layer Security</i>
TSKB	Techniczne Standardy Komunikacji Biznesowej

Skrót	Rozwinięcie
UUID	<i>Universally Unique Identifier</i>
WSS	<i>Web Services Security (WS-Security)</i>
XML	<i>Extensible Markup Language</i>
XSD	<i>XML Schema Definition</i>

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 uprawnionymi do korzystania z Centralnego systemu informacji rynku energii.	IRiESP-OIRE (zatwierdzona 6.04.2023 r., z późn. zm.)	IRiESP-OIRE
2.	Techniczne standardy komunikacji biznesowej.	Techniczne standardy komunikacji biznesowej (wersja z dnia 21 czerwca 2024 r.)	TSKB

Tabela 3. Dokumenty powiązane

1 2. WSTĘP

- 2 Protokół AS4 [AS4-Profile] określa otwarty standard bezpiecznego oraz niezawodnego
3 przesyłania komunikatów poprzez sieć Internet z wykorzystaniem usługi sieciowych.
4 Wykorzystuje powszechnie znane rozwiązania takie, jak SOAP, MIME oraz WS-Security.
5 Zazwyczaj jest stosowany w modelach B2B, B2A oraz A2A.
- 6 Dzięki możliwości przesyłania różnych typów komunikatów takich, jak pliki: binarne, XML lub
7 JSON, zapewnia wysoki poziom elastyczności.
- 8 Powyższe cechy oraz istnienie zarówno komercyjnych, jak i otwartych implementacji protokołu
9 AS4 spowodowały, iż został on przyjęty przez Komisję Europejską do budowy komponentu
10 eDelivery w ramach Digital Europe Programme.
- 11 Ponadto jest on wykorzystywany także przez podmioty skupione w ENTSOG w ramach
12 rozwoju wewnątrzspółnotowego rynku gazu.
- 13 AS4 został przyjęty przez PTPiREE jako standard wymiany komunikatów w projekcie budowy
14 CSWI, a OIRE zaakceptował ten standard dla systemu CSIRE.

15 **3. CEL**

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

20 4. ZAKRES

21 4.1. Podmioty

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

27 4.2. Kompozycja dokumentu

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

31 Bazuje on na "AS4 Profile of ebMS 3.0 Version 1.0 OASIS Standard" [AS4-Profile], który
32 wykorzystuje między innymi standard "OASIS ebXML Messaging Services Version 3.0: Part
33 1, Core Features OASIS Standard" [ebMS3CORE]. Ponadto występują odwołania
34 do dokumentów opracowanych w celu implementacji protokołu AS4 w konkretnych
35 zastosowaniach tj. „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile] oraz "AS4 Interoperability
36 Profile for Four-Corner Networks Version 1.0 Committee Specification 01" [BDX-AS4-v1.0].

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

42 4.3. Język

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

45 **5. KOMUNIKACJA**

46 **5.1. Struktura wiadomości**

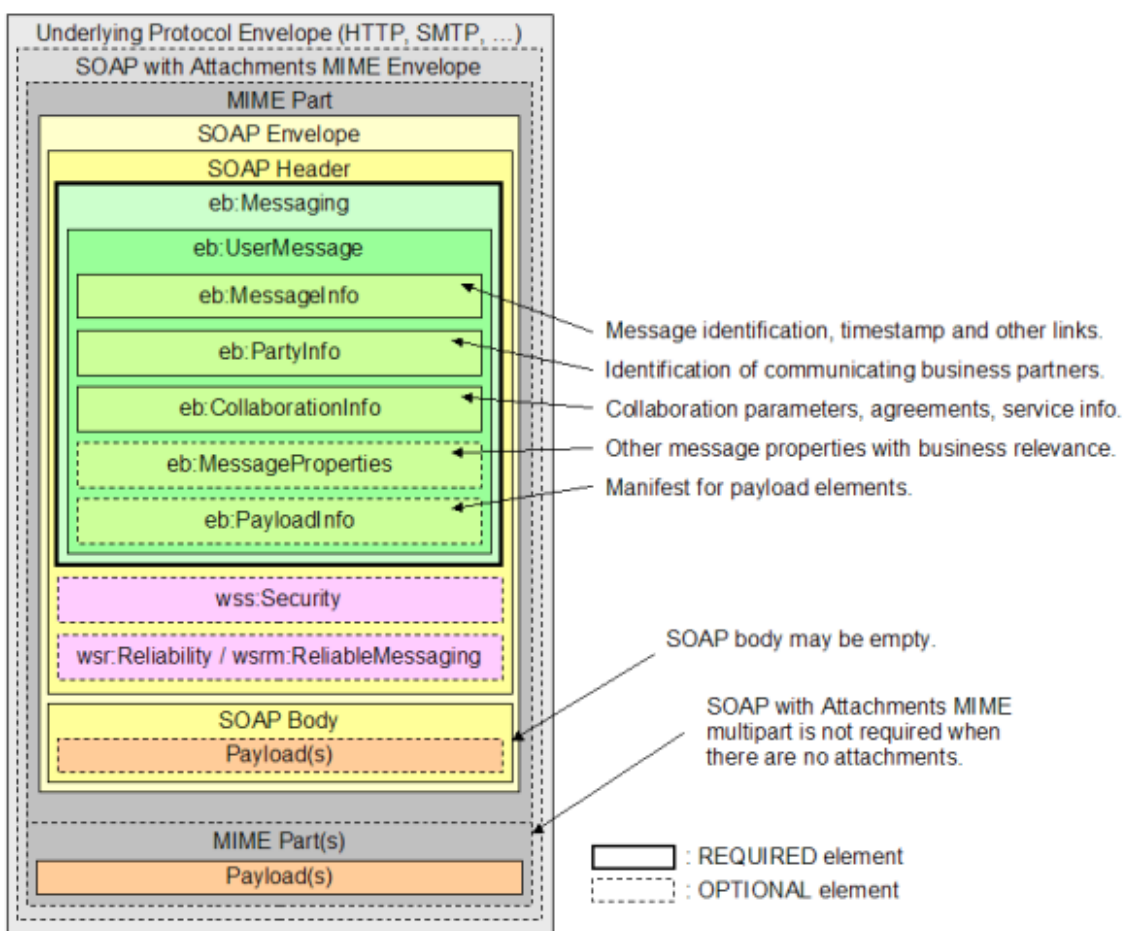
47 Standard wymiany komunikatów na potrzeby wymiany danych z CSIRE bazuje na wymianie
48 komunikatów biznesowych poprzez wiadomości AS4.

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

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

53

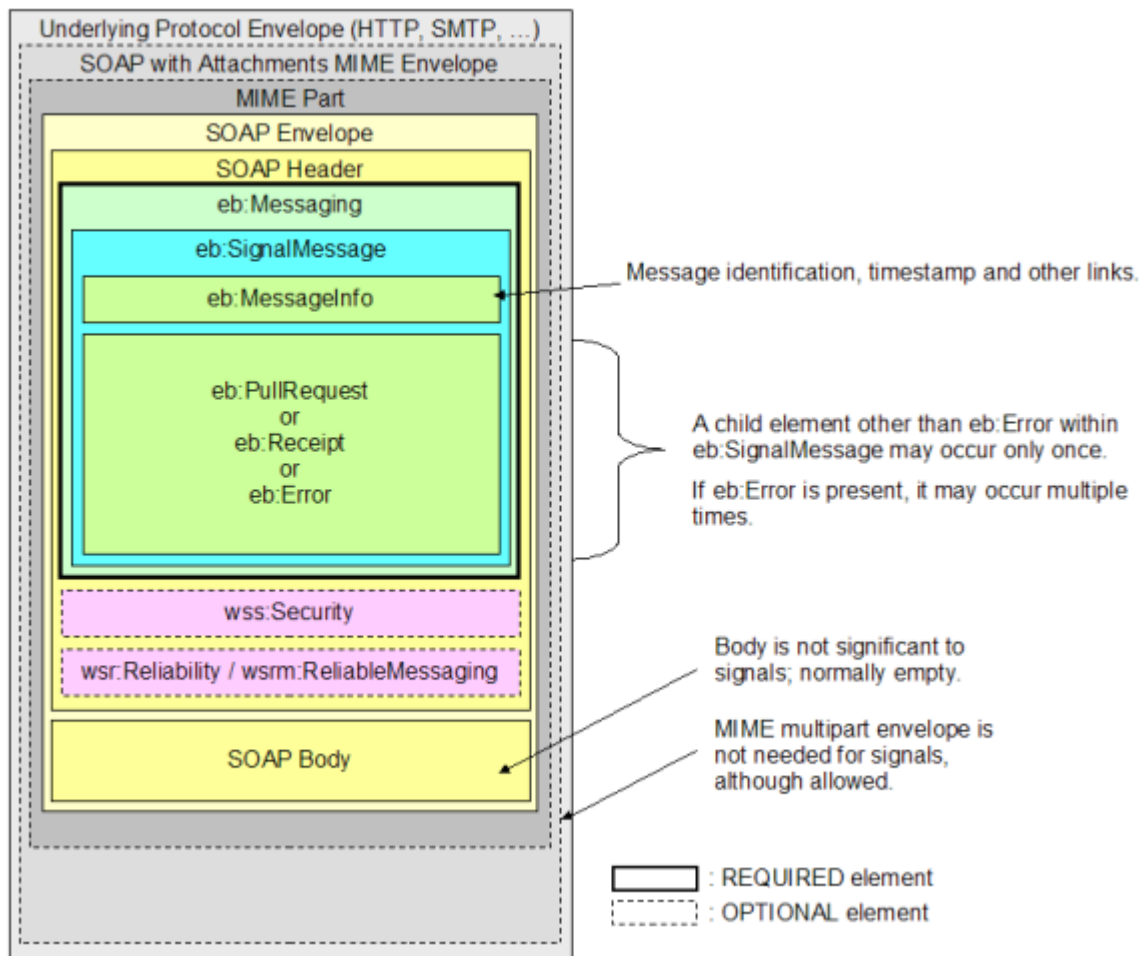
54 Struktura wiadomości biznesowej



55

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

57 Struktura wiadomości sygnałowej



58

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

60

61 5.2. Podstawowe informacje dotyczące wymiany danych

62

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

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

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

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

76

77 Podstawowe założenia komunikacji z CSIRE:

- 78 • Wysyłanie wiadomości do systemu CSIRE odbywać się będzie poprzez
79 wywołanie udostępnionej usługi (operacja SendMessage, patrz 5.4.4)
80 odpowiadającej za przyjęcie i zarejestrowanie transakcji.
- 81 • Wiadomości wychodzące z CSIRE zostaną udostępnione do pobrania i to w
82 gestii systemów zewnętrznych będzie pobranie ich z systemu CSIRE (za pomocą
83 operacji PeekMessage patrz 5.4.5) i potwierdzenie ich poprawnego odebrania
84 (za pomocą operacji DequeueMessage).
- 85 • Wywołanie operacji DequeueMessage zapewnia niezaprzeczalność
86 dostarczenia wiadomości do systemu zewnętrznego (nie da się poprawnie
87 wywołać operacji DequeueMessage bez poprawnego odczytania rezultatu
88 operacji PeekMessage)
89

90 Dla systemów zewnętrznych komunikujących się z CSIRE oznacza to:

- 91 • Aktywna komunikacja z systemów zewnętrznych dla wiadomości wychodzących
92 z CSIRE – konieczność cyklicznego odpytywania CSIRE poprzez wywołanie
93 operacji PeekMessage.
- 94 • Systemy zewnętrzne zarządzają szybkością pobierania i przetwarzania
95 wiadomości.
- 96 • Systemy zewnętrzne zarządzają kolejnością przetwarzania wiadomości (CSIRE
97 wymusza pobranie w kolejności).
- 98 • WSDL opisujący Webservice zawierający operacje SendMessage,
99 PeekMessage oraz DequeueMessage znajduje się w Załączniku 1 – WSDL.

