INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

Centrum Systemów Informacyjnych Ochrony Zdrowia

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Część II - Opis przedmiotu zamówienia

Przedmiotem umowy jest Wykonanie Systemu Administracji oznaczone jako SA. (określanej dalej jako „System SA") dla Centrum Systemów Informacyjnych Ochrony Zdrowia w Warszawie.

Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych - Projekt P2

Projekt „Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych" ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007 – 2013 Dotacje na innowacje Inwestujemy w waszą przyszłość.

Centrum Systemów Informacyjnych Ochrony Zdrowia
ul. Stanisława Dubois 5A, 00-184 Warszawa
tel. +48(22) 597-09-27 fax +48(22) 597-09-47
biuro@csioz.gov.pl www.csioz.gov.pl

Spis Treści

I. *Wstęp*

Celem realizacji przedmiotu zamówienia jest dostarczenie systemu administracji na potrzeby projektu P2 („Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych"). System ma docelowo udostępniać usługi uwierzytelniania i podpisu elektronicznego na potrzeby systemów realizowanych w ramach projektów P1 (Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o zdarzeniach medycznych) i P2. Ponadto system ma udostępniać usługi autoryzacyjne na rzecz podsystemów realizowanych w projekcie P2.

A. Streszczenie menedżerskie

Niniejszy dokument zawiera zestaw wymagań funkcjonalnych i niefunkcjonalnych, które ma zawierać system będący przedmiotem zamówienia. Wykonawca w ramach realizacji zamówienia zobowiązany jest dostarczyć system spełniający wymienione w dokumencie wymagania oraz wszystkie jego niezbędne do poprawnego działania komponenty sprzętowe i programowe. W szczególności Wykonawca w ramach realizacji projektu zrealizuje następujące usługi zgodnie z zapisami niniejszego dokumentu.

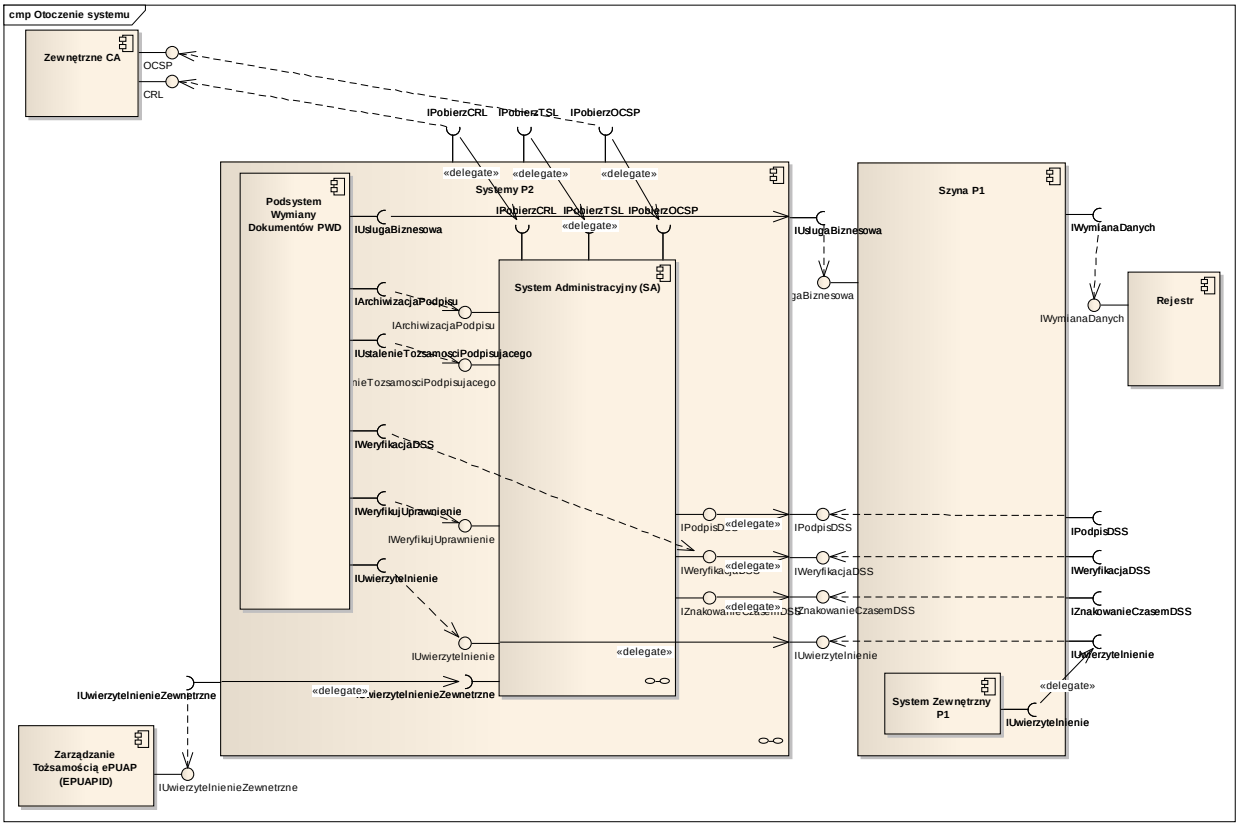
1. Przygotowanie projektu technicznego system
2. Dostarczenie sprzętu i licencji na oprogramowanie dla następujących środowisk:
   a) Środowisko produkcyjne – lokalizacja główna.
   b) Środowisko produkcyjne – lokalizacja zapasowa w serwerowni Zamawiającego.
   c) Środowisko testowe w serwerowni Zamawiającego.
   d) Środowisko szkoleniowe w serwerowni Zamawiającego.
   e) Środowisko rozwojowe w serwerowni Zamawiającego.
3. Zapewnienie tymczasowej lokalizacji głównej wraz z usługą późniejszego przeniesienia wszystkich komponentów systemu do docelowej lokalizacji głównej
4. Utrzymanie systemu w lokalizacji głównej
5. Świadczenie usługi wsparcia technicznego zgodnie z parametrami opisanymi w specyfikacji istotnych warunków zamówienia wraz z załącznikami w ilości 2 000 godzin
6. Uruchomienie i wdrożenie systemu w środowisku testowym, rozwojowym, szkoleniowym
7. Uruchomienie i wdrożenie systemu w środowisku produkcyjnym
8. Wspieranie Zamawiającego w przeprowadzeniu testów akceptacyjnych
9. Przeprowadzenie szkoleń użytkowników systemu.
10. Powykonawcza aktualizacja projektu technicznego.
11. Zapewnienie tymczasowej usługi tworzenia i odtwarzania kopii zapasowych
12. Aktualizację dokumentu „Architektura referencyjna rejestru medycznego" zgodnie z aktualnym projektem technicznym SA.

Definicja ośrodków przetwarzania danych:

1. Centralnym Ośrodku Przetwarzania Danych (COPD) - Ośrodek udostępniony przez Wykonawcę nazywany „lokalizacją główną"
2. Zapasowym Ośrodku Przetwarzania Danych (ZOPD - Ośrodek wskazany przez Zamawiającego nazywany „lokalizacją zapasową"

II. Otoczenie systemu

System musi współpracować z systemami realizowanymi w projekcie P1 w zakresie udostępniania usług uwierzytelnienia, usług składania i weryfikacji podpisu oraz znakowania czasem. System administracji musi udostępniać także na potrzeby podsystemów realizowanych w projekcie P2 usługi autoryzacyjne.



Rysunek 1 – Otoczenie systemu

Podsystem musi udostępniać możliwość uwierzytelnienia za pomocą mechanizmów udostępnianych przez system ePUAP, co powoduje konieczność współpracy na poziomie wymiany informacji dotyczących uwierzytelnienia użytkownika.
Konieczność weryfikacji certyfikatów wydawanych przez podmioty zewnętrzne (Zewnętrzne CA) sprawia, że od tych podmiotów muszą być pobierane informacje o ważności wydanych przezeń certyfikatów.
Otoczenie Systemu Administracji w ramach Systemu 2 będą stanowiły niżej opisane systemy.

A. Platforma Wymiany Dokumentów – wykorzystanie usług

Platforma Wymiany Dokumentów musi współpracować z Systemem Administracji, realizowanym w ramach projektu P2, w zakresie korzystania z usług uwierzytelniania i autoryzacji użytkowników oraz usług składania i weryfikacji podpisu oraz znakowania czasem.

B. System Centralne Zasoby Słownikowe – udostępnianie usług

System Centralne Zasoby Słownikowe (CSZ) zbudowany jest z dwóch podsystemów:

a) CZS intranet – podsystem służący do ładowania klasyfikacji medycznych z plików zewnętrznych oraz utrzymywania ich treści. Aktualna wersja systemu ma wbudowane struktury danych umożliwiające tworzenie powiązań pomiędzy klasyfikacjami medycznymi, które do systemu zostaną załadowane.

b) CZS ekstranet – portal udostępniania danych z klasyfikacji medycznych tak za pośrednictwem interfejsu użytkownika jak i usług webowych, na których ten interfejs użytkownika bazuje.

Aktualna wersja systemu CZS udostępnia wersję polską klasyfikacji ICD-10, utworzoną jako wynik tłumaczenia klasyfikacji ICD-10 z języka angielskiego oraz klasyfikację ICD-9 otrzymaną z NFZ, stosowaną do rozliczeń za usługi medyczne lub produkty lecznicze i wyroby medyczne.

Docelowo system CZS ekstranet ma udostępniać swoje usługi poprzez system Projektu P2 „Platforma udostępniania on-line przedsiębiorcom usług cyfrowych rejestrów medycznych".

ICD-10 jest to Międzynarodowa Klasyfikacja Chorób i Problemów Zdrowotnych opracowana przez WHO. ICD-9 jest to Międzynarodowa Klasyfikacja Procedur Medycznych.

System Centralne Zasoby Słownikowe jest wykonany w technologii Microsoft, w środowisku Visual Studio 2010, MS SQL 2008R2.

C. System Centralny Rejestr Produktów Leczniczych (CRPL) – udostępnianie usług

System CRPL stanowi baza danych CRPL, serwisy WebServices udostępniania danych oraz usługi rejestracji wniosków i ich obsługi. Baza danych CRPL jest raz dziennie zasilana z Rejestru Produktów Leczniczych Dopuszczonych do Obrotu z infrastruktury Urzędu Rejestracji Produktów Leczniczych.

System CRPL nie posiada własnego interfejsu użytkownika, a cała logika biznesowa, zaimplementowana w postaci serwisów WebServices ma być dostępna poprzez interfejs użytkownika Platformy Wymiany Dokumentów.

System Centralny Rejestr Produktów Leczniczych jest wykonany w technologii Microsoft, w środowisku Visual Studio 2010, MS SQL 2008R2.

D. Inne systemy rejestrowe – udostępnianie usług

Platforma Wymiany Dokumentów ma udostępniać usługi rejestrów medycznych, które udostępnią swoje usługi do tego celu. W ramach Projektu P2 mają być udostępnione usługi rejestrów podmiotowych znajdujących się na liście na końcu załącznika nr 1 do Studium Wykonalności.

Systemy rejestrowe mają udostępniać usługi w dwóch grupach funkcjonalnych:

a) Udostępnianie danych z rejestrów.

b) Wpis/zmiana w rejestrze.

E. Szyna usług w ramach P1

Usługi realizowane w Platformie Wymiany Dokumentów mają wykorzystać serwisy udostępniane przez Szynę Usług uruchomioną w ramach projektu P1

F. Obsługa wniosków/dokumentów dla P1

Jedną z usług udostępnianych przez PWD dla projektu P1 ma być możliwość złożenia dokumentu wykorzystując do tego Serwis udostępniony przez PWD.

