Załącznik nr 1

# OPIS PRZEDMIOTU ZAMÓWIENIA – minimalne wymagania integracyjne systemu szpitalnego z RREDM

**Poniżej przedstawione zostały minimalne funkcjonalności RREDM według dokumentacji interoperacyjności:**

Wszystkie wyszczególnione funkcjonalności odnoszą się zarówno do kontekstu kont użytkowników (lekarze, pacjenci) jak i kont podmiotów leczniczych (szpitale, przychodnie)

## 1. GŁÓWNA FUNKCJONALNOŚĆ EDM:

• Deponowanie dokumentów w repozytorium EDM

• Indeksowanie dokumentów w rejestrze EDM

• Udostępnianie EDM

• Ewidencja danych źródłowych

• Tworzenie EDM (np. PIK HL7 CDA)

• Podpisywanie dokumentacji (XADES - otaczany)

• Deponuje EDM w repozytorium (API XDS.b – ITI-41)

• Wyszukiwanie EDM w rejestrze (API XDS.b – ITI-18)

• Pobieranie dokumentacji z repozytorium (API XDS.b – ITI-43)

• Administracja dokumentacją

• Obsługa zgód pacjentów

• Obsługa błędów

• Usuwanie dokumentów, niszczenie dokumentacji ITI-62 i ITI-86)

• Integracja z Platformą P1

## 2. Szczegółowe funkcjonalności RREDM (wg. Dokumentacji interoperacyjności)

4.1 Administracja kontem podmiotu leczniczego (tenanta)

4.1.1 Proces zakładania i aktywacji konta podmiotu leczniczego

4.1.2 Funkcjonalność panelu administratora konta podmiotu leczniczego

4.2 Zarządzanie EDM - Profil integracyjny XDS.b

4.2.2.1 Deponowanie dokumentów w regionalnym repozytorium EDM z poziomu systemu dziedzinowego partnerskiego podmiotu leczniczego (ITI-41)

4.2.2.2 Indeksowanie w rejestrze regionalnym EDM z poziomu systemu dziedzinowego partnerskiego podmiotu leczniczego (ITI-42)

4.2.2.3 Usuwanie dokumentu z regionalnego rejestru EDM z poziomu systemu dziedzinowego partnerskiego podmiotu leczniczego (ITI-62)

4.2.2.5 Wyszukiwanie dokumentów w regionalnym rejestrze EDM (ITI-18)

4.2.2.6 Pobieranie dokumentów z regionalnego repozytorium EDM (ITI-43)

4.2.2.7 Udostępnianie dokumentów zdeponowanych w regionalnym repozytorium EDM zewnętrznym podmiotom leczniczym za pośrednictwem P1

4.3 Logi audytu (ATNA)

4.4.2.1 Interfejsy i model transportowy

4.4 Zgody pacjentów na dostęp do EDM

4.4.1 Rejestr zgód – Przypadki użycia

Rozwiązanie pozwala na definiowanie zgód pacjenta na dostęp do dokumentacji medycznej zgodnie z profilem IHE APPC.

- Rodzaj zgody

o Pozytywne (przyznanie dostępu do dokumentu)

o Uwaga: Nie są wspierane sprzeciwy na dostęp do danych

- Zakres zgody

o Całość dokumentacji

o Wybrane typy dokumentów

o Konkretne dokumenty

- Wystawcy zgody

o Pacjent

o Personel medyczny

- Beneficjenci zgody

o Placówka medyczna

o Pacjent

o Personel

- Ograniczenia

o Zgody mogą być ograniczone czasowo lub bezterminowe

- Wyjątki (zgody automatyczne wynikające z przyjętej polityki dostępu)

4.5 Integracja z platformą P1 (w zakresie EDM)

- Wyszukiwania dokumentacji w P1.

- Pobieranie dokumentacji z Repozytoriów innych podmiotów.

- Udostępnianie dokumentacji innym podmiotom.

- Rejestracja i pobieranie danych dostępowych repozytoriów.

5.1 Wykorzystane standardy integracji

- Interfejs aplikacyjny API (profile IHE: XDS.b, APPC, ATNA).

- WEB-SERVICE (SOAP based Web Services).

- Warstwa bezpieczeństwa,

o Dwustronne uwierzytelnianie systemów oparte na certyfikatach X.509 (mTLS),

o Wszystkie żądania usług biznesowych podpisane zgodnie z WS-Security,

o SAML 2.0. Tokeny SAML jako wiarygodny nośnik kontekstu wywoływanych żądań,

o Pełna separacja logiczna/fizyczna danych podmiotów leczniczych (tenantów),

o Szyfrowanie dokumentacji, klucze symetryczne (obsługa w całości po stronie sytemu RREDM).

- Format prowadzenia dokumentacji,

o HL7 CDA (poziom 1),

o Preferowany PIK HL7 CDA (poziom 3),

o Możliwe deponowanie dokumentów w innych formatach np. załączników PDF.