100

101

102

103 5.2.1. Założenia odnośnie przekazywanych wiadomości biznesowych

- 104 • Wiadomości biznesowe przekazywane w elemencie payload wiadomości AS4
105 UserMessage (niezależnie czy payload jest częścią wiadomości czy
106 załącznikiem) powinny być poprawnymi komunikatami XML zgodnymi z WSDL
107 z Załącznika 1 – WSDL oraz ze schematami XSD udostępnionymi w ramach
108 TSKB.
- 109 • Schematy XSD są zgodne ze specyfikacją XML Schema 1.0.
- 110 • W ramach pojedynczego wysłania lub odebrania wiadomości z/do CSIRE
111 przekazana może być jedna wiadomość biznesowa zgodna z XSD.
- 112 • Grupowanie (paczkowanie) np. dla profili dobowych zostanie uwzględnione
113 w ramach schematów XSD (czyli np. jedna wiadomość, zgodna z XSD, będzie
114 zawierać wiele profili dobowych).
- 115 • Wiadomości biznesowe mogą być przekazywane do CSIRE jako payload będący
116 częścią wiadomości AS4 lub jako załącznik. W przypadku użycia kompresji
117 payload musi być przekazany jako załącznik.
- 118 • CSIRE będzie udostępniać wiadomości w payload będącym częścią wiadomości
119 AS4 z wyjątkiem sytuacji, gdy włączone zostanie użycie kompresji - wtedy
120 wiadomości będą przekazywane w załączniku.
- 121 • W przypadku przekazania wiadomości jako załącznik powinien on zawierać
122 pełną strukturę wywołania dla danej operacji SendMessage, PeekMessage lub
123 DequeueMessage. Przykład dla operacji SendMessage można zobaczyć
124 w rozdziale 5.4.4.2.2.

125

126

127

128

129 **5.3. Parametry przetwarzania wiadomości**

130 Każda wiadomość przekazana do systemu CSIRE musi zawierać w nagłówku sekcje
 131 CollaborationInfo zawierającą min. elementy AgreementRef, Service, Action (przykład
 132 wywołania z rozdziału 5.4.4.2.1). Elementy te służą do wskazania, który zestaw parametrów
 133 PMode z konfiguracji systemu CSIRE należy użyć do procesowania wiadomości. Sposób
 134 mapowania tych elementów na parametry PMode w systemie:

- 135 AgreementRef - PMode.Agreement
- 136 Service - PMode[1].BusinessInfo.Service
- 137 Action - PMode[1].BusinessInfo.Action

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

141 Dla operacji PeekMessage w systemie CSIRE może zostać utworzona para konfiguracji
 142 PMode z takimi samymi wartościami PMode.Agreement oraz PMode[1].BusinessInfo.Service
 143 i różnym PMode[1].BusinessInfo.Action:

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

148 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

149

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

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

155

156 **5.3.1. Parametry PMode dostępne do konfiguracji dla systemów zewnętrznych**

157

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

161

162 Tabela 5 Parametry PMode dostępne do konfiguracji

PMode	Wymagania	Opis	Wartość
PMode.ID	Obowiązkowy	Identyfikuje zestaw parametrów PMode.	Wygenerowany identyfikator UUID

PMode	Wymaga Iność	Opis	Wartość
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.
PMode.Initiator.Party	Obowiązkowy	Kwalifikuje stronę inicjującą MEP.	Stała wartość: Identyfikator Organizacji.
PMode.Initiator.Role	Obowiązkowy	Producent wiadomości pełni rolę inicjatora, czyli rolę strony wysyłającej pierwszą wiadomość wzorca MEP.	Stała wartość: Rola Organizacji na rynku.
PMode.Responder.Party	Obowiązkowy	Kwalifikuje stronę odbierającą MEP.	Stała wartość: Identyfikator Organizacji dla roli OIRE.
PMode.Responder.Role	Obowiązkowy	Rola odbiorcy wiadomości.	Stała wartość: Rola Organizacji na rynku (OIRE).
PMode.MEP	Obowiązkowy	Wzorzec wymiany komunikatów (musi to być identyfikator URI), zob. także 5.4: 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 . 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: • One-Way/Push: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay • Two-Way/Sync: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/twoWay

PMode	Wymagania	Opis	Wartość
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: <ul style="list-style-type: none"> One-Way/Push: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push Two-Way/Sync: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/sync
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. Jego zawartość musi być odwzorowana na element <code>eb:Messaging/eb:UserMessage/eb:CollaborationInfo/eb:Service</code> .	Stała wartość: MarketMessaging
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. Jego zawartość powinna być odwzorowana na element <code>eb:Messaging/eb:UserMessage/eb:CollaborationInfo/eb:Action</code> .	Możliwe wartości zależą od wzorca MEP: <p>One-Way/Push:</p> <ul style="list-style-type: none"> SendMessage DequeueMessage <p>Two-Way/Sync:</p> <ul style="list-style-type: none"> PeekMessage.request PeekMessage.reply
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

PMode	Wymaga Iność	Opis	Wartość
PMode[1].Security.X509.Sign	Obowiązkowy	Wartość logiczna wskazująca, czy wiadomości powinny być podpisywane.	Yes/No
PMode[1].Security.X509.Encryption.Encrypt	Obowiązkowy	<p>Parametr wskazujący (jeśli jest prawdziwy), że MSH zaszyfruje:</p> <ul style="list-style-type: none"> Wszystkie części payloadu: Każda treść SOAP również zostanie zaszyfrowana. Załączniki. <p>MSH nie zaszyfruje nagłówka. Jeśli wymagana jest poufność danych w nagłówku, można to osiągnąć poprzez zabezpieczenie na poziomie transportu.</p>	Yes/No

163

164 **5.3.2. Pozostałe PMode (z wartością stałą bądź nieobsługiwane)**

165

166 Tabela 6 Parametry PMode ze stałą wartością bądź nieobsługiwane

PMode	Opis	Wartość w CSIRE
PMode[1].Protocol.SOAPVersion	Wersja SOAP, która ma być używana (1.1 lub 1.2).	Stała wartość 1.2
PMode[1].Security.WSSVersion	Wartość reprezentuje wersję WS-Security, która ma być używana, i ma dwie możliwe wartości: 1.0 1.1	Stała wartość 1.1
PMode[1].Security.X509.Encryption.Certificate	Certyfikat publiczny do odszyfrowywania otrzymanych wiadomości.	Zarządzanie certyfikatami odbywa się z użyciem Portalu Użytkownika profesjonalnego.
PMode[1].Security.X509.Signature.Certificate	Certyfikat publiczny do weryfikacji otrzymanych podpisanych wiadomości.	Zarządzanie certyfikatami odbywa się z użyciem Portalu Użytkownika profesjonalnego.
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-xmlsig-core-20080610/]	http://www.w3.org/2001/04/xmlenc#sha256

PMode	Opis	Wartość w CSIRE
PMode[1].Security.X509.Signature.Algorithm	Identyfikuje algorytm obliczania wartości podpisu cyfrowego.	<ul style="list-style-type: none"> - (domyślnie) RSA-SHA256 (http://www.w3.org/2001/04/xmlnsig-more#rsa-sha256) - RSA-SHA384 (http://www.w3.org/2001/04/xmlnsig-more#rsa-sha384) - RSA-SHA512 (http://www.w3.org/2001/04/xmlnsig-more#rsa-sha512)
PMode[1].Security.X509.Encryption.Algorithm	Algorytm szyfrowania, który ma być używany.	Patrz 6.3.2
PMode[1].Security.X509.Encryption.MinimumStrength	Wartość całkowita określająca efektywną siłę, którą algorytm szyfrowania musi zapewnić w postaci efektywnych lub losowych bitów. Wartość jest mniejsza niż długość klucza w bitach, gdy w kluczu używane są bity kontrolne. Np. 8 bitów kontrolnych 64-bitowego klucza DES nie zostanie uwzględnionych w zliczaniu. Ustawienie MinimumStrength na 56 jest wymagane, aby mieć minimalną siłę równą tej dostarczanej przez DES.	Stała wartość 128
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.
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.
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.
PMode.Initiator.Authorization.password		
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.
PMode.Responder.Authorization.password		

PMode	Opis	Wartość w CSIRE
PMode[1].Protocol.Address	Reprezentuje adres (adres URL punktu końcowego) odbiornika MSH (lub strony odbiorcy), do którego mają być wysyłane komunikaty.	Nie używany. Organizacje zawsze inicjują komunikację z CSIRE, dlatego konfiguracja adresu URL, na który organizacje mają otrzymywać wiadomości, nie jest wymagana.
PMode[1].BusinessInfo.PayloadProfile.maxSize	Ten parametr pozwala na określenie maksymalnego rozmiaru w kilobajtach dla całego payloadu, czyli dla sumy wszystkich części ładunku.	Nie używany. Dla wszystkich wiadomości wymienianych z CSIRE stosowana jest stała wartość maksymalna wynosząca 100 MB.
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.	Nie używany.
PMode[1].BusinessInfo.PayloadProfile[]	Ten parametr pozwala na określenie ograniczenia lub profilu dla payloadu.	Nie używany.
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.	Nie używany.

PMode	Opis	Wartość w CSIRE
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.	Nie używany.
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.	Nie używany
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.	Nie używany.
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.	Nie używany.
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.	Nie używany.
PMode[1].Protocol.Address	Adres URL punktu końcowego odbiornika MSH (lub strony odbiorcy), do którego mają być wysyłane komunikaty w części PMode.	Nie używany.
PMode[1].ReceptionAwareness	Parametr logiczny wskazujący (jeśli prawda), że należy podjąć kroki w celu zapewnienia odbioru wiadomości.	Nie używany.