G. Współpraca z systemami zewnętrznymi – ePUAP

W celu zapewnienia Interoperacyjności z systemem ePUAP PWD ma umożliwiać komunikację z wykorzystaniem formularzy systemu ePUAP.

III. Mapowanie planowanych komponentów oraz zadań systemu na poszczególne wymagania Studium Wykonalności Projektu P2.

Rezultaty oraz mapowanie wymagań zostało przygotowane na podstawie zapisów następujących dokumentów:

a) Studium Wykonalności dla projektu: Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych. Wersja 2.0, Warszawa, 10 kwietnia 2009 r.

b) Streszczenie Studium Wykonalności dla projektu: Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych Wersja 1.0, Warszawa, 17 grudnia 2009 r.

Rezultaty wdrożenia całego projektu P2		
Rezultat	**Nazwa**	**Opis**
R1	Umożliwienie elektronicznej rejestracji i aktualizacji danych rejestrowych	Implementacja rozwiązań informatycznych w ramach realizacji Projektu umożliwi podmiotom (dotyczyć to będzie w szczególności użytkowników rejestrów) dokonywanie elektronicznej rejestracji działalności w obszarze ochrony zdrowia i aktualizacji danych rejestrowych. Dla przedsiębiorców oznaczać to będzie przede wszystkim skrócenie czasu związanego z czynnościami rejestrowymi. Ponadto, dzięki udostępnieniu standardowych formularzy rejestracyjnych on-line, podmioty ubiegające się o rejestrację będą mogły jej dokonać niezależnie od miejsca przebywania. Dla organów rejestrowych rozwiązanie skutkować będzie poprawą obiegu dokumentów, możliwością szybkiej kontroli stanu rozpatrywania wniosków oraz bardziej efektywnym zarządzeniem procesem rejestracji.
R2	Umożliwienie pobierania odpisów i zaświadczeń drogą elektroniczną	Realizacja Projektu stworzy podmiotom funkcjonującym w obszarze ochrony zdrowia, przede wszystkim użytkownikom rejestrów, możliwość szybkiego dostępu do wymaganych zaświadczeń i wypisów z rejestrów podmiotowych. Możliwe będzie dotarcie do dokumentów niezależnie od aktualnego miejsca pobytu interesanta. Podmiotom prowadzącym rejestry podmiotowe realizacja Projektu pozwoli na obniżenie kosztów administracyjnych w związku z mniejszym obciążeniem osób zatrudnionych przy wydawaniu wypisów i zaświadczeń w formie papierowej.
R3	Umożliwienie administracji publicznej pobierania danych rejestrowych	Realizacja Projektu umożliwi administracji publicznej łatwiejszy i szybszy dostęp do danych rejestrowych, co wpłynie na ograniczenie kosztów administracyjnych związanych ze zbędnymi procedurami administracyjnymi w tym zakresie. Co więcej, ma zostać poprawiona efektywność wykorzystania danych rejestrowych przez administrację publiczną.
R4	Elektroniczne przechowywanie dokumentów	Wynikiem wprowadzenia rozwiązań informatycznych w ramach Projektu będzie umożliwienie organom rejestrowym przechowywania elektronicznej wersji dokumentów rejestrowych (w ramach elektronicznego archiwum) zgodnie z obowiązującymi w

		tym zakresie regulacjami System umożliwi łatwiejsze i szybsze dotarcie do materiałów archiwalnych zainteresowanym podmiotom. Ponadto, realizacja Projektu wpłynie korzystnie na bezpieczeństwo oraz efektywność przechowywania wersji elektronicznych dokumentów, w tym elektronicznych obrazów wersji papierowych. Skalowalność systemu umożliwi przechowywanie nawet bardzo dużej liczby dokumentów bez obniżenia wydajności i wygody obsługi.
R5	Upowszechnienie wykorzystania podpisu elektronicznego.	Zastosowane w ramach Projektu rozwiązania informatyczne pozwalające na wykorzystanie podpisu elektronicznego wpłyną na uproszczenie czynności administracyjnych związanych z procesem rejestracji działalności zarówno dla przedsiębiorców funkcjonujących w ramach obszaru ochrony zdrowia, jak również podmiotów zajmujących się administrowaniem ich działalności. Dzięki upowszechnieniu wykorzystania podpisu cyfrowego stworzony zostanie nowy kanał komunikacji, który umożliwi zarówno przedsiębiorcom jak i przedstawicielom administracji publicznej jednoznaczne uwiarygodnienie swoich danych osobowych. W konsekwencji spowoduje to rozszerzenie możliwości korzystania z usług e-administracji, a także pozwoli na szybsze i prostsze załatwianie spraw związanych z rejestracją działalności drogą elektroniczną.

Mapowanie wymagań dla całego projektu P2			
Rezultat	**Wymaganie ze Studium Wykonalności projektu P2**	**Opis szczegółowy**	**Zakres realizacji przez System Administracji**
R1	Wsparcie dla kluczowych czynności związanych z obsługą rejestrów	Realizowany w ramach Projektu system informatyczny dostarczy narzędzi wspierających realizację kluczowych czynności związanych z obsługa rejestrów, takich jak: • czynności związane z uzyskaniem dostępu do rejestru, • czynności związane z uzyskaniem wpisu do rejestru, • czynności związane z modyfikacją istniejącego w rejestrze wpisu, • czynności związane z uzyskaniem odpisu z rejestru bądź zaświadczenia o wpisaniu do rejestru, • czynności związane z usunięciem istniejącego wpisu z rejestru, • czynności związane z uzyskiwaniem danych rejestrowych przez jednostki administracji publicznej, zarówno po stronie użytkownika rejestru, jak i po stronie właścicieli rejestrów.	Wspiera w zakresie: 1. Uwierzytelnienia, 2. Zarządzania uprawnieniami.
R1, R5	Funkcjonalności	Wypełnianie, podpisywanie i składanie	Wspiera w zakresie:

	podstawowe – obsługa przedsiębiorców	elektronicznych wniosków, w szczególności dotyczących: • rejestracji (wpisu do rejestru), • aktualizacji danych dotyczących danego podmiotu, • usunięcia z rejestru wpisu dotyczącego danego podmiotu. Wdrażane rozwiązanie pozwoli przedsiębiorcom na przygotowanie i podpisanie elektronicznych wniosków zarówno w trybie on-line, przy użyciu oferowanej przez Platformę aplikacji on-line, dostępnej za pośrednictwem przeglądarki internetowej, jak i w trybie off-line, przy użyciu instalowanej na komputerze przedsiębiorcy aplikację pozwalającą na wypełnienie, podpisanie i wysłanie wniosku.	1. Podpisywania wiadomości i weryfikacji złożonych podpisów,
R1	Śledzenie statusu realizacji spraw.	Funkcjonalności Platformy pozwolą wnioskodawcom na sprawdzenie statusu realizacji sprawy. W systemie zaimplementowana zostanie także funkcja automatycznego powiadamiania wnioskodawcy o stanie realizacji sprawy.	Wspiera w zakresie: 1. Uwierzytelnienia, 2. Zarządzania uprawnieniami.
R1	Uiszczanie elektronicznych płatności.	Proces składania elektronicznych wniosków może obejmować dokonywanie elektronicznych płatności. W celu umożliwienia przedsiębiorcom uiszczania elektronicznych płatności, platforma będzie umożliwiać korzystanie z możliwie szerokiej gamy kanałów płatności elektronicznych.	Wspiera w zakresie: 1. Podpisywania wiadomości.
R1	Obsługa wniosków	Przy użyciu wdrażanego rozwiązania, wnioskodawca będzie mógł przygotować i podpisać elektroniczny wniosek w dwóch trybach: • poprzez aplikację on-line dostępną za pośrednictwem przeglądarki internetowej, • poprzez instalowaną na stacji roboczej aplikację pozwalającą na wypełnienie, podpisanie i wysłanie wniosku. Dodatkowo zakładana jest możliwość wprowadzania wniosków wypełnianych przez wnioskodawcę w formie papierowej.	Wspiera w zakresie: 1. Weryfikacji złożonych podpisów i certyfikatów.
R3	Obsługa jednostek administracji publicznej	W ramach Platformy udostępnione także zostaną narzędzia umożliwiające jednostkom administracji publicznej dostęp do danych rejestrów podmiotowych. Analogicznie jak w przypadku przedsiębiorców, funkcjonalności Platformy pozwolą jednostkom administracji publicznej na składanie elektronicznych wniosków, pozwalających na otrzymanie żądanych informacji z rejestrów podmiotowych.	Wspiera w zakresie: 1. Uwierzytelnienia, 2. Zarządzania uprawnieniami. 3. Weryfikacji złożonych podpisów i certyfikatów.

		Informacje te będą mogły być przesyłane przez organy rejestrowe w formie elektronicznej, przy użyciu Platformy. Docelowo, w miarę dostosowywania i integracji z Platformą kolejnych rejestrów podmiotowych, funkcjonalności Platformy pozwolą jednostkom administracji publicznej na przeglądanie i pobierania danych rejestrowych w trybie on-line.	
R4	Funkcjonalności systemowe - archiwizacja dokumentów elektronicznych	Projekt obejmuje budowę elektronicznego archiwum dokumentów, w którym gromadzone będą wszystkie dokumenty elektroniczne przekazywane za pośrednictwem Platformy. Przechowywanie takiej dokumentacji jest niezbędne dla zapewnienia wiarygodności danych w rejestrach ochrony zdrowia. Dokumenty gromadzone w elektronicznym archiwum będą zawierały podpisy elektroniczne oraz znaczniki czasu, które umożliwią wiarygodną identyfikację autorów tych dokumentów i czasu ich powstania. Dzięki konserwacji podpisów elektronicznych, możliwe będzie utrzymanie wiarygodnej wartości dowodowej składowanych w nim dokumentów. Forma archiwum umożliwi elektroniczny sposób realizacji całego procesu związanego z obsługą rejestrów (wpis, aktualizacja, usunięcie wpisu, pobranie odpisu) oraz pozwoli na osiągnięcie oszczędności dzięki odejściu od tradycyjnej archiwizacji dokumentów papierowych.	Wspiera w zakresie: 1. Weryfikacji złożonych podpisów i certyfikatów. 2. Uzyskania postaci archiwalnej podpisu.
R3	Funkcjonalności systemowe - wykorzystanie danych zawartych w rejestrach referencyjnych	W celu zapewnienia spójności i zgodności danych rejestrowych, realizowana w ramach Projektu Platforma będzie zintegrowana z rejestrami referencyjnymi, w szczególności z systemami rejestrów PESEL, REGON, TERYT, m.in. w zakresie weryfikacji z tymi rejestrami danych, zawartych w składanych wnioskach. W zakresie integracji realizowanego w ramach Projektu rozwiązania z rejestrami referencyjnymi możliwe będzie wykorzystanie platformy ePUAP.	Wspiera w zakresie: 1. Uwierzytelnienia, 2. Zarządzania uprawnieniami.
R5	Bezpieczeństwo - zapewnienie bezpiecznego uwierzytelnienia oraz niezaprzeczalności informacji	Z punktu widzenia ryzyka utraty poufności oraz integralności przetwarzanych danych rejestrowych, istotne jest zapewnienie następujących elementów bezpieczeństwa: uwierzytelnienia, autoryzacji oraz rozliczalności. W wyniku realizacji Projektu (oraz powiązanego projektu P1 – w zakresie	System Administracji: 1. Podsystem Raportowania i Logowania 2. Podsystem Zarządzania Tożsamością