5.2 Klasyfikacje typów dokumentów

- Dla dokumentów indeksowanych w P1

o classCode musi przyjmować wartości ze słownika https://www.cez.gov.pl/HL7POL-1.3.1.2/plcda-1.3.1.2/plcda-html-1.3.1.2/plcda-html-1.3.1.2/voc-2.16.840.1.113883.3.4424.13.11.1-2018-09-30T000000.html

o typeCode powinien przyjmować wartość odpowiedniego kodu LOINC.

- Dla dokumentów spoza klasyfikacji P1 deponowanych w AMDX 2.0 (nie indeksowanych w P1) metadane „classCode” oraz „typeCode” powinny przyjmować wartość odpowiedniego kodu LOINC.

5.3 Podpisywanie EDM

- Podpis składany bezpośrednio w systemie dziedzinowym podmiotu leczniczego LIS, RIS, HIS itd.

- Format podpisu (XADES, wymagany jest podpis otaczany ze względu na zgodność z P1).

5.5 Wzajemne uwierzytelnianie stron biorących udział w komunikacji

Komunikacja realizowana jest za pomocą protokołu TLS w wersji 1.2. Podczas nawiązywania połączenia następuje obustronne uwierzytelnienie stron biorących udział w komunikacji (system RREDM oraz system w podmiocie leczniczym). Do nawiązania połączenia należy użyć certyfikatu TLS wydanego przez operatora systemu RREDM. Każda ze stron przedstawia się certyfikatem TLS. System RREDM weryfikuje certyfikat przekazany przez system podmiotu leczniczego. System RREDM

porównuje przekazany certyfikat z certyfikatem zapisanym na koncie podmiotu leczniczego w systemie RREDM. Analogicznie system podmiotu leczniczego powinien zweryfikować certyfikat systemu RREDM.

5.6 Uwierzytelnianie i autoryzacja w usługach SOAP systemu RREDM, generowanie tokenu SAML

Nośnikiem kontekstu wywołania usług SOAP systemu RREDM jest token SAML. Token SAML jest niezbędny do uzyskania dostępu do zasobów udostępnianych poprzez usługi SOAP. System RREDM udostępnia interfejs SecurityTokenService, który umożliwia generację tokenów SAML.

5.7 Nagłówek WS-Security

W celu zabezpieczenia przekazywanych komunikatów przed niepożądaną zmianą, wprowadzono zabezpieczenia oparte na protokole WS-Security. Oprócz certyfikatu TLS, podmiot leczniczy na etapie wdrożenia otrzyma certyfikat służący do podpisywania komunikatów (oznaczony jako certyfikat WSS). Certyfikatu WSS należy użyć do podpisywania komunikatów. Do nagłówka komunikatu dodawany jest nagłówek WS-Security – element wsse:Security, zawierający wymienione poniżej sekcje:

- Sekcja wsse:BinarySecurityToken. Sekcja zawiera certyfikat WSS, który służy do weryfikacji podpisu. Certyfikat jest zakodowany w standardzie Base64.

- Sekcja wsu:Timestamp. Sekcja zawiera czas utworzenia i czas wygaśnięcia komunikatu.

- Sekcja ds:Signature. Sekcja zawiera informacje na temat podpisu oraz podpis komunikatu. Podpisem objęte jest całe Body komunikatu oraz sekcja Timestamp.

5.11 Obsługa błędów związanych z przetwarzaniem EDM w profilu XDS.b

Kategorie błędów zwracanych przez interfejs XDS.b:

1. Błędy na poziomie warstwy TLS, np. nieprawidłowy lub wygasły certyfikat uwierzytelniania systemu. Obsługa błędów poprzez wyjątki, np.: javax.net.ssl.SSLHandshakeException, opis błędu w języku angielskim.

2. Błędy na poziomie warstwy SOAP, np. nieprawidłowy XML, nieprawidłowy lub wygasły certyfikat douwierzytelniania danych. Obsługa błędów poprzez odpowiedź SOAP-ENV:Fault, opis błędu w języku angielskim.

3. Błędy na poziomie tokenu SAML

Na potrzeby generowania logów ATNA, oraz ewentualnego wykorzystania adaptera do systemu P1, wymagane jest dodanie do komunikatów XDS.b, tokenu SAML zawierającego m.in. informacje o autorze komunikatu. Brak lub błędny token skutkuje odpowiedzią SOAP-ENV:Fault o kodzie: wsse:FailedAuthentication

4. Błędy na poziomie XDS.b.

Błędy przekazywane są w ramach odpowiedzi RegistryResponse (lub AdHocQueryResponse). Element RegistryResponse posiada atrybut status, który może zawierać następujące wartości:

- urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success – żądanie zakończyło się sukcesem

- urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure – żądanie zakończyło się błędem

- urn:ihe:iti:2007:ResponseStatusType:PartialSuccess – żądanie zakończyło się częściowym sukcesem, dotyczy jedynie transakcji ITI-18 oraz ITI-43