PMode	Opis	Wartość w CSIRE
PMode[1].ReceptionAwareness.Retry.Parameters	Parametr określający wymagania dotyczące ponownych prób wywołania.	Nie używany.
PMode[1].ReceptionAwareness.DuplicateDetection	Wykrywanie zduplikowanych wiadomości jest zawsze włączone w CSIRE i nie można nim sterować za pomocą parametrów.	Nie używany.
PMode[1].ReceptionAwareness.DuplicateDetection.Parameters	Wykrywanie zduplikowanych wiadomości jest zawsze włączone w CSIRE i nie można nim sterować za pomocą parametrów.	Nie używany.
PMode[1].Security.PModeAuthorize	<p>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 .</p> <p>PMode.Initiator.Authorization, jeśli wiadomość jest wysyłana przez Initiator .</p> <p>np. po ustawieniu na true dla komunikatu PushRequest wysłanego przez inicjatora, push będzie autoryzowany tylko przez MPC wskazany przez ten sygnał Push , jeśli:</p> <p>MPC jest taki sam , jak określono w nodze PMode dla przesyłanej wiadomości; I</p> <p>sygnał zawiera ważne dane uwierzytelniające (tj. nazwę użytkownika/hasło).</p>	Nie używany.
PMode[1].Security.SendReceipt	Parametr logiczny wskazujący (jeśli true), że podpisana wiadomość Receipt zawierająca skrót wiadomości musi zostać odesłany.	Nie używany.

PMode	Opis	Wartość w CSIRE
PMode[1].Security.SendReceipt.NonRepudiation	Parametr logiczny wskazujący (jeśli true), że wymagana jest niezaprzeczalność odbioru . W przeciwnym razie (jeśli false) wymagana jest tylko świadomość odbioru. Niezaprzeczalność uniemożliwia odbiorcy zaprzeczenie odbioru wiadomości. Potwierdzenia niezaprzeczalności muszą być wysyłane synchronicznie dla każdego typu wiadomości.	Nie używany.
PMode[1].Security.SendReceipt.ReplyPattern	Wskazuje, czy ma zostać wysłany sygnał odbioru: jako wywołanie zwrotne na oddzielnym połączeniu. (wartość " wywołanie zwrotne "); Lub synchronicznie w odpowiedzi HTTP lub kanale zwrotnym (wartość „ response ”). Jeśli nie ma go w PMode, można użyć dowolnego wzorca.	Nie używany.
PMode[1].Security.UserNameToken.userName	Nazwa użytkownika do uwzględnienia w tokenie nazwy użytkownika WSS .	Nie używany.
PMode[1].Security.UserNameToken.password	Hasło do użycia wewnątrz tokena nazwy użytkownika WSS.	Nie używany.
PMode[1].Security.UserNameToken.Digest	Wskazuje, czy skrót hasła zostanie uwzględniony w elemencie WSS UsernameToken.	Nie używany.
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.	Nie używany.
PMode[1].Security.UserNameToken.Created	Wskazuje, czy element WSS UsernameToken będzie miał utworzony element sygnatury czasowej.	Nie używany.

167

168

169 5.4. Wzorce wymiany komunikatów AS4 (MEP)

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

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

175 Poniżej przedstawione zostaną poszczególne wzorce wymiany wiadomości.

176

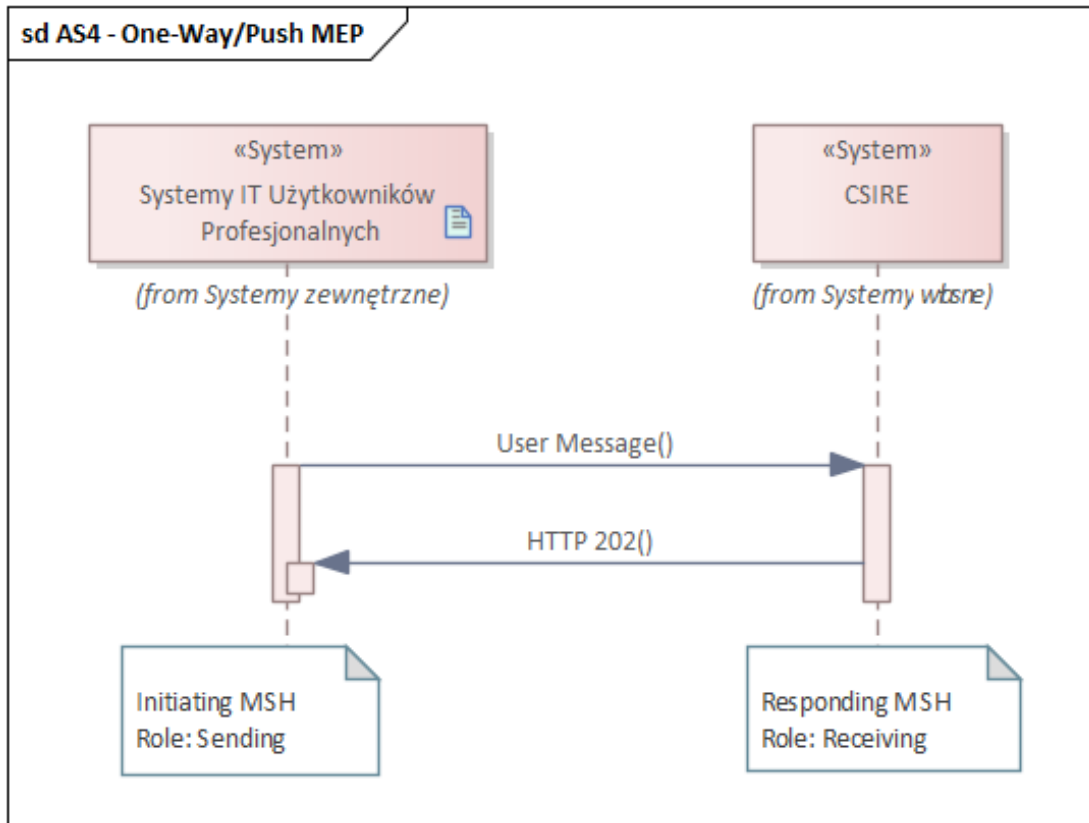
177 5.4.1. One-Way/Push MEP

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

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

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

184 Wzorzec ten obrazuje następujący diagram:



185

186 Rysunek 3 One-Way/Push MEP

187

188 5.4.2. Two-Way/Sync MEP

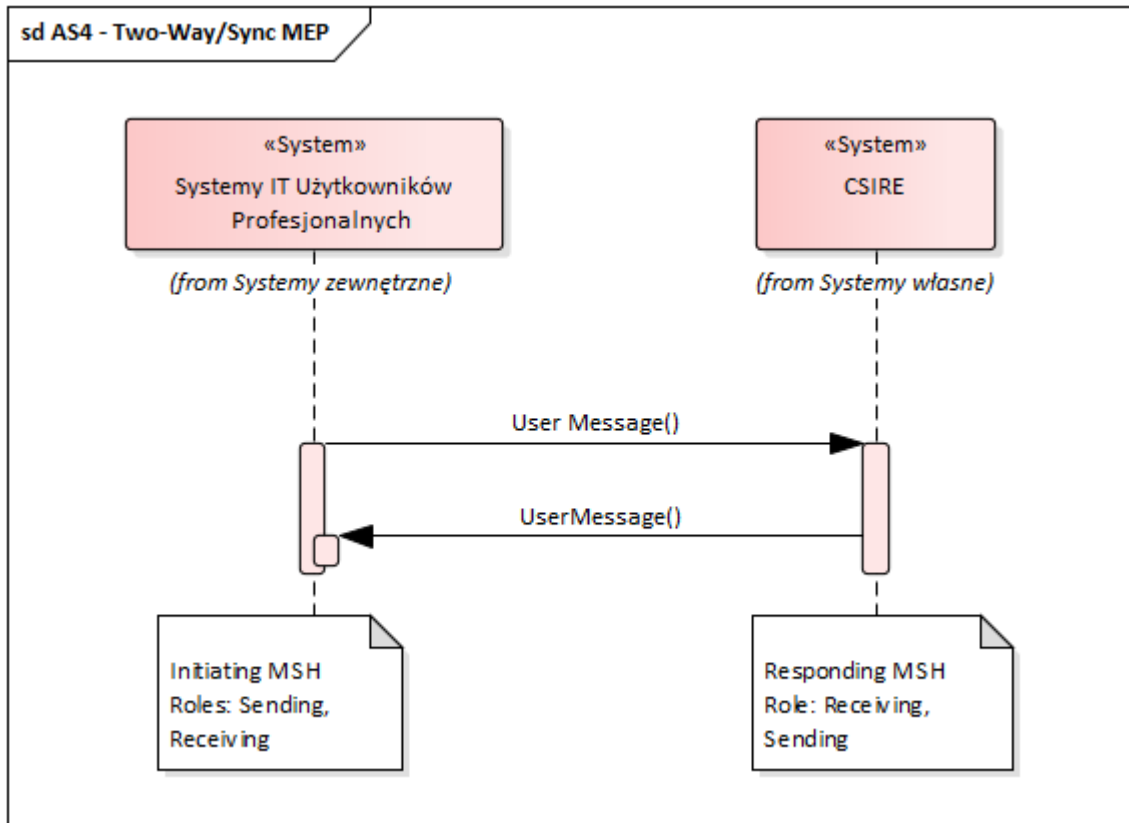
189 Opis wzorca komunikacji można przedstawić za pomocą sekwencji następujących po sobie
 190 zdarzeń.

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

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

195

196 Wzorec ten obrazuje następujący diagram:



197

198 Rysunek 4 Two-Way/Sync MEP

199 5.4.3. Wzorce komunikacji systemu CSIRE

200 W następnym rozdziale przedstawiono sposób komunikacji z systemem CSIRE przy
201 wykorzystaniu mechanizmów AS4.

202 Dla przedstawionych operacji opisane są jedynie techniczne kody błędów tzn. takie które
203 wynikają wprost z implementacji warstwy transportowej lub warstwy AS4. Dokument nie
204 opisuje biznesowych kodów błędów pochodzących z TSKB – wiadomości zawierające takie
205 kody biznesowe będą pobierane z użyciem operacji PeekMessage opisanej w rozdziałach
206 5.4.5.2. i 5.4.5.3. (analogicznie jak wszystkie inne wiadomości opisane w TSKB).