		elementów podsystemu zarządzania zabezpieczeniami i prywatnością) stworzony zostanie mechanizm uwierzytelniania użytkowników całości rozwiązania, realizowanego w ramach projektów P1 oraz P2, oparty na wykorzystaniu podpisu elektronicznego. Rozwiązanie to umożliwi bezpieczne uwierzytelnienie w samej Platformie oraz autoryzowany dostęp do danych rejestrowych. Podpis elektroniczny posłuży również do podpisywania składanych przy użyciu Platformy wniosków i wydawanych wypisów czy zaświadczeń, co przy zastosowaniu znakowania czasem umożliwi niezaprzeczalność złożenia wniosków w określonym czasie. System umożliwi również rozliczalność użytkowników, a w szczególności administratorów rozwiązania za wykonane w systemie działania. Dodatkowo bezpieczeństwo danych rejestrowych będzie zapewnione przez ich szyfrowanie, zarówno podczas transmisji, jak również w miejscu ich przechowywania na nośnikach danych.	3. Podsystem Zarządzania Uprawnieniami 4. Podsystem Podpisu Elektronicznego Wspiera w zakresie: 1. Uwierzytelnienia, 2. Zarządzania uprawnieniami. 3. Weryfikacji złożonych podpisów i certyfikatów. 4. Rejestracji zdarzeń.
R2	Integracja z ePUAP oraz z rejestrami referencyjnymi	W celu zachowania spójności z projektowanym przez Ministerstwo Spraw Wewnętrznych i Administracji modelem elektronicznych usług administracji publicznej (zgodnie z założeniem zastosowania zaleceń i wytycznych MSWiA), wdrażane w ramach Projektu rozwiązania będą zintegrowane z platformą ePUAP, realizowaną w ramach projektów ePUAP oraz ePUAP 2. Rezultatem projektu ePUAP 2 będzie uruchomienie platformy, na której udostępniane będą obywatelowi usługi elektroniczne budowane przez instytucje publiczne. Platforma ePUAP będzie umożliwiała w przyszłości definiowanie kolejnych procesów obsługi obywatela i przedsiębiorstw, tworzenie kanałów dostępu do poszczególnych systemów administracji publicznej oraz rozszerzenie zestawu usług publicznych świadczonych elektronicznie. Zakres projektu ePUAP obejmuje budowę platformy, Centralnego Repozytorium Wzorów Dokumentów, portalu informacyjnego ePUAP oraz portalu interoperacyjności. W wyniku integracji rozwiązań wdrażanych w ramach Projektu z platformą ePUAP,	Wspiera w zakresie: 1. Uwierzytelnienia, 2. Weryfikacji złożonych podpisów i certyfikatów.

		możliwe będzie uwierzytelnienie użytkowników wdrażanego rozwiązania za pośrednictwem tej platformy na potrzeby autoryzacji dostępu do aplikacji online, udostępnionych w ramach Platformy. Rozwiązania wdrażane w ramach Projektu będą także mogły być zintegrowane z platformą ePUAP w następujących obszarach: • skrzynka podawcza (Urzędowe Poświadczenie Przedłożenia, Urzędowe Poświadczenie Doręczenia), • usługi dokumentowe (tworzenie, udostępnianie formularzy, tworzenie elektronicznych dokumentów), • dostęp do rejestrów publicznych (walidacje formularzy), • usługi komunikacyjne (przesyłanie dokumentów elektronicznych), • usługi bezpieczeństwa (utrzymanie kont użytkowników, zapewnienie bezpieczeństwa i niezaprzeczalności komunikacji), • usługi płatności elektronicznych. Integracja wdrażanego rozwiązania z ePUAP będzie następować w miarę udostępniania usług w wymienionych wyżej obszarach przez ePUAP.	

IV. Wymagania

1. Wymagania funkcjonalne określają zakres działania dla poszczególnych elementów systemu i są szczegółowo opisane w rozdziale V- Specyfikacja systemu. Rolą wymagań niefunkcjonalnych jest wskazanie warunków realizacji poszczególnych funkcjonalności.
2. Wymagania niefunkcjonalne mają istotny wpływ na architekturę systemu. Poniżej opisano charakterystykę każdego wymagania:
   a) Wymagania wydajnościowe, determinują liczbę i rozmieszczenie urządzeń obsługujących poszczególne usługi.
   b) Wymagania dotyczące dostępności i ciągłości działania opisują zastosowanie odpowiednich mechanizmów umożliwiających unikanie, bądź niwelowanie skutków awarii.
   c) Wymagania dotyczące skalowalności wymuszają stosowanie środków takich jak partycjonowanie danych, lub rozkładanie obciążenia.
   d) Wymagania dotyczące bezpieczeństwa określają sposoby zabezpieczania poszczególnych komponentów systemu.
   e) Wymagania dotyczące komunikacji determinują stosowanie wymienionych protokołów oraz ich wersji.
   f) Wymagania utrzymania określają przede wszystkim sposoby zapewnienia odzyskania danych w przypadku wystąpienia awarii.
   g) Wymagania dotyczące szkoleń wymuszają przeszkolenie zarówno zespołu projektowego jak i osób zajmujących się docelowo administracją i utrzymaniem sytemu.
   h) Wymagania na środowiska testowe, rozwojowe i szkoleniowe wymuszają stworzenie środowiska o parametrach odpowiadających środowisku produkcyjnemu
   i) Wymagania dotyczące licencjonowanie określają sposoby użytkowania i rozszerzania praw związanych z wykorzystywanym oprogramowaniem
   j) Wymagania dotyczące dokumentacji determinują zasady tworzenia i przekazywania dokumentacji technicznej związanej z realizowanym projektem
3. Lista wymagań dla systemu P2 została przygotowana z uwzględnieniem i w zgodzie z wymaganiami nałożonych na system P1 zdefiniowanymi w opracowaniu „Projekt koncepcyjny, część 2. Model Systemu. Wymagania funkcjonalne i pozafunkcjonalne" z dnia 26 października 2010r.
4. W wyliczeniach wymagań wydajnościowych i dostępności uwzględniono zapisy rozdziału 11.2.3 - Studium Wykonalności dla projektu: Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych. Wersja 2.0, Warszawa, 10 kwietnia 2009 r.

Ogólne wymagania funkcjonalne dotyczące bezpieczeństwa

Identyfikator	**Wymaganie**
WF.ODS.1	System, do ochrony poufności i integralności informacji zawartych w systemie, wykorzystując funkcje skrótu i algorytmy szyfrowania powinien stosować zalecenia standardu ETSI TS 102 176.
WF.ODS.2	System musi zapewniać ochronę poufności i integralności przesyłanych informacji pomiędzy współpracującymi komponentami i systemami.

WF.ODS.3	System musi zapewniać ochronę integralności informacji gromadzonych w podsystemie raportowania i logowania (PRL) dotyczących zdarzeń zachodzących w innych podsystemach wchodzących w skład platformy P2.
WF.ODS.4	System powinien umożliwić dostęp do zasobów chronionych oraz wykonanie chronionej operacji wyłącznie po poprawnej identyfikacji i uwierzytelnieniu użytkownika.

A. Wydajność

Identyfikator	Wymaganie
WNF.WYD.1	Rozwiązanie ma zapewnić wydajność systemu pod kątem następujących parametrów na nie mniejszym poziomie niż: Liczba poprawnych odpowiedzi udzielanych na zapytania o możliwość uwierzytelnienia się w ciągu jednaj sekundy dla każdego z rodzajów uwierzytelnień – 75
WNF.WYD.2	Rozwiązanie ma zapewnić wydajność systemu pod kątem następujących parametrów na nie mniejszym poziomie niż: Liczba poprawnych odpowiedzi udzielanych na zapytania o poprawność złożonego podpisu w ciągu jednej sekundy –190
WNF.WYD.3	Rozwiązanie ma zapewnić wydajność systemu pod kątem następujących parametrów na nie mniejszym poziomie niż: Liczba poprawnych odpowiedzi udzielanych na zapytania OCSP o status certyfikatu w ciągu jednej sekundy - 460
WNF.WYD.4	Rozwiązanie ma zapewnić wydajność systemu pod kątem następujących parametrów na nie mniejszym poziomie niż: Liczba automatycznie, poprawnie utworzonych podpisów w formacie XAdES-A w ciągu jednej sekundy dla długość klucza min 1024 bity– 380
WNF.WYD.5	Rozwiązanie ma zapewnić wydajność systemu pod kątem następujących parametrów na nie mniejszym poziomie niż: Liczba poprawnie generowanych znaczników czasu z wykorzystaniem klucza min. 1024 bity w ciągu jednej sekundy –200 dla każdego z obu wariantów (RFC i DSS)
WNF.WYD.6	Rozwiązanie przy zakładanej liczbie kont użytkowników (45 mln.) ma zapewnić wydajność systemu pod kątem następujących parametrów na poziomie: Czas odpowiedzi na pojedyncze zapytanie polegające na poprawnym wyszukaniu tożsamości ma wynosić mniej niż jedna sekunda dla: • Wyszukania tożsamości po identyfikatorze • Wyszukania tożsamości na podstawie wybranego atrybutu konta (PESEL/numer paszportu, imię/nazwa systemu, nazwisko, e-mail)
WNF.WYD.7	Rozwiązanie ma zapewnić wydajność systemu pod kątem następujących parametrów na nie mniejszym poziomie niż: Liczba poprawnie generowanych odpowiedzi autoryzacyjnych w ciągu jednej sekundy - 190

B. Dostępność

Identyfikator	Wymaganie
WNF.DOS.1	System ma zapewniać utrzymanie ciągłości działania na poziomie 99,9 %, dla wszystkich usług łącznie w skali roku. Przeniesienie świadczenia usług do ośrodka zapasowego nie może zmniejszyć poziomu bezpieczeństwa świadczonych usług
WNF.DOS.2	Czas niedostępności usługi realizującej uwierzytelnianie i autoryzację. Łączny czas niedostępności systemu w wymienionym zakresie nie może być większy niż 8 godz./rok.
WNF.DOS.3	Czas niedostępności usługi realizującej składanie i archiwizację podpisu Łączny czas niedostępności systemu w wymienionym zakresie nie może być większy niż 24 godz./rok.
WNF.DOS.4	Czas niedostępności usługi realizującej weryfikację podpisów Łączny czas niedostępności systemu w wymienionym zakresie nie może być większy niż 12 godz./rok.
WNF.DOS.5	Czas niedostępności usługi generującej znaczniki czasu Łączny czas niedostępności systemu w wymienionym zakresie nie może być większy niż 12 godz./rok
WNF.DOS.6	Czas niedostępności usługi udzielającej odpowiedzi OCSP Łączny czas niedostępności systemu w wymienionym zakresie nie może być większy niż 12 godz./rok
WNF.DOS.7	System ma mieć architekturę wysokiej dostępności, czyli wymienione poniżej elementy powinny być redundantne w ramach jednego serwera: • Zasilacz sieciowy
WNF.DOS.8	Architektura systemu ma umożliwiać wykorzystanie systemu w dwóch lokalizacjach: • Centralnym Ośrodku Przetwarzania Danych (COPD), • Zapasowym Ośrodku Przetwarzania Danych (ZOPD) • w trybie Active-Active (Hot Site)
WNF.DOS.9	Przełączenie przetwarzania z COPD na ZOPD i odwrotnie ma być możliwe bez utraty integralności danych.
WNF.DOS.10	Rozwiązanie COPD i ZOPD ma być transparentne z poziomu szyny usług SIOZ
WNF.DOS.11	W przypadku awarii pojedynczej lokalizacji powinna być zapewniona dostępność wszystkich realizowanych przez system funkcjonalności.
WNF.DOS.12	Konfiguracja systemu ma umożliwiać przełączenie ośrodków w czasie nie dłuższym niż 5 minut. Procedura przełączania ma ograniczać do minimum konieczność wpisywania danych przez Administratora. Dopuszcza się jedynie podawanie danych uwierzytelniających i wykonywanie wcześniej przygotowanych skryptów.
WNF.DOS.13	Wykonawca zapewni usługę kompleksowego przeniesienia tymczasowej lokalizacji głównej do docelowej lokalizacji głównej wskazanej przez Zamawiającego. Czas przeniesienia nie może być