207

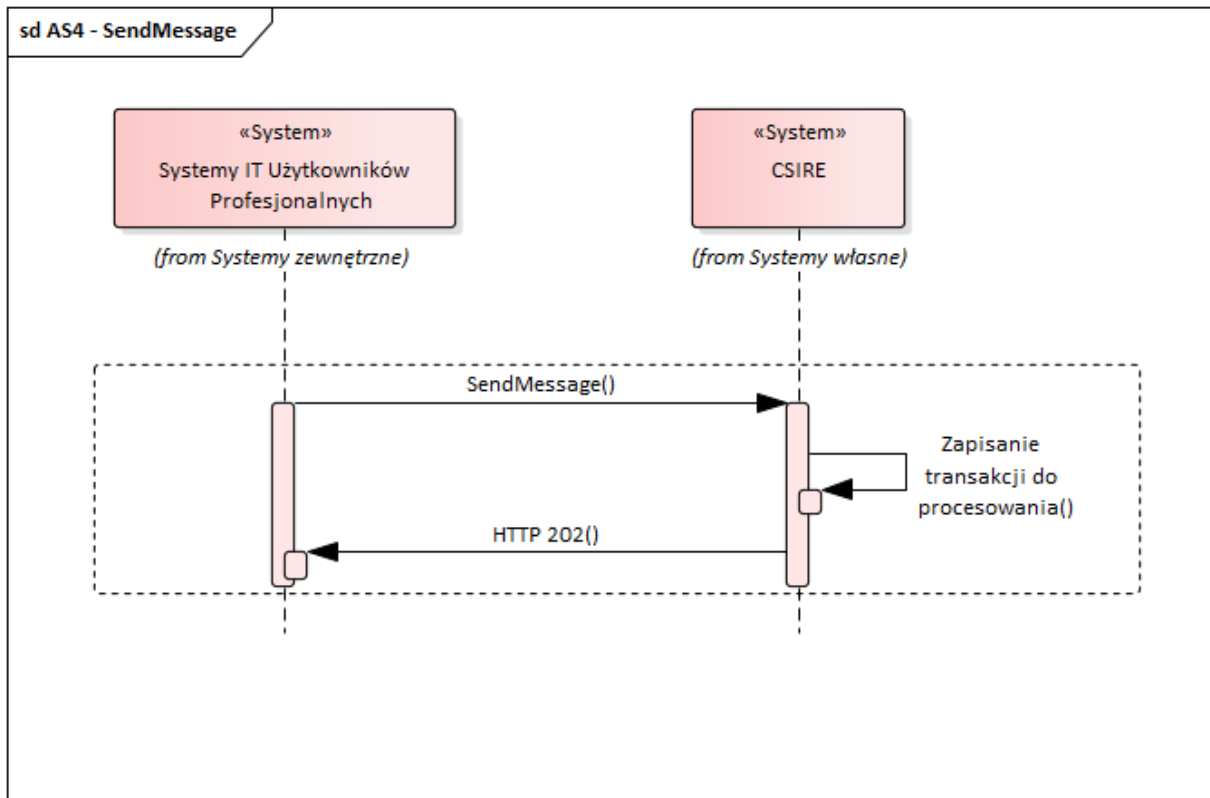
208 5.4.4. Wysłanie wiadomości do CSIRE

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

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

214

215



216

217 Rysunek 5 Operacja SendMessage

218 5.4.4.1. Operacja SendMessage

219

- 220 - Jako wywołanie jest przesyłana wiadomość UserMessage (AS4) zawierająca payload
- 221 zgodny z XSD (patrz 5.4.4.2).
- 222 - W przypadku przyjęcia wiadomości do procesowania zwracany jest kod HTTP 202,
- 223 a wiadomość zapisywana jest w systemie do dalszego procesowania.
- 224 Notyfikacje dotyczące przetwarzania (zgodne ze specyfikacją wiadomości opisaną
- 225 w TSKB) zostaną wygenerowane przez CSIRE i będą pobierane z użyciem operacji
- 226 PeekMessage, opisaney w rozdziałach 5.4.5.2. i 5.4.5.3.
- 227 - W przypadku błędu przyjęcia wiadomości do procesowania zwracany jest komunikat
- 228 zgodny z opisem w punktach 5.4.6 oraz 5.4.7
- 229

230 5.4.4.2. Struktura wiadomości dla SendMessage

231 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

Element	Kardynalność	Typ	Opis
			komunikatów z TSKB i zgodnym ze specyfikacją XML Schema 1.0.

232

233

5.4.4.2.1. Przykład wywołania SendMessage

234

```

235 <soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
236 xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
237   <soapenv:Header>
238     <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
239     soapenv:mustUnderstand="1">
240       <eb:UserMessage>
241         <eb:MessageInfo>
242           <eb:Timestamp>2023-08-03T07:36:20.656Z</eb:Timestamp>
243           <eb:MessageId>d7c3eccf-0781-4789-a456-035b39e8bb20</eb:MessageId>
244         </eb:MessageInfo>
245         <eb:PartyInfo>
246           <eb:From>
247             <eb:PartyId>ExampleParty1</eb:PartyId>
248             <eb:Role>ExampleParty1Role</eb:Role>
249           </eb:From>
250           <eb:To>
251             <eb:PartyId>ExampleParty2</eb:PartyId>
252             <eb:Role>ExampleParty2Role</eb:Role>
253           </eb:To>
254         </eb:PartyInfo>
255         <eb:CollaborationInfo>
256           <eb:AgreementRef>SendMessageAgreementExample</eb:AgreementRef>
257           <eb:Service>MarketMessaging</eb:Service>
258           <eb:Action>SendMessage</eb:Action>
259           <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
260         </eb:CollaborationInfo>
261       </eb:UserMessage>
262     </eb:Messaging>
263   </soapenv:Header>
264   <soapenv:Body>
265     <urn:SendMessageRequest>
266       <urn:MessageContainer>
267         <urn:Payload>
268           ...
269         </urn:Payload>
270       </urn:MessageContainer>
271     </urn:SendMessageRequest>
272   </soapenv:Body>
273 </soapenv:Envelope>

```

274

5.4.4.2.2. Przykład wywołania SendMessage ze skompresowanym załącznikiem

275

Wywołanie na poziomie HTTP pokazujące sposób przekazania załącznika:

276

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

277

```

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

```

290

```

291 <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
292   xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
293   1.0.xsd"
294   xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
295   1.0.xsd"
296   xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
297   <soap:Header>

```

```

298 <eb:Messaging soap:mustUnderstand="true">
299   <eb:UserMessage>
300     <eb:MessageInfo>
301       <eb:Timestamp>2023-11-16T07:56:03</eb:Timestamp>
302       <eb:MessageId>31ad9125-2023-4293-af39-6c891a724c13</eb:MessageId>
303     </eb:MessageInfo>
304     <eb:PartyInfo>
305       <eb:From>
306         <eb:PartyId>ExampleParty1</eb:PartyId>
307         <eb:Role> ExampleParty1Role</eb:Role>
308       </eb:From>
309       <eb:To>
310         <eb:PartyId>ExampleParty2
311         </eb:PartyId>
312         <eb:Role>ExampleParty2Role</eb:Role>
313       </eb:To>
314     </eb:PartyInfo>
315     <eb:CollaborationInfo>
316       <eb:AgreementRef> SendMessageAgreementExample</eb:AgreementRef>
317       <eb:Service>MarketMessaging</eb:Service>
318       <eb:Action>SendMessage</eb:Action>
319       <eb:ConversationId>2011-921</eb:ConversationId>
320     </eb:CollaborationInfo>
321     <eb:PayloadInfo>
322       <eb:PartInfo href="cid:payload1_att.xml.gz">
323         <eb:PartProperties>
324           <eb:Property name="MimeType">application/xml</eb:Property>
325           <eb:Property name="CharacterSet">utf-8</eb:Property>
326           <eb:Property name="CompressionType">application/gzip</eb:Property>
327         </eb:PartProperties>
328       </eb:PartInfo>
329     </eb:PayloadInfo>
330   </eb:UserMessage>
331 </eb:Messaging>
332 </soap:Header>
333 <soap:Body/>
334 </soap:Envelope>
335 -----_Part_9_1507953070.1700139714536
336 Content-Type: application/gzip; name=payload1_att.xml.gz
337 Content-Transfer-Encoding: binary
338 Content-ID: <payload1_att.xml.gz>
339 Content-Disposition: attachment; name="payload1_att.xml.gz"; filename="payload1_att.xml.gz"
340 --- BINARY COMPRESSED ATTACHMENT
341

```

342 Zdekompresowany, ze względu na czytelność, załącznik:

```

343   <urn:SendMessageRequest xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:pl:oire:unk_2_1_1_1"
344   xmlns:urn2="urn:pl:oire:technical">
345     <urn:MessageContainer>
346       <urn:Payload>
347         ...
348       </urn:Payload>
349     </urn:MessageContainer>
350   </urn:SendMessageRequest>
351
352
353

```

354 5.4.4.2.3. Przykład odpowiedzi w przypadku błędu EBMS:0001

```

355 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
356   xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
357   <soapenv:Header>
358     <eb:Messaging soapenv:mustUnderstand="1">
359       <eb:SignalMessage>
360         <eb:MessageInfo>
361           <eb:Timestamp>2023-08-03T07:21:17.993Z</eb:Timestamp>
362           <eb:MessageId>d7c3eccc-0781-4789-a456-035b39e8bb20</eb:MessageId>
363         </eb:MessageInfo>
364         <eb:Error origin="ebMS"
365           category="Content"
366           errorCode="EBMS:0001"
367           severity="failure"
368           refToMessageInError="d7c3eccc-0781-4789-a456-375b39e8bccf">
369           <eb:Description>Value not recognized</eb:Description>
370         </eb:Error>
371

```

```

372     </eb:SignalMessage>
373     </eb:Messaging>
374     </soapenv:Header>
375     <soapenv:Body/>
376 </soapenv:Envelope>

```

377 5.4.5. Pobranie wiadomości z CSIRE

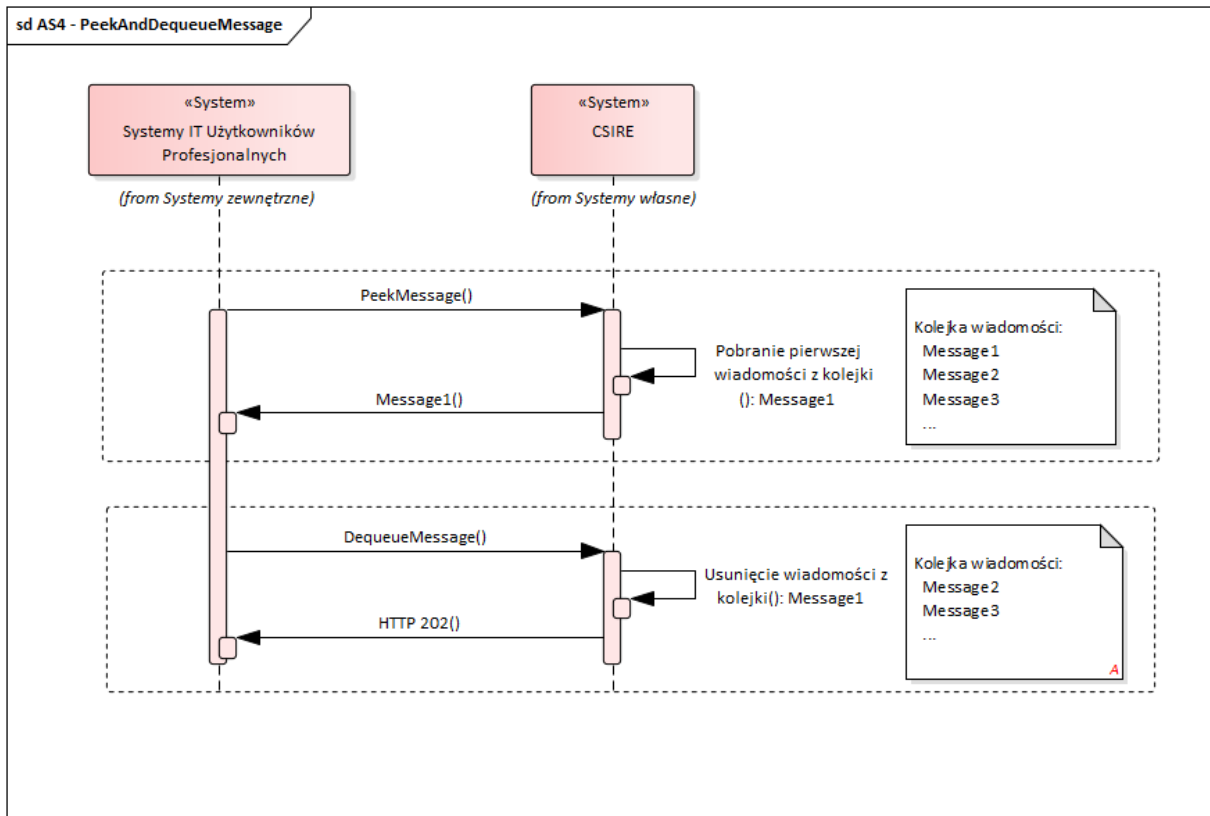
378 W celu zapewnienia niezaprzeczalności odebranie wiadomości z CSIRE zostało podzielone
 379 na dwie techniczne operacje:

- 380 • PeekMessage – zrealizowaną wg. wzorca Two-Way Sync,
- 381 • DequeueMessage - zrealizowaną wg. wzorca One-Way Push.

382

383

384



385

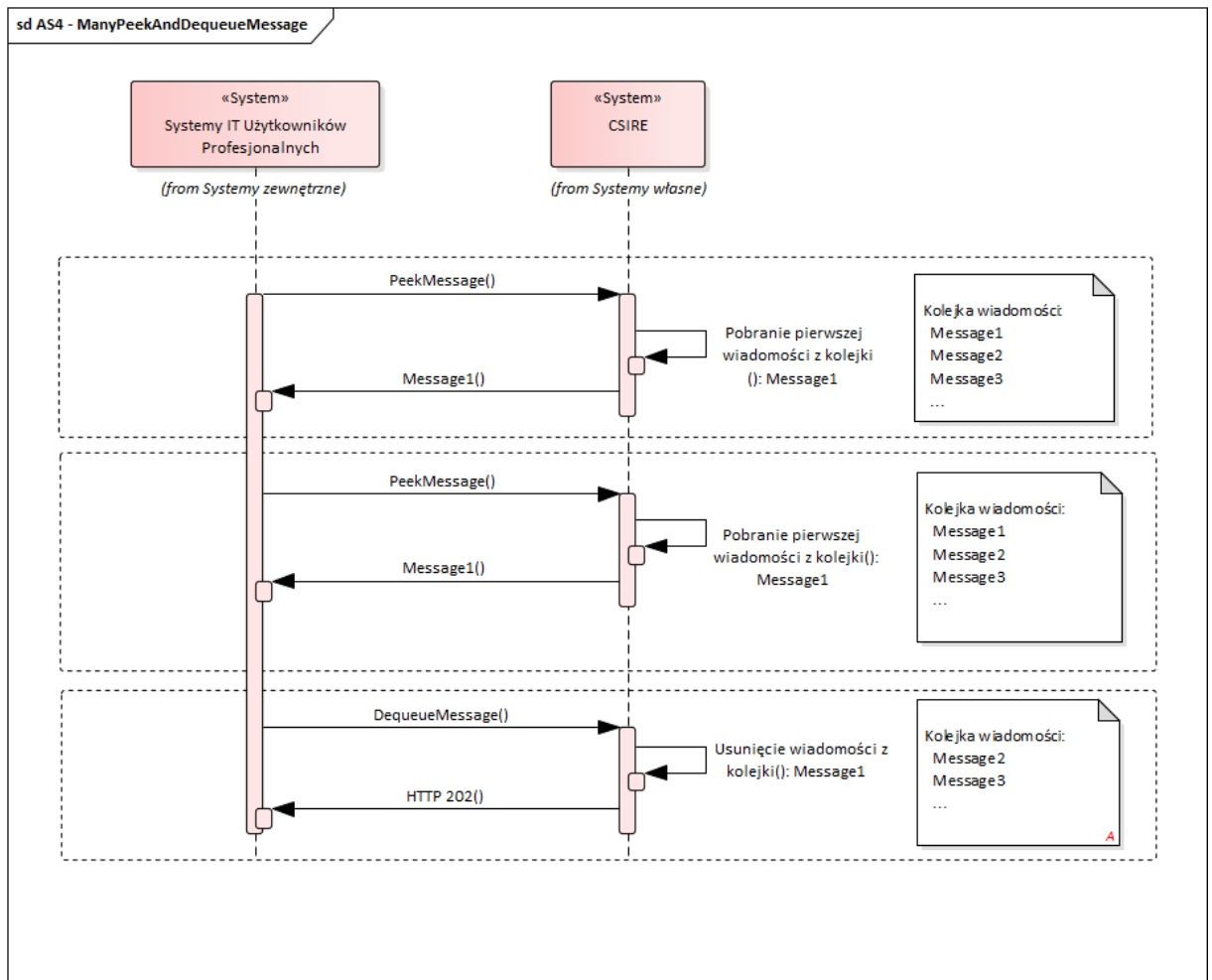
386 Rysunek 6 Operacje PeekMessage i DequeueMessage – prawidłowa sekwencja wywołań

387

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

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

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



400

401 Rysunek 7 Pierwsze wywołanie PeekMessage bez DequeueMessage – nieprawidłowa sekwencja wywołań (jeśli
 402 nie chcemy ponownie pobrać tej samej wiadomości)

403

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

407

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

410

- W przypadku pobrania wiadomości z użyciem PeekMessage i technicznego potwierdzenia z użyciem DequeueMessage kolejne wywołanie PeekMessage powinno nastąpić niezwłocznie po wywołaniu DequeueMessage.

411

412

413

414

415

- W przypadku wywołania PeekMessage, dla którego CSIRE nie zwróciło wiadomości kolejne wywołanie PeekMessage powinno nastąpić po 15 sekundach.

416

417 **5.4.5.1. Kolejki wyjściowe z CSIRE**

- 418 - Operacja PeekMessage (opisana w 5.4.5.2) umożliwia podanie nazwy kolejki
 419 (w elemencie MessageDomain), z której chcemy pobrać wiadomość.
 420 - Jeśli w wywołaniu operacji PeekMessage podamy wiele nazw kolejek (wiele
 421 elementów MessageDomain) system CSIRE zwróci jedną, najstarszą wiadomość
 422 z kolejek przekazanych w wywołaniu.
 423 - Jeśli w wywołaniu operacji PeekMessage nie podamy nazwy kolejki, system CSIRE
 424 zwróci jedną, najstarszą wiadomość ze wszystkich kolejek.
 425 - Zdefiniowanie wielu kolejek wyjściowych umożliwia systemom zewnętrznym
 426 równoległe pobieranie z nich wiadomości.
 427

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 przerywania realizacji procesów (macierz priorytetyzacji, timery oraz manualne)
SOFTVALIDATIONS	Wiadomości dotyczące „wyników walidacji miękkich” (pozostałe typu S)

428 Tabela 7 Nazwy kolejek wyjściowych CSIRE

429
430

431 **5.4.5.2. Operacja PeekMessage**

- 432 - Zrealizowana wg. wzorca Two-Way Sync
 433 - Wywołanie odpowiada wiadomości typu UserMessage (AS4) zawierającej payload
 434 zgodny z XSD (patrz 5.4.5.3)
 435 - System zewnętrzny może w ramach wiadomości UserMessage wysłać informacje,
 436 z jakiej kolejki systemu CSIRE chce pobrać wiadomość (element Message
 437 Domain).
 438 - Poprawne wywołanie skutkuje zwróceniem wiadomości typu UserMessage (AS4)
 439 zawierającej payload zgodny z XSD (patrz 5.4.5.3).
 440 - Niepoprawne wywołanie skutkuje błędem zgodnym z punktami 5.4.6 oraz 5.4.7.
 441

442 **5.4.5.3. Struktura wiadomości dla PeekMessage**

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

Element	Kardynalność	Typ	Opis
PeekMessageRequest	1..1	Complex Element	Główny element reprezentujący wywołanie PeekMessage

Element	Kardynalność	Typ	Opis
MessageDomains	0..1	Complex Element	Opcjonalny element zawierający listę 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

444

445 Struktura wiadomości UserMessage (AS4) przekazywanej z CSIRE jako odpowiedź na
446 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.

447

448 5.4.5.3.1. Przykład wywołania PeekMessage

```

449 <soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
450 xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
451   <soapenv:Header>
452     <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
453     soapenv:mustUnderstand="1">
454       <eb:UserMessage>
455         <eb:MessageInfo>
456           <eb:Timestamp>2023-08-03T07:36:20.656Z</eb:Timestamp>
457           <eb:MessageId>d7c3eccf-0781-4789-a456-035b39e8bb20</eb:MessageId>
458         </eb:MessageInfo>
459         <eb:PartyInfo>
460           <eb:From>
461             <eb:PartyId>ExampleParty1</eb:PartyId>
462             <eb:Role>ExampleParty1Role</eb:Role>
463           </eb:From>
464           <eb:To>
465             <eb:PartyId>ExampleParty2</eb:PartyId>
466             <eb:Role>ExampleParty2Role</eb:Role>

```

```

467         </eb:To>
468     </eb:PartyInfo>
469     <eb:CollaborationInfo>
470         <eb:AgreementRef>PeekMessageAgreementExample</eb:AgreementRef>
471         <eb:Service>MarketMessaging</eb:Service>
472         <eb:Action>PeekMessage.request</eb:Action>
473         <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
474     </eb:CollaborationInfo>
475 </eb:UserMessage>
476 </eb:Messaging>
477 </soapenv:Header>
478 <soapenv:Body>
479     <urn:PeekMessageRequest>
480         <urn:MessageDomains>
481             <urn:MessageDomain>DATALOAD</urn:MessageDomain>
482         </urn:MessageDomains>
483     </urn:PeekMessageRequest>
484 </soapenv:Body>
485 </soapenv:Envelope>
486