Identyfikator	Wymaganie
	dłuższy niż 30 dni od daty wskazania docelowej lokalizacji.
WNF.DOS.14	System musi wystawić interfejsy umożliwiające wykorzystanie zewnętrznego systemu kopii bezpieczeństwa (system P1)
WNF.DOS.15	Wykonawca ma zapewnić bezpieczne przechowywanie kopii zapasowych w innej lokalizacji niż dane zostały utworzone
WNF.DOS.16	System ma dostarczać aktualnych i kompletnych informacji o kopiach zapasowych i obowiązujących dla nich wersji procedur odtwarzania
WNF.DOS.17	System ma umożliwiać tworzenie kopii zapasowych w trybie pełnym
WNF.DOS.18	System ma umożliwiać tworzenie kopii zapasowych w trybie przyrostowym
WNF.DOS.19	System ma umożliwiać tworzenie kopii zapasowych w trybie różnicowym
WNF.DOS.20	System ma umożliwiać definiowanie harmonogramów wykonywania kopii zapasowych oraz wykonywać kopie zapasowe zgodnie ze zdefiniowanymi harmonogramami
WNF.DOS.21	System ma umożliwiać jego odtworzenie z wcześniej wykonanych kopii zapasowych
WNF.DOS.22	System ma umożliwiać testowanie kopii zapasowych
WNF.DOS.23	System ma umożliwiać tworzenie kopii zapasowych na urządzeniach umieszczonych w innej lokalizacji fizycznej.

C. Skalowalność

Identyfikator	Wymaganie
WNF.SKA.1	System ma zapewnić poprawne zarządzanie 45 milionami aktywnych kont użytkowników
WNF.SKA.2	System ma umożliwiać automatyzację zadań związanych z obsługą cyklu życia certyfikatów, np. pobieranie i aktualizacja w repozytorium list CRL i TSL
WNF.SKA.3	System ma zapewniać przechowywanie pełnej konfiguracji w sposób umożliwiający instalację nowego systemu i zasilenie go tą konfiguracją.
WNF.SKA.4	System ma mieć architekturę z możliwością łatwego skalowania wydajności poprzez dodawanie kolejnych instancji usług kluczowych dla zwiększenia wydajności.
WNF.SKA.5	System ma umożliwiać skalowalność poprzez uruchomienie kilku kopii usług kluczowych (TSP, OCSP, usług składania i archiwizacji podpisu, usług weryfikacji podpisu)

D. Komunikacja

Identyfikator	Wymaganie
WNF.KOM.1	System ma zapewnić wsparcie dla standardu przesyłania komunikatów SOAP z załącznikami (z kodowaniem komunikatów: "document/literal") w wersji 1.1 lub wyższej (http://www.w3.org/TR/soap/)
WNF.KOM.2	System ma umożliwiać przesyłanie komunikatów na poziomie protokołów transportowych: HTTP, HTTPS, MTOM, SMTP, DSS,

WNF.KOM.3	Do opisu struktury i semantyki usług sieciowych (web services) powinien zostać wykorzystany standard WSDL w wersji 1.X lub wyższej (http://www.w3.org/TR/wsdl20/)
WNF.KOM.4	Interfejsy usług mają być skonstruowane w taki sposób, aby narzędzia pracujące z WSDL (np. soapUI) mogły wygenerować poprawne składniowo żądanie dla usługi oraz dokonać walidacji odpowiedzi.
WNF.KOM.5	Do zbudowania rejestru usług sieciowych ma zostać zastosowany standard UDDI w wersji 3.X lub wyższej (http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm)
WNF.KOM.6	Do optymalizacji transportu danych w oparciu o protokół SOAP i technologię usług sieciowych ma zostać zastosowany standard MTOM (www.w3.org/TR/soap12-mtom)
WNF.KOM.7	Udostępniane WebService'y muszą być zgodne ze specyfikacjami: - WS-I Basic Profile w wersji 1.0 lub wyższej, - WS-Policy w wersji 1.5 lub wyższej, - WS-Security w wersji 1.0 lub wyższej;
WNF.KOM.8	Błędy działania WebService'u muszą być zwracane z wywołania jako komunikaty SOAP-Fault, o standardowej strukturze (XSD). Zakres i kody błędów powinny zostać uzgodnione na etapie opracowywania projektu technicznego.
WNF.KOM.9	Dla formatu podpisu XAdES moduł ma umożliwić złożenie podpisu za pośrednictwem interfejsu zgodnego ze specyfikacją OASIS Digital Signature Services w wersji 1.0. Dla pracy w trybie asynchronicznym należy stosować protokół: OASIS Digital Signature Service Asynchronous Profile 1.0
WNF.KOM.10	Obsługa żądań OCSP ma być realizowana zgodnie ze specyfikacją RFC 2560
WNF.KOM.11	Usługa znakowania czasem ma udostępniać swoją funkcjonalność zgodnie z: • RFC 3161 • OASIS DSS Timestamp Profile
WNF.KOM.12	Podsystemy zarządzania tożsamością i uprawnieniami mają korzystać z technologii SAML 2.0 i querystring

E. Tymczasowa lokalizacja główna utrzymywana przez Wykonawcę

Identyfikator	Wymaganie
WNF.LZ.1	Serwerownia ma być wyposażona w system kontroli dostępu ograniczający dostęp do Systemu Administracji wyłącznie do osób uprawnionych a ich obecność powinna być rejestrowana.
WNF.LZ.2	Serwerownia ma być wyposażona w system wykrywania włamania, pożaru i zalania umożliwiający przekazanie ostrzeżeń do odpowiedniego personelu ochrony.
WNF.LZ.3	Serwerownia ma gwarantować ciągłość i stabilność zasilania oraz poziom dostaw energii elektrycznej zgodny z potrzebami zaproponowanego rozwiązania.

WNF.LZ.4	Serwerownia ma posiadać system klimatyzacji zapewniający nieprzerwalne odprowadzenie ciepła w ilości zgodnej z potrzebami zaproponowanego rozwiązania.
WNF.LZ.5	W tymczasowej lokalizacji głównej Wykonawca ma zapewnić niezbędną ilość szaf rack 19”
WNF.LZ.6	W tymczasowej lokalizacji głównej Wykonawca ma zapewnić łącze gwarantujące spełnienie wymagań komunikacyjnych opisanych w przedmiocie zamówienia (przełączanie lokalizacji, synchronizacja danych)
LZ.7	Wykonawca zapewni kompleksową usługę utrzymania tymczasowej i docelowej lokalizacji głównej oraz lokalizacji zapasowej (czas trwania usługi do 31 grudnia 2012).

F. Sieć

Identyfikator	Wymaganie
WNF.NET.1	Polityka komunikacji pomiędzy Systemem Administracji a otoczeniem zewnętrznym ma być ograniczona do ruchu niezbędnego do realizacji wymaganych funkcjonalności.
WNF.NET.2	Otoczenie zewnętrzne może się komunikować z Systemem Administracji wyłącznie za pośrednictwem sprzętowych zapór sieciowych (firewall).
WNF.NET.3	Sieć wewnętrzna LAN ma być zbudowana z wykorzystaniem urządzeń zapewniających komunikację z prędkością minimum 1000 Mbit.
WNF.NET.4	Urządzenia zapór sieciowych mają zapewnić przepustowość minimum 1000 Mbit.
WNF.NET.5	Zapory sieciowe mają być wyposażone w mechanizm wykrywania zagrożeń (IPS) oparty o metody heurystyczne oraz sygnaturowe.
WNF.NET.6	Zapory sieciowe mają posiadać mechanizm powiadamiania osób uprawnionych o niepożądanych zdarzeniach w czasie rzeczywistym.
WNF.NET.7	Sieć LAN obsługująca System Administracji ma być podzielona na dwa segmenty „Frontend” i „Backend” rozdzielonych zaporą sieciową.
WNF.NET.8	W segmencie „Frontend” mają być zlokalizowane usługi dostępowe dla użytkowników.
WNF.NET.9	W segmencie „Backend” mają być zlokalizowane serwery które komunikują się między sobą oraz z otoczeniem zewnętrznym za pośrednictwem usług „frontend”.
WNF.NET.10	Urządzenia sieciowe mają umożliwiać tworzenie wydzielonych sieci wirtualnych w warstwie 2 i 3 modelu OSI.
WNF.NET.11	Połączenia mają Systemem Administracji a otoczeniem zewnętrznym mają być zabezpieczone za pomocą rodziny protokołów IPSEC w trybie tunelowym z wykorzystaniem certyfikatów lub współdzielonego klucza.
WNF.NET.12	Urządzenia aktywne sieci wewnętrznej oraz urządzenia brzegowe mają być redundantne w ramach pojedynczej lokalizacji. W przypadku awarii jednego z urządzeń ma zostać zachowana ciągłość funkcjonowania systemu.

WNF.NET.13	Wykonawca ma zapewnić redundantne łącze (w tymczasowej lokalizacji głównej) pomiędzy ośrodkiem podstawowym i zapasowym o przepustowości umożliwiającej replikację danych pozwalającą na zapewnienie poziomu aktualności danych niezbędnego do przełączenia ośrodka zgodnie z wymaganiami dostępności.
WNF.NET.14	Wykonawca zapewni redundantne łącze dostępowe do sieci Internet w tymczasowym ośrodku głównym o parametrach niezbędnych do realizacji zakładanych wymagań wydajnościowych i dostępności.
WNF.NET.15	W ciągu dwóch tygodni od podpisania umowy na realizację projektu budowy Systemu Administracji, Wykonawca opracuje specyfikację wymagań dla łącza internetowego niezbędnego do funkcjonowania Systemu Administracji..
WNF.NET.16	W ramach wynagrodzenia wykonawca zapewni przełączanie systemu w ośrodku podstawowym z tymczasowego łącza internetowego na łącze docelowe udostępnione przez zamawiającego.
WNF.NET.17	Wszystkie urządzenia sieciowe mają być wyposażone w uchwyty mocujące rack.
WNF.NET.18	Wykonawca w ramach wynagrodzenia skonfiguruje zapory sieciowe do obsługi niezbędnego ruchu dla systemu PWD budowanego w ramach projektu P2.
WNF.NET.19	Wykonawca dostarczy minimum **4 sprzętowe zapory sieciowe** do każdej lokalizację.
WNF.NET.20	Wykonawca dostarczy minimum **2 sprzętowe przełączniki sieciowe** do każdej lokalizacji.
WNF.NET.21	Wykonawca ma przewidzieć po **4 wolne porty** Ethernet do podłączenia przełączników systemu PWD zarówno w segmencie „Frontend” jak i „Backend”.

G. System antywirusowy

Identyfikator	**Wymaganie**
WNF.AV.1	Wykonawca zapewni bezpłatny system ochrony antywirusowej dla Systemu Administracji przez **cały okres trwania serwisu gwarancyjnego** z możliwością przedłużenia o kolejne lata
WNF.AV.2	W ciągu dwóch tygodni od podpisania umowy na realizację projektu budowy Systemu Administracji, Wykonawca razem z Zamawiającym opracuje specyfikację wymagań niezbędnych do realizacji usług ochrony antywirusowej dla Systemu Administracji poza Systemem Administracji.
WNF.AV.3	W ramach wynagrodzenia wykonawca zapewni migrację procesów obsługi ochrony antywirusowej do usług obsługi ochrony antywirusowej wskazanej przez Zamawiającego oraz dostosuje odpowiednie procedury bezpiecznej eksploatacji i przeprowadzi niezbędne prace instalacyjne.
WNF.AV.4	System antywirusowy musi obejmować swoim zasięgiem wszystkie stacje robocze dostarczone w ramach zamówienia oraz serwery Systemu Administracji.
WNF.AV.5	System antywirusowy ma umożliwiać centralne zarządzanie oprogramowaniem antywirusowym znajdującym się na serwerach.
WNF.AV.6	System antywirusowy ma umożliwiać definiowanie działań podejmowanych wobec podejrzanych plików.

H. Backup

Identyfikator	Wymaganie
WNF.BA.1	W ciągu dwóch tygodni od podpisania umowy na realizację projektu budowy Systemu Administracji, Wykonawca razem z Zamawiającym opracuje specyfikację wymagań niezbędnych do realizacji usług obsługi kopii zapasowych poza Systemem Administracji.
WNF.BA.2	W ramach wynagrodzenia wykonawca zapewni migrację procesów tworzenia kopii zapasowych do usług obsługi kopii zapasowych wskazanej przez Zamawiającego oraz dostosuje odpowiednie procedury bezpiecznej eksploatacji i przeprowadzi niezbędne prace instalacyjne.
WNF.BA.3	Do czasu migracji procesów obsługi kopii zapasowych do usług obsługi kopii zapasowych wskazanych przez Zamawiającego, Wykonawca zapewni własną usługę obsługi kopii.
WNF.BA.4	Kopie zapasowe mają być zabezpieczone przed modyfikacją.
WNF.BA.5	System ma umożliwiać szyfrowanie kopii zapasowych we wskazanym zakresie danych.

I. System monitorowania

Identyfikator	Wymaganie
WNF.BA.1	Wykonawca zapewni centralny system monitorowania parametrów pracy wszystkich urządzeń sieciowych i systemów komputerowych.
WNF.BA.2	System monitorowania ma w czasie rzeczywistym informować upoważnione osoby o zakłóceniach pracy monitorowanych komponentów.
WNF.BA.3	System monitorowania ma umożliwiać generowanie raportów obrazujących stan monitorowanych parametrów.
WNF.BA.4	System monitorowania ma na bieżąco prezentować stan monitorowanych parametrów w sposób graficzny, na ekranie dedykowanej stacji roboczej.

J. Szkolenia

Identyfikator	Wymaganie
WNF.SZK.1	Wykonawca ma zapewnić szkolenia dla dwóch grup pracowników Zamawiającego: • członków zespołu projektowego, • administratorów systemu. Szkolenia muszą być przeprowadzone w siedzibie Zamawiającego. Zamawiający zapewnia dostęp do Internetu oraz sale szkoleniową.

WNF.SZK.2	Szkolenia dla minimum 3 członków zespołu projektowego od strony Zamawiającego w zakresie metodyk i narzędzi stosowanych przez Wykonawcę do budowy projektowanego systemu w szczególności: • budowy systemów teleinformatycznych, w ilości 5 dni, • analizy systemowej i modelowania, w ilości 3 dni, • specyfikacji wymagań, w ilości 3 dni, • narzędzi CASE, w ilości 3 dni.
WNF.SZK.3	Szkolenia dla administratorów systemu w zakresie: • zastosowanych przez wykonawcę systemów operacyjnych dla 2 osób/system w ilości 5 dni, • zastosowanych systemów bazodanowych dla 2 osób/system w ilości 5 dni, • zastosowanych systemów aplikacyjnych dla 2 osób/system w ilości 5 dni, • administrowania systemem dla 4 osób w ilości 3 dni, • zastosowanych zabezpieczeń (zapory sieciowe, ips, antywirus, itp.) dla 2 osób/zabezpieczenie w ilości 5 dni, • tworzenia kopii zapasowych oraz odtwarzania systemu po awarii dla 2 osób w ilości 5 dni, szkolenie powinno przewidywać wszystkie scenariusze zawarte w planach odtwarzania systemu po awarii. • zarządzania i konfiguracji urządzeń sieciowych, dla 2 osób w ilości 5 dni, • bieżącej obsługi zastosowanych maszyn, dla 2 osób/system w ilości 3 dni, • zastosowanego oprogramowania narzędziowego i programistycznego dla 2 osób w ilości 5 dni.
WNF.SZK.4	Jeden dzień szkolenia oznacza 8 godzin wykładowych (45-cio minutowych).

K. Środowiska testowe, rozwojowe i szkoleniowe

Identyfikator	Wymaganie
WNF.ŚROD.1	Wykonawca w ramach realizacji projektu dostarczy, oprócz systemu produkcyjnego również następujące środowiska: • Rozwojowe • Testowe • Szkoleniowe Środowiska zostaną uruchomione w lokalizacji zapasowej
WNF.ŚROD.2	Środowisko testowe musi stanowić dokładny model eksploatowanego Systemu Administracji.
WNF.ŚROD.3	Środowisko testowe musi umożliwić przeprowadzenie testów oprogramowania przed wdrożeniem w Systemie Administracji oraz przed zmianą konfiguracji już wdrożonych elementów oprogramowania.
WNF.ŚROD.4	Środowiska testowe, rozwojowe i szkoleniowe muszą być skalowalne i umożliwiać dołączenie nowych komponentów Systemu Administracji.
WNF.ŚROD.5	Środowiska testowe, rozwojowe i szkoleniowe mogą być wykonane w technologii maszyn wirtualnych.
WNF.ŚROD.6	Środowiska testowe, rozwojowe i szkoleniowe muszą być od siebie odseparowane.
WNF.ŚROD.7	Środowiska testowe, rozwojowe i szkoleniowe mogą korzystać z tych samych licencji oprogramowania jeśli nie narusza to praw autorskich stron trzecich. Przy założeniu, że będzie istniała możliwość uruchomienia wszystkich środowisk jednocześnie.

L. Licencjonowanie.

Identyfikator	Wymaganie
WNF.LIC.1	Wykonawca musi zapewnić ilość licencji na oprogramowanie standardowe w liczbie odpowiedniej dla zapewnienia działania Systemu Administracji w ośrodku podstawowym, zapasowym oraz środowisku testowym, rozwojowym i szkoleniowym. Oprogramowanie standardowe to każde oprogramowanie, które jest objęte gwarancją i licencją producenta oraz nie jest dostarczane wraz z kodem źródłowym i nie ma możliwości ingerencji w jego kod źródłowy.
WNF.LIC.2	Wykonawca musi wyposażyć **pięć stanowisk** komputerowych w oprogramowanie narzędziowe niezbędne do budowy Systemu Administracji dla członków zespołu projektowego oraz zapewnić odpowiednią liczbę licencji dla tego oprogramowania.
WNF.LIC.3	Wykonawca musi wyposażyć pięć stanowisk deweloperskich w oprogramowanie niezbędne do tworzenia oprogramowania dedykowanego dla Systemu Administracji zapewnić odpowiednią liczbę licencji dla oprogramowania deweloperskiego.

WNF.LIC.4	W zakresie dedykowanego oprogramowania dla Platformy Wymiany Dokumentów, Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe, prawo do wykonywania zależnych praw autorskich oraz prawo do zezwalania na wykonywanie zależnych praw autorskich na polach eksploatacji i w sposób określony w postanowieniach Wzoru umowy, stanowiącego załącznik nr 3 do SIWZ.
WNF.LIC.5	Wykonawca przekaże Zamawiającemu wszystkie wytworzone kody źródłowe i kody konfiguracji dedykowanego oprogramowania.
WNF.LIC.6	Wykonawca przenosi prawa własności do nośników, na których oprogramowanie zarówno dedykowane jak i standardowe jest utrwalone
WNF.LIC.7	Dedykowane oprogramowanie oznacza każde oprogramowanie niezbędne do funkcjonowania systemu z wyłączeniem oprogramowania standardowego.
WNF.LIC.8	Warunki licencji nie mogą ograniczać liczby stanowisk i użytkowników zewnętrznych (nie będących pracownikami Zamawiającego) korzystających z systemu
WNF.LIC.9	.Warunki licencji muszą umożliwiać pracę dla **minimum 300 pracowników** Zamawiającego(bez względu na podstawę nawiązania stosunku zatrudnienia i dysponowania pracownikiem) bez ograniczeń czasowych. Licencja nie może być wypowiedziana
WNF.LIC.10	Licencje nie mogą być ograniczone w czasie

M. Dokumentacja

Identyfikator	**Wymaganie**
WNF.DOK.1	Dokumentacja ma zostać dostarczona w postaci elektronicznej w formacie wskazanym przez Zamawiającego.
WNF.DOK.2	Wskazane przez wykonawcę składniki dokumentacji mają zostać dostarczone w formie papierowej w ilości egzemplarzy wskazanej przez Zamawiającego, jednak nie więcej niż 5 sztuk.

WNF.DOK.3	Dokumentacja architektoniczna i projektowa Systemu Administracji ma zawierać co najmniej: • opis koncepcyjny Systemu Administracji, • opis przypadków i scenariuszy użycia Systemu Administracji, • architekturę danych na etapie projektowym i powykonawczym, • architekturę aplikacji na etapie projektowym i powykonawczym, • architekturę fizyczną na etapie projektowym i powykonawczym, • architekturę bezpieczeństwa na etapie projektowym i powykonawczym, • projekt techniczny na etapie projektowym i powykonawczym. • opis środowisk testowego, rozwojowego, szkoleniowego i produkcyjnego zawierającego minimum: specyfikację sprzętu, specyfikację maszyn wirtualnych (jeśli zostaną użyte), specyfikację ilości sprzętu, specyfikację wymagań dla systemów operacyjnych i systemów bazodanowych, parametry eksploatacyjne.
WNF.DOK.4	Wykonawca ma dostarczyć plan, scenariusze, metodyki, zakresy, kryteria akceptacji i harmonogramy testów, z uwzględnieniem uwag Zamawiającego, w zakresie: • integracji z systemami zewnętrznymi w stosunku do Systemu Administracji, • akceptacji, • wydajności, • niezawodności, • dostępności, • bezpieczeństwa, • skalowalności. Zamawiający zastrzega sobie prawo przeprowadzenia własnych testów.
WNF.DOK.5	Wykonawca ma dostarczyć raporty z wykonania testów wraz z analizą spełnienia wymagań uwzględnionych w przypadkach testowych.

WNF.DOK.6	Testy mają być wykonane zgodnie z wymaganiami ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.) oraz rozporządzenia w sprawie testów akceptacyjnych (Dz. U. z 2005 r. Nr 217, poz.1836).
WNF.DOK.7	Dokumentacja techniczna ma zawierać: • dokumentację pakietów oprogramowania, • dokumentację baz danych, w tym konfigurację, schematy, procedury składowane i wyzwalacze, • konfiguracje systemów operacyjnych wykorzystanych do budowy Systemu Administracji, • dokumentację interfejsów i protokołów komunikacyjnych, • opis wdrożenia • dokumentację komunikatów wykorzystywanych przez System Administracji, • kody źródłowe rozwiązań wykonany w ramach niniejszego zamówienia wraz z listą pakietów, listą klas w poszczególnych pakietach, hierarchią klas w pakiecie, opisami pakietów, klas, interfejsów i metod wraz z parametrami, indeksem wszystkich klas, konstruktorów, pól i metod.
WNF.DOK.8	Wykonawca ma dostarczyć instrukcję instalacji i konfiguracji, umożliwiającą zbudowanie kompletnego i w pełni funkcjonalnego \Systemu Administracji opracowaną w języku polskim
WNF.DOK.9	Wykonawca ma dostarczyć czytelny i zrozumiały dokument polityki bezpieczeństwa zgodnej z ustawą o ochronie danych osobowych i rozporządzeniami wykonawczymi do ustawy.
WNF.DOK.10	Wykonawca ma dostarczyć podręcznik administratora Systemu Administracji opisujący zarządzanie wszystkimi komponentami i usługami.
WNF.DOK.11	Wykonawca ma dostarczyć plan ciągłości działania i plan odtwarzania systemu po awarii oraz procedury bezpiecznej eksploatacji zgodnie z załączoną Listą procedur bezpiecznej eksploatacji niniejszego dokumentu w zakresie systemu administracji.