```

487 5.4.5.3.2. Przykład odpowiedzi PeekMessage

```

488
489 <soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
490 xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
491     <soapenv:Header>
492         <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
493 soapenv:mustUnderstand="true">
494             <eb:UserMessage>
495                 <eb:MessageInfo>
496                     <eb:Timestamp>2023-08-03T07:36:21.641Z</eb:Timestamp>
497                     <eb:MessageId>d7c3eccf-0781-4789-a456-375b39e8bccf</eb:MessageId>
498                 </eb:MessageInfo>
499                 <eb:PartyInfo>
500                     <eb:From>
501                         <eb:PartyId>ExampleParty2</eb:PartyId>
502                         <eb:Role>ExampleParty2Role</eb:Role>
503                     </eb:From>
504                     <eb:To>
505                         <eb:PartyId>ExampleParty1</eb:PartyId>
506                         <eb:Role>ExampleParty1Role</eb:Role>
507                     </eb:To>
508                 </eb:PartyInfo>
509                 <eb:CollaborationInfo>
510                     <eb:AgreementRef>PeekMessageAgreementExample</eb:AgreementRef>
511                     <eb:Service>MarketMessaging</eb:Service>
512                     <eb:Action>PeekMessage.reply</eb:Action>
513                     <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
514                 </eb:CollaborationInfo>
515             </eb:UserMessage>
516         </eb:Messaging>
517     </soapenv:Header>
518     <soapenv:Body>
519         <urn:PeekMessageResponse>
520             <urn:MessageContainer>
521                 <urn:DocumentReferenceNumber>cc3ae4a7-e93f-406a-99c8-
522 4bbc66ab5140</urn:DocumentReferenceNumber>
523                 <urn:Payload>
524                     ...
525                 </urn:Payload>
526             </urn:MessageContainer>
527         </urn:PeekMessageResponse>
528     </soapenv:Body>
529 </soapenv:Envelope>
530

```

530

531 5.4.5.3.3. Przykład odpowiedzi PeekMessage, gdy brak wiadomości w kolejce 532 (EBMS:0006).

```

533 <env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
534     <env:Header>
535         <ns2:Messaging xmlns:ns2="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
536             xmlns:ns3="http://schemas.xmlsoap.org/soap/envelope/"

```

```

537         env:mustUnderstand="true">
538     <ns2:SignalMessage>
539     <ns2:MessageInfo>
540     <ns2:Timestamp>2023-08-03T07:21:17.993Z</ns2:Timestamp>
541     <ns2:MessageId>7d3e50b4-f372-4c48-865b-8193f3dd674c</ns2:MessageId>
542     <ns2:RefToMessageId>10891C6e-8d0c-4701-9a1d-c84fd39d4832</ns2:RefToMessageId>
543     </ns2:MessageInfo>
544     <ns2:Error category="Communication"
545         errorCode="EBMS:0006"
546         origin="ebMS"
547         refToMessageInError="10891C6e-8d0c-4701-9a1d-c84fd39d4832"
548         severity="warning"
549         shortDescription="EmptyMessagePartitionChannel">
550     <ns2:Description xml:lang="En">The Message queue is empty</ns2:Description>
551     <ns2:ErrorDetail>The Message queue is empty</ns2:ErrorDetail>
552     </ns2:Error>
553     </ns2:SignalMessage>
554 </ns2:Messaging>
555 </env:Header>
556 <env:Body/>
557 </env:Envelope>

```

558

559 5.4.5.4. Operacja DequeueMessage

- 560 - Zrealizowaną jako wzorzec One-Way Push.
- 561 - Wywołanie odpowiada wiadomości typu UserMessage (AS4) zawierającej payload
- 562 zgodny z XSD (patrz 5.4.5.5).
- 563 - Poprawne wywołanie skutkuje zwróceniem kodu HTTP 202.
- 564 - W przypadku błędu zwracany jest komunikat zgodny z opisem w punktach 5.4.6
- 565 oraz 5.4.7.
- 566

567 5.4.5.5. Struktura wiadomości dla DequeueMessage

568 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).

569

570 5.4.5.5.1. Przykład wywołania DequeueMessage

```

571 <soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
572 xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:cms:b2b:message:v01:v1">
573   <soapenv:Header>
574     <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
575     soapenv:mustUnderstand="1">
576       <eb:UserMessage>
577         <eb:MessageInfo>
578           <eb:Timestamp>2023-08-03T07:36:20.656Z</eb:Timestamp>
579           <eb:MessageId>d7c3eccf-0781-4789-a456-035b39e8bb20</eb:MessageId>
580         </eb:MessageInfo>
581         <eb:PartyInfo>
582           <eb:From>
583             <eb:PartyId>ExampleParty1</eb:PartyId>
584             <eb:Role>ExampleParty1Role</eb:Role>

```

```

585     </eb:From>
586     <eb:To>
587         <eb:PartyId>ExampleParty2</eb:PartyId>
588         <eb:Role>ExampleParty2Role</eb:Role>
589     </eb:To>
590 </eb:PartyInfo>
591 <eb:CollaborationInfo>
592     <eb:AgreementRef>DequeueMessageAgreementExample</eb:AgreementRef>
593     <eb:Service>MarketMessaging</eb:Service>
594     <eb:Action>DequeueMessage</eb:Action>
595     <eb:ConversationId>2a81ffbd-0d3d-4cbd-8601-d916e0ed2fe2</eb:ConversationId>
596 </eb:CollaborationInfo>
597 </eb:UserMessage>
598 </eb:Messaging>
599 </soapenv:Header>
600 <soapenv:Body>
601     <urn:DequeueMessageRequest>
602         <urn:DocumentReferenceNumber>cc3ae4a7-e93f-406a-99c8-
603 4bbc66ab5140</urn:DocumentReferenceNumber>
604     </urn:DequeueMessageRequest>
605 </soapenv:Body>
606 </soapenv:Envelope>

```

607 5.4.6. Techniczne kody błędów na poziomie warstwy transportowej

608

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

609 Tabela 8 Techniczne kody błędów

610

611 5.4.7. Techniczne kody błędów AS4

612

613 Kanał AS4 zawsze zwraca błędy jako ebMS SignalMessages (ze statusem HTTP: 4xx lub
614 5xx).

Kod błędu	Opis	Ważność	Znaczenie	Sugerowany sposób obsługi
EBMS:0001	Wartość nierozpoznana	Błąd	Dokument komunikatu jest dobrze sformułowany, a schemat prawidłowy, niemniej jednak jakiś element/atribut zawiera wartość, której nie można rozpoznać i dlatego MSH nie może go użyć.	Popraw wiadomość i wyślij ponownie.
EBMS:0002	Funkcja nieobsługiwana	Ostrzeżenie	Chociaż dokument komunikatu jest prawidłowo sformułowany, a schemat prawidłowy, niektórych wartości elementu/atributu nie można przetworzyć zgodnie z oczekiwaniami, ponieważ powiązana funkcja nie jest obsługiwana przez MSH.	Usuń nieobsługiwane funkcje z wiadomości i wyślij poprawioną wiadomość.
EBMS:0003	Wartości niespójne	Błąd	Chociaż dokument komunikatu jest dobrze sformułowany, a schemat prawidłowy, wartość niektórych elementów/atributów jest niespójna albo z treścią innego elementu/atributu, albo z trybem przetwarzania MSH, albo z wymaganiami normatywnymi specyfikacji ebMS.	Sprawdź, czy poprawić komunikat lub zmienić konfigurację PMode. Po poprawieniu wyślij ponownie wiadomość.

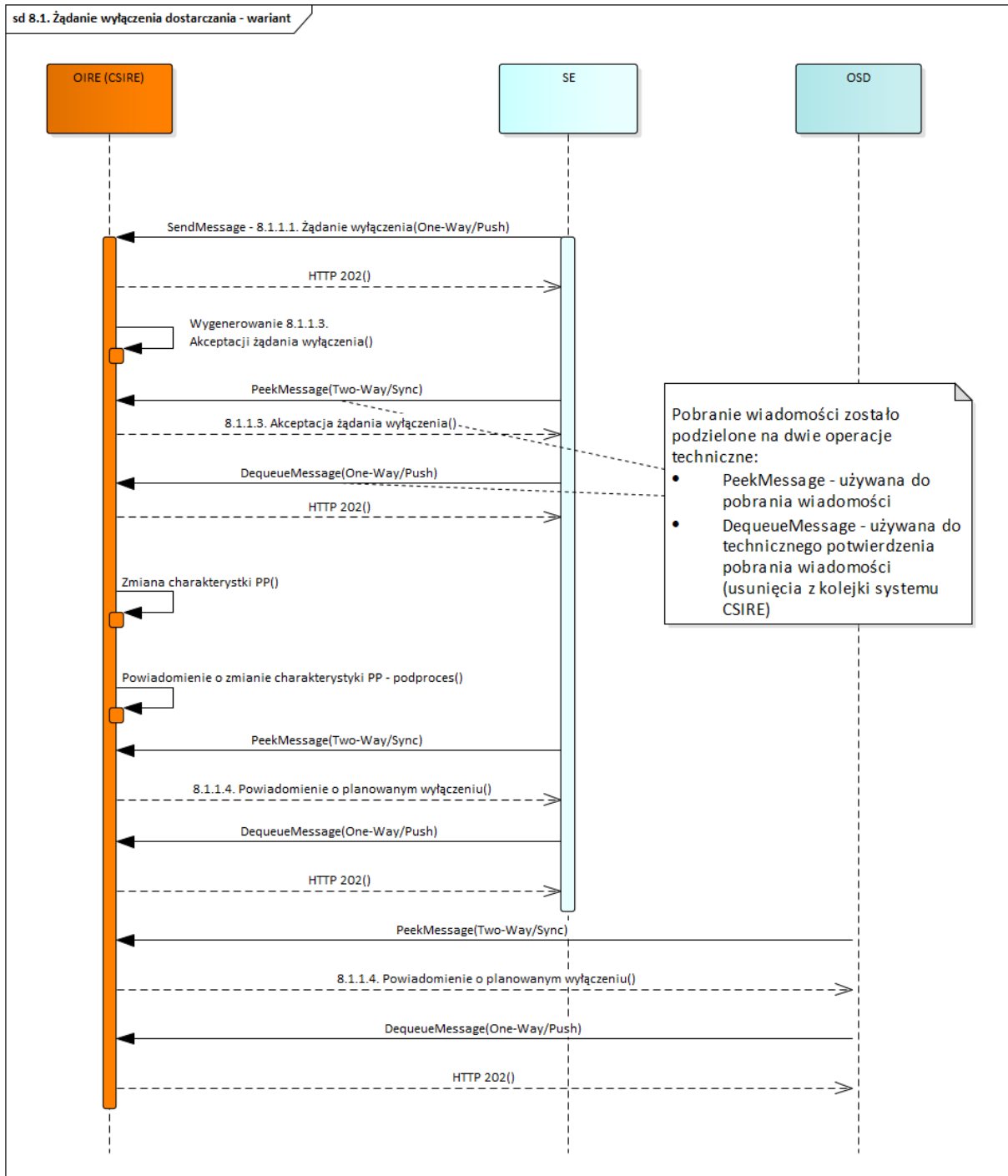
Kod błędu	Opis	Ważność	Znaczenie	Sugerowany sposób obsługi
EBMS:0004	Inny	Błąd		Sprawdź element ErrorDetail w Error, aby dowiedzieć się, co poszło nie tak. W przypadku, gdy payload nie jest prawidłowo sformułowany/schemat jest nieprawidłowy, payload musi zostać poprawiony przed próbą ponownego wysłania.
EBMS:0005	Błąd połączenia	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	Pusty kanał partycji wiadomości	Ostrzeżenie	W kolejce wiadomości nie ma dostępnych wiadomości.	Ponów wywołanie po określonym czasie.
EBMS:0007	Niepoprawna wartość MIME	Błąd	Użycie MIME nie jest zgodne z wymaganym użyciem w tej specyfikacji.	Popraw załącznik i wyślij ponownie.
EBMS:0008	Funkcja nieobsługiwana	Błąd	Chociaż dokument komunikatu jest dobrze sformułowany, a schemat prawidłowy, obecność lub brak niektórych elementów/atributów nie jest zgodna z możliwościami MSH w odniesieniu do obsługiwanych funkcji.	Popraw wiadomość i wyślij ponownie.
EBMS:0009	Nieprawidłowy nagłówek	Błąd	Nagłówek ebMS jest albo źle sformułowany jako dokument XML, albo nie jest zgodny z regułami pakowania ebMS.	Popraw wiadomość i wyślij ponownie.