WNF.DOK.12	Wykonawca ma dostarczyć podręcznik użytkownika Systemu Administracji zawierający: • zasady pracy w Systemie Administracji, • opis procesów biznesowych realizowanych w Systemie Administracji, • opis modułów, funkcji i ekranów dostępnych z poziomu użytkownika, • opis ról systemowych i uprawnień użytkownika, • instrukcję pomocy on-line
WNF.DOK.13	Przy tworzeniu dokumentacji technicznej Wykonawca zobowiązuje się korzystać z narzędzi typu CASE i notacji UML 2.0
WNF.DOK.14	Wykonawca musi zaktualizować dokumentację „Architektura referencyjna rejestru medycznego" o doświadczenie i zalecenia wynikające z wdrożenia PWD.

N. Minimalne wymagania dla serwerów

Identyfikator	**Wymaganie**
WNF.SRV.1	Wykonawca dostarczy na potrzeby realizacji przedmiotu zamówienia minimum **10 serwerów** montowanych w szafie rack wraz ze standardowymi, zamykanymi szafami RACK 19'' (minimum 2 sztuki).
WNF.SRV.2	Wykonawca musi zagwarantować, że dostarczane serwery umożliwiają spełnienie wszystkich wymagań wydajnościowych określonych w punkcie „A. Wydajność". Dodatkowo, poszczególne typy serwerów powinny osiągać wynik testu SPECint_base2006 na poziomie powyżej 35 punktów. Wykonawca może zaoferować inne rozwiązania sprzętowe niż te opublikowane na stronie http://www.spec.org/cpu2006/results/cpu2006.html pod warunkiem wykorzystania komponentów bazowych takich jak procesor/y i płyta główna tożsamych z konfiguracja która osiągnęła wynik testu SPECint_base2006 na poziomie powyżej 35 punktów.
WNF.SRV.3	Dostarczane przez Wykonawcę serwery muszą posiadać możliwość montowania zasilaczy i dysków twardych w trybie hot swap
WNF.SRV.4	Każdy serwer powinien być wyposażony w min. **2 redundantne zasilacze**
WNF.SRV.5	Wymiana, dodanie lub awaria pojedynczych dysków lub zasilaczy nie może powodować przerwy w pracy serwera.
WNF.SRV.6	Każdy serwer ma być wyposażony w płytę główną obsługującą min**. 2 procesory sześciordzeniowe**
WNF.SRV.7	Każdy serwer ma być wyposażony w minimum w **2 procesory** sześciordzeniowe. Wykonawca może zastosować procesowy o większej ilości rdzeni w zainstalowanych procesorach
WNF.SRV.8	Każdy serwer ma być wyposażony w min. 96GB pamięci RAM
WNF.SRV.9	Każdy serwer ma być wyposażony w min. **6 dysków twardych** typu hotswap o pojemności co najmniej 2TB każdy
WNF.SRV.10	Każdy serwer ma być wyposażony w sprzętowy kontroler RAID umożliwiający konfigurację następujących typów RAID: 0,1,5,10

WNF.SRV.11	Wielkość każdego serwera nie może przekraczać 2U, dołączone szyny do montażu w szafie RACK 19”.
WNF.SRV.12	Każdy serwer ma posiadać podsystem umożliwiający kontrolę poprawności działania elementów serwera, diagnostykę oraz narzędzie sprzętowe ułatwiające lokalizację uszkodzenia (np. świetlny wskaźnik uszkodzonego elementu);
WNF.SRV.13	Obsługiwane systemy operacyjne: Microsoft® Windows Server® 2003/2008 R2, Red Hat Enterprise Linux®, SUSE Linux Enterprise Server, VMware ESX Server
WNF.SRV.14	1. Wymagane warunki gwarancji: - świadczona w miejscu instalacji; - termin gwarancji biegnie od dnia podpisania przez Zamawiającego protokołu odbioru, **(zakończenia III - ostatniego etapu umowy)** bez zastrzeżeń - wszelkie koszty związane z naprawami gwarancyjnymi ponosi Wykonawca; Szczegółowe warunki świadczenia usługi serwisu gwarancyjnego (czas trwania, czasy reakcji, czas naprawy itp.) zostały zawarte w umowie świadczenia usług serwisowych stanowiącej załącznik do SIWZ

O. Gwarancja

Identyfikator	**Wymaganie**
WNF.GWA.1	Gwarancji podlega System Administracji oraz sprzęt komputerowy i telekomunikacyjny dostarczone przez Wykonawcę.
WNF.GWA.2	W ramach gwarancji Wykonawca jest zobowiązany do usunięcia na swój koszt wad całości lub części Systemu Administracji oraz naprawy lub wymiany sprzętu w przypadku jego awarii.
WNF.GWA.3	Okres gwarancji Systemu Administracji został określony w umowie na realizację systemu.
WNF.GWA.4	Okres gwarancji sprzętu komputerowego i telekomunikacyjnego został określony w umowie na realizację systemu.
WNF.GWA.5	W okresie do 31.12.2011 Wykonawca zapewni wsparcie technicznie świadczone na miejscu u Zamawiającego. Zamawiający w ramach oferowanej ceny może skorzystać z **2 000 godzin** pracy specjalistów wskazanych przez Wykonawcę jako osoby biorące udział w projekcie. Możliwe jest wskazanie przez Wykonawcę innych osób o ile ich doświadczenie jest takie sam lub większe.

P. Wymagania na projekt techniczny

Identyfikator	**Wymaganie**

WNF.PRT.1	Projekt techniczny ma zawierać: 1.Opis projektowanego systemu 2.Szczegółowy opis realizacji przypadków użycia 3. Model procesów biznesowych: • Model procesów biznesowych ma opisywać zachowanie i przepływ informacji w obrębie projektowanego systemu. • Model procesu powinien obejmować wejścia, wyjścia, zasoby, oraz kluczowe zdarzenia. 4. Model logiczny projektowanego systemu ma zawierać: • Opis struktury logicznej systemu wraz z podziałem na poszczególne moduły wchodzące w skład systemu • Sposób komunikacji między komponentami • Sposób komunikacji i współpracy z systemami zewnętrznymi • Opis komponentów logicznych projektowanego systemu oraz komponentów zewnętrznych 5. Model architektoniczny: • Opisujący sposoby realizacji poszczególnych komponentów logicznych. Dla każdego z komponentów przedstawione mają być przykładowe sposoby realizacji umożliwiające osiągnięcie zakładanej wydajności i dostępności. Dla poszczególnych komponentów wskazywane mają być także możliwe techniki skalowania. • Przykładowy model wdrożenia opisuje przykład wdrożenia zgodnego z zaprezentowaną architekturą 6. Model fizyczny projektowanego systemu ma zawierać: • Parametry i konfiguracje serwerów • Parametry i konfiguracje modułów i usług 7.Infrastruktura sieciowa ma zawierać: • Model współpracy z innymi systemami • Specyfikacja interfejsów • Opis algorytmów i protokołów komunikacyjnych • Model logiczny i fizyczny sieci. 8. Architektura bezpieczeństwa ma zawierać: • Identyfikację procesów i aktywów podlegających ochronie • Model zabezpieczeń dla każdego z modułów • Zabezpieczenia fizyczne, logiczne i organizacyjne • Sposób zapewnienia rozliczalności i audytu
	• Sposób realizacji archiwizacji danych

Q. Systemy zarządzania

Identyfikator	Wymaganie
WNF.SZ.1	Po zakończeniu wdrożenia Systemu Administracji Wykonawca przy współudziale Zamawiającego opracuje założenia zintegrowanego systemu zarządzania bezpieczeństwem informacji zgodnie z normą PN ISO/IEC 27001* przy uwzględnieniu norm PN-EN ISO 27799*, systemu zarządzania jakością usług zgodnie z normą PN ISO/IEC 20000* oraz systemu zarządzania ciągłością działania z uwzględnieniem norm BS 25999*, PN ISO/IEC 24762* oraz projektu ISO/IEC 22301*. *dopuszcza się rozwiązania równoważne do opisanych przenoszące normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego.
WNF.SZ.2	Wykonawca wdroży opisane w wymaganiu WBF.SZ.1 systemy.

R. Pozostałe

Identyfikator	Wymaganie
WNF.POZ.1	Wszelkie interfejsy operatora systemu (w tym również użytkownika) mają być przedstawione w języku polskim.
WNF.POZ.2	Wykonawca dostarcza wszystkie niezbędne do poprawnej pracy przedmiotu zamówienia elementy, takie jak: certyfikaty cyfrowe, przenośne pamięci masowe, karty i tokeny kryptograficzne, czytniki, itp. nie ujęte w wymaganiach funkcjonalnych i niefunkcjonalnych

V. Specyfikacja systemu

A. System Administracji (SA)

1. Do głównych zadań systemu administracji należy:
   a) uwierzytelnianie użytkowników na potrzeby wewnętrzne,

   b) uwierzytelnianie użytkowników na potrzeby systemów zewnętrznych,

   c) autoryzacja dostępu do zasobów wewnętrznych,

   d) weryfikacja podpisu elektronicznego,

   e) składanie podpisu elektronicznego,

   f) archiwizacja podpisu elektronicznego,

   g) znakowanie czasem,

   h) weryfikacja uprawnień do zasobów wewnętrznych na podstawie podpisanego dokumentu,