Kod błędu	Opis	Ważność	Znaczenie	Sugerowany sposób obsługi
EBMS:0010	Niezgodność trybu przetwarzania	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.
EBMS:0011	Błąd zewnętrznego payload	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	Nieudane uwierzytelnianie	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	Nieudane odszyfrowywanie	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 poprawnym kluczem.
EBMS:0103	Niezgodność z polityką bezpieczeństwa	Błąd	Metody zabezpieczeń, parametry, zakres lub inne wymagania lub umowy na poziomie polityki bezpieczeństwa nie zostały spełnione.	Popraw wiadomość i wyślij ponownie.

615

616 Tabela 9 Techniczne kody błędów AS4

617 5.4.8. Przykład realizacji początkowych kroków procesu SWI z mapowaniem na
 618 wywołania interfejsu CSIRE
 619



620
 621 Rysunek 8 Diagram sekwencji wywołań systemu CSIRE dla początkowych kroków procesu 8.1. Żądanie
 622 wyłączenia dostarczania" dla "poprawnego" przebiegu.

623
 624 Na powyższym diagramie przedstawiono sekwencję wywołań dla pierwszych kroków procesu
 625 „8.1. Żądanie wyłączenia dostarczania” z SWI przy założeniu rozpoczęcia procesu przez
 626 SE/SEu i poprawnej komunikacji z systemem CSIRE (brak błędów technicznych
 627 i biznesowych).

- 628
- 629
- 630
- 631
- 632
- 633
- 634
- 635
- 636
- 637
- 638
- 639
- 640
- 641
- 642
- 643
- 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 operację 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.

644 6. BEZPIECZEŃSTWO

645 Rozdział ten opisuje zagadnienia konfiguracji zabezpieczeń dla wykorzystania Profilu AS4
 646 zdefiniowanego w dokumencie „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile], w sposób zgodny
 647 z wymaganiami określonymi dla ENTSOG AS4 ebHandler oraz uwzględniający bieżące
 648 rekomendacje obowiązujące w PSE w zakresie stosowania zabezpieczeń kryptograficznych.
 649 Wymienione niżej wymagania konfiguracji zabezpieczeń stanowią aktualizację treści sekcji
 650 2.3.4 „Security” dokumentu „ENTSOG AS4 Profile 3.6” [EG-AS4-Profile].

651

652 6.1. Zabezpieczenie komunikacji w warstwie sieci

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

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

660 6.2. Zabezpieczenie komunikacji w warstwie transportowej

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

- 666 1. Wymagane jest użycie protokołu TLS w wersji 1.2 lub 1.3 (rekomendowana). Obsługa
 667 protokołów SSL 2.x, 3.x oraz TLS w wersjach 1.0, 1.1, 1.2 musi być wyłączona.
- 668 2. W przypadku użycia TLS w wersji 1.3 strony komunikacji muszą wspierać obsługę
 669 zestawów algorytmów kryptograficznych TLS_AES_128_GCM_SHA256,
 670 TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256.
- 671 3. W przypadku użycia TLS w wersji 1.2 strony komunikacji muszą wspierać obsługę
 672 zestawów algorytmów kryptograficznych ECDHE-ECDSA-AES128-GCM-SHA256,
 673 ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384,
 674 ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305,
 675 ECDHE-RSA-CHACHA20-POLY1305, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-
 676 AES256-GCM-SHA384, DHE-RSA-CHACHA20-POLY1305
- 677 4. Obsługa zestawów algorytmów kryptograficznych innych, niż wymienione powyżej
 678 musi być wyłączona.
- 679 5. Obustronne uwierzytelnianie mTLS musi być stosowane. W tym celu dopuszcza się
 680 wykorzystanie odpowiednich certyfikatów wydanych dla nazw DNS urządzeń
 681 występujących w podwójnej roli serwera i klienta TLS.
- 682 6. Certyfikaty wykorzystywane przez odrębne komponenty infrastruktury zapewniające
 683 obsługę komunikacji TLS muszą spełniać wszystkie warunki określone w punkcie
 684 6.4 „Certyfikaty oraz Infrastruktura Klucza Publicznego (PKI)”.

685

6.3. Zabezpieczenie komunikacji w warstwie komunikatu

687

688 Lista wspieranych algorytmów podpisywania i szyfrowania wiadomości przedstawiona
689 w poniższych rozdziałach może być rozszerzona w kolejnych wersjach niniejszego
690 dokumentu.

691

6.3.1. Podpisywanie wiadomości

693

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

697 Rekomendowane jest aby certyfikat do podpisu wiadomości posiadał wartość atrybutu użycia
698 klucza (ang. *key usage*): niezaprzeczalność (ang. *non-repudiation*).

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

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

705

706 Parametry/warianty dostępne do podpisywania wiadomości:

- 707 • Algorytmy podpisu dostępne w CSIRE:
 - 708 - (default) RSA-SHA256 (<http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>)
 - 709 - RSA-SHA384 (<http://www.w3.org/2001/04/xmldsig-more#rsa-sha384>)
 - 710 - RSA-SHA512 (<http://www.w3.org/2001/04/xmldsig-more#rsa-sha512>)
 - 711
- 712 • Funkcje skrótu dostępne w CSIRE:
 - 713 - SHA-1 (<http://www.w3.org/2000/09/xmldsig#sha1>)
 - 714 - (default) SHA-256 (<http://www.w3.org/2001/04/xmlenc#sha256>)
 - 715 - SHA-384 (<http://www.w3.org/2001/04/xmldsig-more#sha384>)
 - 716 - SHA-512 (<http://www.w3.org/2001/04/xmlenc#sha512>)

717

6.3.2. Szyfrowanie wiadomości

719

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

724

725 Wiadomości wejściowe:

- 726 • brak konfiguracji dla szyfrowania dla wiadomości wejściowych.

- 727 • CSIRE sprawdza wiadomość, czy jakiegokolwiek element zawiera znacznik
728 EncryptedData i wtedy odszyfrowuje wiadomość.

729

730 Wiadomości wyjściowe:

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

734

735 Parametry i opcje używane do szyfrowania wiadomości:

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

738 CSIRE stosuje następujący typ: Binary security token

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

- 744 • Algorytm szyfrowania klucza: Algorytm asymetryczny używany do szyfrowania klucza
745 symetrycznego (np. AES).
746 • Wybór dostępny na liście jest kontrolowany przez WS-Security Framework.

747 Algorytmy szyfrowania klucza dostępne w CSIRE:

- 748 - (default) RSA-OAEP including MGF1 with SHA1
749 (<http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p>)
750 - RSA-v1.5 (http://www.w3.org/2001/04/xmlenc#rsa-1_5)
751 - RSA-OAEP (<http://www.w3.org/2009/xmlenc11#rsa-oaep>)
752
753 • Algorytm szyfrowania: Algorytm stosowany do szyfrowania payload przy użyciu klucza
754 symetrycznego wiadomości.

755 CSIRE udostępnia poniższe algorytmy:

- 756 - (default) AES128-GCM (<http://www.w3.org/2009/xmlenc11#aes128-gcm>)
757 - AES192-GCM (<http://www.w3.org/2009/xmlenc11#aes192-gcm>)
758 - AES256-GCM (<http://www.w3.org/2009/xmlenc11#aes256-gcm>)
759

760 Zachowane ze względu na kompatybilność wsteczną – niezalecane:

- 761 - AES-128-CBC (<http://www.w3.org/2001/04/xmlenc#aes128-cbc>)
762 - AES-192-CBC (<http://www.w3.org/2001/04/xmlenc#aes192-cbc>)
763 - AES-256-CBC (<http://www.w3.org/2001/04/xmlenc#aes256-cbc>)
764

765 6.4. Certyfikaty oraz Infrastruktura Klucza Publicznego (PKI)

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

- 771 1. Wybór Urzędu Certyfikacji PKI wydającego certyfikaty nie podlega przeglądowi przez
772 ENTSOG.
- 773 2. Certyfikaty przeznaczone do wykorzystania produkcyjnego muszą być wydane przez
774 powszechnie zaufane Centrum Certyfikacji PKI, spełniające warunki dla
775 kwalifikowanych podmiotów świadczących usługi zaufania, zgodnie z przepisami
776 rozporządzenia eIDAS i zarejestrowane na liście zaufania opublikowanej w witrynie
777 „EU Trust Services Dashboard” Komisji Europejskiej, lub posiadające pieczęć
778 AICPA/CICA WebTrust.
- 779 3. Nie dopuszcza się stosowania tych samych certyfikatów w środowiskach
780 produkcyjnych i środowiskach testowych, za wyjątkiem certyfikatów uwierzytelniania
781 serwera TLS, wydanych dla wielu domen DNS lub dla domen z „dziką kartą”.
- 782 4. Informacje o statusie odwołania wykorzystywanych certyfikatów, muszą być
783 udostępniane w sposób niezawodny pod dostępnym dla stron uczestniczących w
784 komunikacji adresem wskazanym w atrybutach CDP (CRL Distribution Point) lub AIA
785 OCSP certyfikatu pod rygorem odrzucenia weryfikowanych tymi certyfikatami połączeń
786 lub wiadomości.