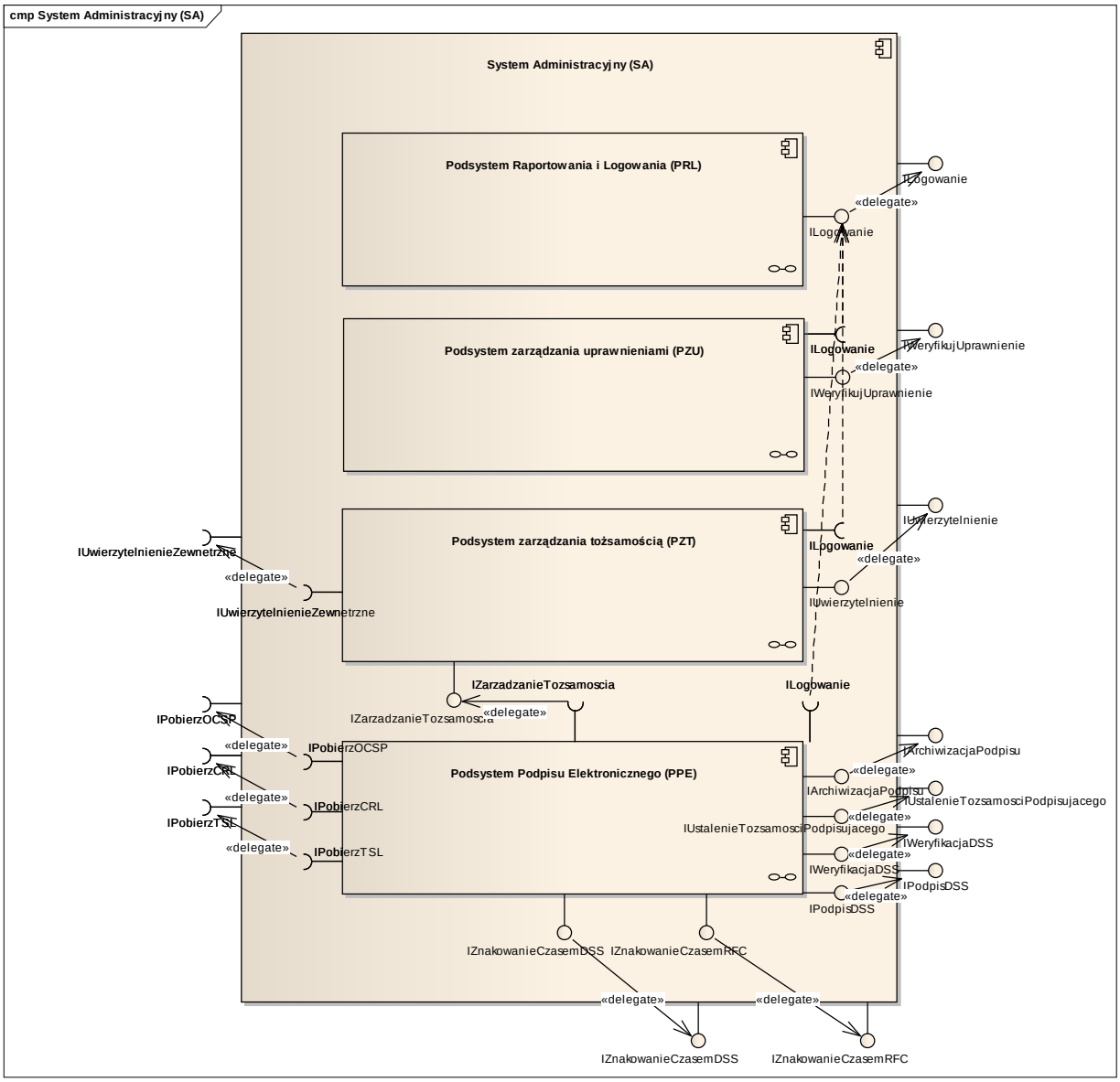
   i) zarządzanie użytkownikami.

2. System składa się z czterech głównych komponentów udostępniających na jego potrzeby interfejsy. Te komponenty to:
   a) podsystemu podpisu elektronicznego (PPE),

   b) podsystemu zarządzania tożsamością (PZT),

   c) podsystemu zarządzania uprawnieniami (PZU),

   d) podsystem raportowania i logowania (PRL).

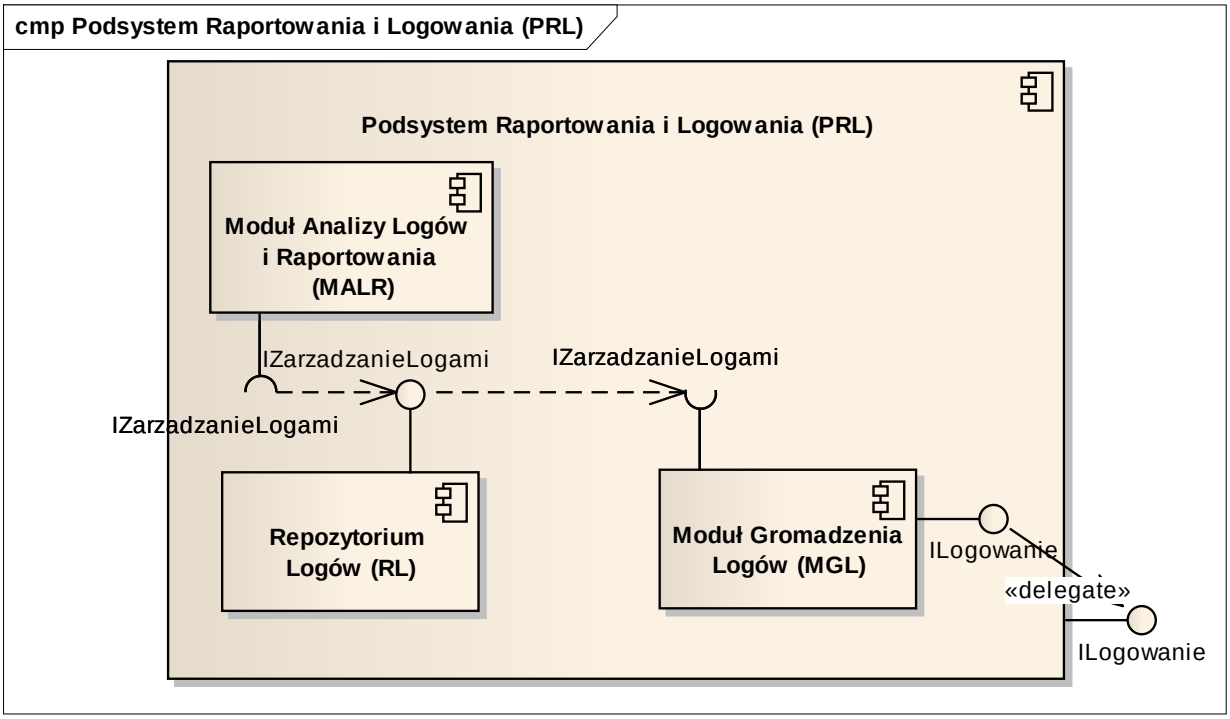


Rysunek 2 – System administracji

B. Podsystem Raportowania i Logowania (PRL)

Podsystem jest odpowiedzialny za gromadzenie informacji o zdarzeniach zachodzących w systemie administracji. Ma udostępniać na rzecz innych systemów realizowanych w ramach projektu P2 interfejs umożliwiający gromadzenie informacji o zachodzących w nich zdarzeniach.

W ramach podsystemu ma zostać także zrealizowany moduł pozwalający na tworzenie zaawansowanych raportów na podstawie zgromadzonych informacji.



Rysunek 3 – Podsystem raportowania i logowania

1. Moduł Analizy Logów i Raportowania (MALR)

Moduł Analizy Logów i Raportowania wchodzi w skład Podsystemu Raportowania i Logowania. Moduł ten jest odpowiedzialny za gromadzenie logów z podsystemów i ma umożliwiać generowanie raportów.

2. Moduł Gromadzenia Logów (MGL)

Moduł Gromadzenia Logów, wchodzący w skład Podsystemu Raportowania i Logowania odpowiada za zbieranie logów z komponentów systemu i umieszczanie ich w Repozytorium Logów.

3. Repozytorium Logów (RL)

Repozytorium logów będące składnikiem Podsystemu Raportowania i Logowania jest odpowiedzialne za archiwizowanie logów zbieranych przez Moduł Gromadzenia Logów

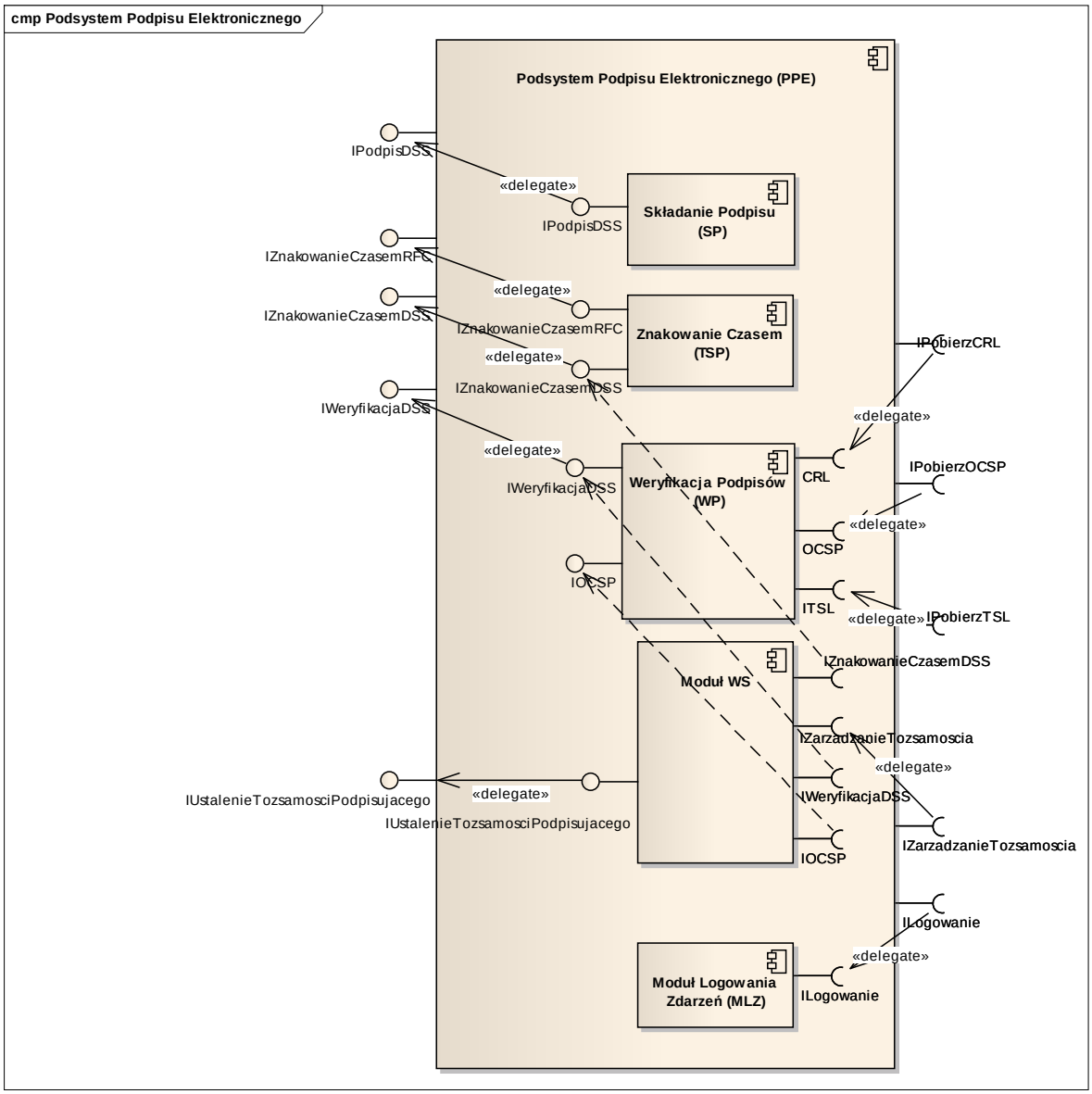
4. Zestawienie wymagań dla PRL

Identyfikator	Wymaganie
WF.PRL.1	System ma zapewnić mechanizm: • raportowania umożliwiający generowanie raportów na podstawie zadanych kryteriów. • automatycznego tworzenia raportów według predefiniowanych szablonów i zgodnie z określonym harmonogramem, • automatycznego wysyłania raportów do wskazanych użytkowników lub grup użytkowników.
WF.PRL.2	Podsystem ma zapewnić integralność zapisów związanych co najmniej: z użyciem tożsamości, zarządzania tożsamością i zapisów z procesu zarządzania uprawnieniami.
WF.PRL.3	Podsystem musi zapewnić audyt zapisów związanych z użyciem tożsamości, zarządzania tożsamością i zapisów z procesu zarządzania uprawnieniami.
WF.PRL.4	Podsystem ma zapewnić narzędzia do korelacji zdarzeń oraz wykrywania anomalii.
WF.PRL.5	Podsystem ma zapewnić mechanizmy automatycznego powiadamiania administratorów o wystąpieniu określonego przez administratora rodzaju zdarzenia i/lub źródła zdarzenia.
WF.PRL.6	Podsystem ma zapewnić metody archiwizacji zapisów z zastosowaniem mechanizmów zapewniających integralność zapisów.
WF.PRL.7	Wykonawca ma dostarczyć narzędzia umożliwiające analizę zapisów poza systemem. Narzędzia te mają zapewnić co najmniej taką samą funkcjonalność jak narzędzia wbudowane w system.
WF.PRL.8	System ma umożliwiać filtrowanie wyświetlanych zdarzeń według zadanych kryteriów. Minimalny zestaw kryteriów obsługiwanych przez PRL: • Data zdarzenia • Rodzaj operacji (logowanie, dodanie, modyfikacja, usunięcie) • Rodzaj zdarzenia (informacja, błąd,) • Identyfikator użytkownika

C. Podsystem Podpisu Elektronicznego (PPE)

a) Podsystem Podpisu Elektronicznego jest odpowiedzialny za czynności związane ze składaniem i weryfikacją podpisu elektronicznego. Zakres funkcjonalności podsystemu obejmuje także obsługę znaczników czasu.

b. Ze względu na konieczność obsługi podpisu kwalifikowanego, osobistego i profilu zaufanego konieczne jest pobieranie informacji o ważności certyfikatów od podmiotów zewnętrznych.