787

788 6.5. Wymiana Certyfikatu

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

793 **7. KOMPRESJA**

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

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

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

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

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

809 8. IMPLEMENTACJA ROZWIĄZANIA

810 8.1. Wprowadzenie

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

815

816 8.2. Identyfikacja stron

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

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

824 Identyfikatory EIC stron komunikacji AS4 pozwalają na jednoznaczną identyfikację
825 Kontrahenta.

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

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

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

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

841 8.2.1. Identyfikacja i rola rynkowa OIRE

842 OIRE identyfikują wartości podane w poniższej tabeli.

843 Tabela 10 Kod EIC OIRE

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

844 Rola rynkowa wykorzystywana przez OIRE będzie podawana na bieżąco przed rozpoczęciem
845 interakcji z CSIRE.

846

847 **8.2.2. Przykład wywołania SendMessage**

848 Dla Kontrahenta A (ExampleParty1=Kod EIC Kontrahenta A; ExampleParty1Role= Rola
849 rynkowa Kontrahenta A).

850 Dla Kontrahenta B (ExampleParty1=Kod EIC Kontrahenta B; ExampleParty1Role= Rola
851 rynkowa Kontrahenta B).

852 Dla kolejnych Kontrahentów identycznie.

853

854 OIRE to zawsze (ExampleParty2=Kod EIC OIRE; ExampleParty2Role= Rola rynkowa OIRE).

855

```

856 <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
857 xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
858 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
859 xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
860 <soap:Header>
861   <eb:Messaging soap:mustUnderstand="true">
862     <eb:UserMessage>
863       <eb:MessageInfo>
864         <eb:Timestamp> 2024-05-25T00:00:00+02:00</eb:Timestamp>
865         <eb:MessageId>181c3aa2-53b8-4eb5-a521-d6236cfae85f</eb:MessageId>
866       </eb:MessageInfo>
867       <eb:PartyInfo>
868         <eb:From>
869           <eb:PartyId>ExampleParty1</eb:PartyId>
870           <eb:Role>ExampleParty1Role</eb:Role>
871         </eb:From>
872         <eb:To>
873           <eb:PartyId>ExampleParty2</eb:PartyId>
874           <eb:Role>ExampleParty2Role</eb:Role>
875         </eb:To>
876       </eb:PartyInfo>
877       <eb:CollaborationInfo>
878         <eb:AgreementRef>urn:pl:oire:as4:agreement:SendMessage</eb:AgreementRef>
879         <eb:Service>MarketMessaging</eb:Service>
880         <eb:Action>SendMessage</eb:Action>
881         <eb:ConversationId>2011-921</eb:ConversationId>
882       </eb:CollaborationInfo>
883       <eb:PayloadInfo>
884         <eb:PartInfo/>
885       </eb:PayloadInfo>
886     </eb:UserMessage>
887   </eb:Messaging>
888 </soap:Header>
889 <soap:Body>
890   <urn:SendMessageRequest xmlns:urn="urn:cms:b2b:v01" xmlns:urn1="urn:pl:oire:unk_2_1_1_1:v1"
891   xmlns:urn2="urn:pl:oire:technical:v1">
892     <urn:MessageContainer>
893       <urn:Payload>
894         <urn1:MeteringPointCreationNotification>
895           <urn1:Header>
896             <urn2:MessageId>5c9b488f-4af2-4d02-14fd-583e9090dbd9</urn2:MessageId>
897             <urn2:MessageType>2.1_1</urn2:MessageType>
898             <urn2:MessageTypeResponsibleOrganization>x</urn2:MessageTypeResponsibleOrganization>
899             <urn2:MessageTimestamp>2024-05-25T00:00:00+02:00</urn2:MessageTimestamp>
900             <urn2:PhysicalSenderId>ExampleParty1</urn2:PhysicalSenderId>
901             <urn2:PhysicalSenderIdResponsibleOrganization>x</urn2:PhysicalSenderIdResponsibleOrganization>
902             <urn2:JuridicalSenderId>ExampleParty1</urn2:JuridicalSenderId>
903             <urn2:JuridicalSenderIdResponsibleOrganization>x</urn2:JuridicalSenderIdResponsibleOrganization>
904             <urn2:PhysicalRecipientId>ExampleParty2/CSIRE</urn2:PhysicalRecipientId>
905             <urn2:PhysicalRecipientIdResponsibleOrganization>x</urn2:PhysicalRecipientIdResponsibleOrganization>
906             <urn2:JuridicalRecipientId>ExampleParty2</urn2:JuridicalRecipientId>
907             <urn2:JuridicalRecipientIdResponsibleOrganization>x</urn2:JuridicalRecipientIdResponsibleOrganization>
908           </urn1:Header>
909           . . . . .
910           . . . . .
911           . . . . .
912         </urn1:Header>
913       </urn:Payload>

```



```
914     </urn1:MeteringPointCreationNotification>
915     </urn:Payload>
916     </urn:MessageContainer>
917     </urn:SendMessageRequest>
918 </soap:Body>
919 </soap:Envelope>
920
```

921 8.3. Dostarczenie wiadomości, powtórzenia, obsługa niedostępności

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

925 Jednocześnie należy dopilnować, by żaden system zewnętrzny nie wygenerował zbyt dużego
926 ruchu sieciowego, poprzez nieustanne podejmowane próby ponownego wysłania wiadomości,
927 która nie może być z powodów technicznych dostarczona (patrz kody błędów opisane w 5.4.6
928 i 5.4.7).

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

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

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

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

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

941 Kolejgowanie wiadomości powinno być zrealizowane w taki sposób, aby zapewnić
942 persystencję wiadomości, odporność na awarie (wyłączenie) oraz możliwość ponowienia
943 zgodnie z oryginalną kolejnością.

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

948

949 8.4. Wymagania odnośnie środowisk systemów współpracujących 950 z CSIRE

951

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

- 955 • certyfikacyjnym,
- 956 • pilotażowym.

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

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

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

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

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

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

971 8.5. Wymagania w zakresie rejestracji zdarzeń

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

975 Zdarzenia muszą być przechowywane przez okres co najmniej dwóch lat.

976 Dzienniki zdarzeń muszą zawierać co najmniej następujące informacje:

- 977 • źródło danych (Message Producer),
- 978 • datę zdarzenia,
- 979 • użytkownika (właściciela procesu na poziomie systemu operacyjnego),
- 980 • znak czasu (Timestamp) ,
- 981 • adresy IP: źródłowy (Message Producer) oraz docelowy (CSIRE),
- 982 • użyta operacja (SendMessage, PeekMessage, DequeueMessage),
- 983 • status odpowiedzi serwera (techniczne kody błędów opisane w 5.4.6 i 5.4.7).

985 **9. REKOMENDACJE W ZAKRESIE CERTYFIKACJI AS4**

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

990 Aktualna lista zweryfikowanych rozwiązań znajduje się w: [https://www.drummondgroup.com/
991 certified-products-2/b2b-interoperability/#appst](https://www.drummondgroup.com/certified-products-2/b2b-interoperability/#appst)

992 10. PRZYSZŁE FUNKCJE I ZMIANY

993 Daty wprowadzenia i udostępnienia zmian zostaną podane dedykowanymi komunikatami.

994 10.1. Obsługa operacji PeekMessage z wykorzystaniem wzorca One-Way/Pull

996 Dla operacji PeekMessage do istniejącego wzorca Two-Way/Sync zostanie dodany wzorzec
997 One-Way/Pull.

998 Niezależnie od obsługiwanego wzorca operacja PeekMessage pobiera wiadomości z tego
999 samego zestawu kolejek.

1000 Operacja PeekMessage będzie umożliwiać podanie danych o kolejkach w nagłówku SOAP
1001 jako atrybut MPC (istniejący mechanizm umożliwiający podanie danych o kolejkach w *payload*
1002 nie ulegnie zmianie).

1003 W wypadku chęci pobrania pierwszej dostępnej wiadomości ze wszystkich kolejek wymagane
1004 jest użycie domyślnej wartości kolejki "[http://docs.oasis-open.org/ebxml-
1005 msg/ebms/v3.0/ns/core/200704/defaultMPC](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC)" w polu MPC.

1006 Podczas wykonywania operacji PeekMessage wymagane będzie używanie jednego
1007 z powyższych mechanizmów.

1008 Dla wzorca One-Way/Pull możliwe będzie pobieranie wiadomości z wielu kolejek.
1009 Separatorem, pomiędzy nazwami kolejek, podanymi w MPC będzie średnik (;).

1010 Obsługa pozostałych operacji nie ulegnie zmianie.

1011 10.2. Zmiana statusu HTTP z 4xx na 2xx

1012 Dla poniższego błędu zostanie zmieniony status HTTP.

Kod błędu	Opis	Ważność	Znaczenie	Sugerowany sposób obsługi
EBMS:0006	Pusty kanał partycji wiadomości	Ostrzeżenie	W kolejce wiadomości nie ma dostępnych wiadomości.	Ponów wywołanie po określonym czasie.

1013

11.SPIS TABEL I RYSUNKÓW

1014	Tabela 1. Wykaz definicji.....	6
1015	Tabela 2. Lista skrótów.....	8
1016	Tabela 3. Dokumenty powiązane	9
1017	Tabela 4 Przykład pary konfiguracji PMode dla operacji PeekMessage.....	16
1018	Tabela 5 Parametry PMode dostępne do konfiguracji	16
1019	Tabela 6 Parametry PMode ze stałą wartością bądź nieobsługiwane	19
1020	Tabela 7 Nazwy kolejek wyjściowych CSIRE	32
1021	Tabela 8 Techniczne kody błędów	36
1022	Tabela 9 Techniczne kody błędów AS4.....	39
1023	Tabela 10 Kod EIC OIRE	47
1024	Tabela 11 Odniesienia.....	54
1025	Rysunek 1 Struktura wiadomości (User Message Structure, [ebMS3CORE]).....	13
1026	Rysunek 2 Struktura wiadomości sygnałowej (Signal Message Structure, [ebMS3CORE]).....	14
1027	Rysunek 3 One-Way/Push MEP.....	25
1028	Rysunek 4 Two-Way/Sync MEP	26
1029	Rysunek 5 Operacja SendMessage	27
1030	Rysunek 6 Operacje PeekMessage i DequeueMessage – prawidłowa sekwencja wywołań	30
1031	Rysunek 7 Pierwsze wywołanie PeekMessage bez DequeueMessage – nieprawidłowa sekwencja wywołań (jeśli	
1032	nie chcemy ponownie pobrać tej samej wiadomości)	31
1033	Rysunek 8 Diagram sekwencji wywołań systemu CSIRE dla początkowych kroków procesu 8.1. Żądanie	
1034	wyłączenia dostarczania" dla "poprawnego" przebiegu.	40

12.ODNIESIENIA

1035

Nazwa	Źródło
[AS4-Profile]	AS4 Profile of ebMS 3.0 Version 1.0 OASIS Standard 23 January 2013 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 https://docs.oasis-open.org/bdxb/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 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 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 Publication date : 2021-02 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 Publication date : 2021-02 https://www.iso.org/standard/79109.html
[SOAP12]	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) W3C Recommendation 27 April 2007 https://www.w3.org/TR/soap12/
[SOAPATTACH]	SOAP Messages with Attachments: W3C Note 11 December 2000 https://www.w3.org/TR/SOAP-attachments/
[XMLDSIG]	XML-Signature Syntax and Processing (Second Edition). W3C Recommendation. 10 June 2008. http://www.w3.org/TR/xmlsig-core/
[WSS10]	Web Services Security: SOAP Message Security 1.0, 2004 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 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SOAPMessageSecurity.pdf

1036

Tabela 11 Odniesienia

1037

1038 **13.ZAŁĄCZNIKI**

1039 13.1. Załącznik 1 – WSDL

1040

1041 13.2. Załącznik 2 – Parametry PMode CSIRE