Rysunek 4 – Podsystem podpisu elektronicznego

c. Podsystem podpisu elektronicznego musi spełniać następujące wymagania:

Identyfikator	Wymaganie
WNF.PPE.1	Urządzenia HSM wykorzystywane przez podsystem mają wspierać algorytm RSA z długościami kluczy co najmniej 1024 bit i 2048 bit
WNF.PPE.2	Urządzenia HSM wykorzystywane przez podsystem mają wspierać funkcje skrótu SHA1, SHA256
WNF.PPE.3	Urządzenia HSM wykorzystywane przez podsystem mają umożliwiać przechowywanie co najmniej 5 kluczy kryptograficznych RSA o długości 2048 bit.
WNF.PPE.4	Urządzenia HSM wykorzystywane przez podsystem mają posiadać certyfikat poziomu CC EAL4+ albo FIPS 140-2 level 3.

WNF.PPE.5	Podsystem ma posiadać architekturę pozwalającą na skalowanie wydajności zgodnie z wymaganiami zawartymi w punkcie dot. usług kluczowych.
WNF.PPE.6	Podsystem ma posiadać mechanizmy wysokiej dostępności, pozwalające na jego pracę nawet w przypadku awarii dowolnego serwera obsługującego podsystem.
WNF.PPE.7	Usługa TSP nie może współdzielić urządzenia HSM z innymi usługami kluczowymi wchodzącymi w skład PPE.
WNF.PPE.8	Urządzenia HSM mają posiadać mechanizm zarządzania rolami i umożliwiać podział ról na co najmniej administratora i operatora.
WNF.PPE.9	Urządzenia HSM maja wspierać mechanizm kontroli dostępu za pomocą kart operatora i administratora.
WNF.PPE.10	Urządzenia HSM mają wspierać mechanizmy zarządzania pod podwójną kontrolą.
WNF.PPE.11	Urządzenia HSM maja umożliwić bezpieczny eksport kluczy
WNF.PPE.12	Urządzenia HSM mają umożliwić podział kluczy w schemacie progowym stopnia (m, n), gdzie wartość „m" wynosi co najmniej 2, natomiast n > m + 1.
WNF.PPE.13	Urządzenie HSM musi obsługiwać protokół PKCS#11 oraz CSP

1. Moduł usług sieciowych (WS)

1.1 Moduł WS jest komponentem wchodzącym w skład podsystemu podpisu elektronicznego.

1.2 Moduł ten jest odpowiedzialny za udostępnianie usług po interfejsie WebService:

a) ustalenie tożsamości w systemie zarządzania tożsamością na podstawie przekazanego podpisu

b) archiwizację podpisu realizowaną jako pojedyncze wywołanie usługi

1.3 Moduł WS musi spełniać następujące wymagania:

Identyfikator	**Wymaganie**
WF.WS.1	Moduł udostępnia usługę wykonania postaci archiwalnej podpisu dla podpisów w formatach XAdES, CAdES, PAdES
WF.WS.2	Moduł udostępnia funkcjonalność ustalenia identyfikatora użytkownika na podstawie podpisu, weryfikowanego pozytywnie przez usługę weryfikacji podpisu.
WF.WS.3	Moduł udostępnia funkcjonalność ustalenia danych użytkownika (imię, nazwisko, PESEL lub numer paszportu) na podstawie podpisu weryfikowanego zaufanym certyfikatem
WF.WS.4	Moduł umożliwia logowanie zdarzeń związanych z: * czynnościami administracyjnymi * uruchamianiem/zatrzymaniem usług
WF.WS.5	Moduł umożliwia przesyłanie logowanych zdarzeń do modułu logowania zdarzeń
WF.WS.6	Moduł udostępnia funkcjonalność ustalenia identyfikatora użytkownika na podstawie weryfikacji podpisu zrealizowanego z wykorzystaniem profilu zaufanego

WF.WS.7	Moduł udostępnia funkcjonalność ustalenia danych użytkownika (imię, nazwisko, PESEL, narodowość) na podstawie podpisu zrealizowanego z wykorzystaniem profilu zaufanego
WNF.WS.1	Moduł udostępnia usługi za pośrednictwem interfejsów WebService
WNF.WS.2	Moduł udostępnia usługi za pośrednictwem protokołów SOAP i HTTPS

2. Moduł składania Podpisu (SP)

2.1 Moduł składania podpisu jest komponentem podsystemu podpisu elektronicznego i odpowiada za udostępnianie interfejsu zgodnego ze standardem OASIS DSS umożliwiającego złożenie podpisu.

2.2 Moduł powinien umożliwiać:

a) Złożenie podpisu w formacie XAdES BES

b) Złożenie podpisu z wykorzystaniem kluczy kryptograficznych przechowywanych przez urządzenie HSM w ramach modułu

c) Złożenie podpisu na podstawie żądania zawierającego skrót z przesyłanego dokumentu

d) Złożenie podpisu na podstawie żądania zawierającego dokument

e) Złożenie kontrasygnaty do istniejącego podpisu

f) Złożenie podpisu równoległego

g) Rozbudowę modułu poprzez dokładanie kolejnych usług podpisu wykorzystujących te same, albo inne klucze kryptograficzne

h) Obsługę algorytmu RSA z długościami kluczy 2048bit

j) Obsługę funkcji skrótu SHA-1 oraz SHA256

2.3 Moduł składania podpisu musi spełniać następujące wymagania:

Identyfikator	**Wymaganie**
WF.SP.1	Moduł ma umożliwić złożenie dowolnego typu podpisu w formacie XAdES-BES i XAdES-EPES przy użyciu kluczy systemowych
WF.SP.2	Moduł ma obsługiwać możliwość wskazania kluczy służących do składania podpisu w ramach żądania generacji podpisu
WF.SP.3	Moduł ma umożliwić złożenie podpisu na podstawie przesłanej funkcji skrótu lub dokumentu
WF.SP.4	Moduł ma współpracować z urządzeniami do bezpiecznego przechowywania kluczy (HSM)z wykorzystaniem protokołu PKCS#11 lub CSP.

WF.SP.5	System ma umożliwiać logowanie zdarzeń związanych ze: • złożonymi podpisami • błędami podczas składania podpisu • uruchomieniem i zatrzymaniem usługi • czynnościami związanymi ze zmianą konfiguracji usługi
WF.SP.6	Moduł ma umożliwiać przesyłanie logowanych zdarzeń do modułu logowania zdarzeń
WF.SP.7	Moduł ma umożliwiać utworzenie archiwalnej wersji podpisu dla przesłanego podpisu w formacie XAdES, innym niż XAdES-A
WNF.SP.1	Moduł ma umożliwiać rozbudowę o dodanie kolejnych instancji usługi umożliwiających składanie podpisu elektronicznego
WNF.SP.2	Moduł ma umieć skorzystać z różnych kluczy kryptograficznych do składania podpisu
WNF.SP.3	Dla formatu podpisu XAdES moduł ma umożliwić złożenie podpisu za pośrednictwem interfejsu zgodnego ze specyfikacją OASIS Digital Signature Services w wersji 1.0
WNF.SP.4	moduł ma umożliwiać pracę w trybie asynchronicznym zgodnie z OASIS Digital Signature Service Asynchronous Profile 1.0
WNF.SP.5	Wykorzystanie asynchronicznego trybu pracy ma być możliwe co najmniej dla tworzenia archiwalnej postaci podpisu (XAdES-A)

3. Moduł weryfikacji podpisów (WP)

3.1 Moduł weryfikacji podpisów jest komponentem podsystemu podpisu elektronicznego i jest usługą typu VA (Validation Authority) umożliwiającą weryfikację podpisów. Usługa umożliwia weryfikację podpisów:

a) weryfikowanych certyfikatem kwalifikowanym

b) weryfikowanych certyfikatem podpisu osobistego

c) złożonych przy wykorzystaniu profilu zaufanego

3.2 Lista weryfikowanych podpisów ma być dynamicznie rozszerzana. Na potrzeby komponentu utrzymywane jest Repozytorium przechowujące informacje:

a) List certyfikatów unieważnionych CRL dla zdefiniowanych punktów zaufania

b) List certyfikatów usług zaufanych (TSL) dla zdefiniowanych punktów zaufania

3.3 W ramach komponentu uruchomione są usługi realizujące następujące funkcjonalności:

a) Pobranie list CRL z zewnętrznego źródła

b) Pobranie zaufanej listy TSL z zewnętrznego źródła

c) Udzielenie odpowiedzi OCSP na podstawie odpytania zewnętrznej usługi

d) Udzielenie odpowiedzi OCSP na podstawie zawartości Repozytorium

Repozytorium list CRL przechowuje w bezpieczny sposób pobrane listy CRL na podstawie, których udzielane są informacje o ważności certyfikatów użytkowników

Repozytorium list TSL odpowiedzialne jest za bezpieczne przechowywanie wpisów zawierających zaufane listy usług i urzędów CA (ang. Trusted-service Status List).

3.4 Moduł weryfikacji podpisu musi spełniać następujące wymagania:

Identyfikator	**Wymaganie**
WF.WP.1	Moduł ma umożliwić weryfikację podpisów w formatach XAdES, CAdES, PAdES we wszystkich odmianach zgodnie ze standardami ETSI w tym zakresie.
WF.WP.2	Moduł ma umożliwić weryfikację podpisów wielokrotnych w tym kontrasygnat
WF.WP.3	Moduł ma umożliwić konfigurację punktów zaufania w postaci wybranych list TSL lub odwołania do "listy list" udostępnianej na stronach Komisji Europejskiej
WF.WP.4	Moduł ma automatycznie wykrywać aktualizację listy TSL i pobierać jej najnowszą wersję
WF.WP.5	Moduł ma umożliwiać konfigurację punktów zaufania w postaci list CRL i TSL
WF.WP.6	Moduł ma automatycznie wykrywać aktualizację listy CRL oraz TSL i pobierać jej najnowszą wersję
WF.WP.7	Moduł ma umożliwiać konfigurację usług weryfikacji ważności certyfikatów w postaci zewnętrznej usługi OCSP zgodnej z RFC 2560
WF.WP.8	Moduł ma udzielać odpowiedzi OCSP na podstawie skonfigurowanych punktów zaufania
WF.WP.9	Moduł ma umożliwiać współpracę z urządzeniem do bezpiecznego przechowywania kluczy (HSM)
WF.WP.10	Moduł ma przechowywać i archiwizować dane (listy CRL, odpowiedzi OCSP) na podstawie których została wygenerowana odpowiedź OCSP
WF.WP.11	Moduł ma umożliwiać weryfikację podpisu zaawansowanego na podstawie list TSL
WF.WP.12	Moduł ma umożliwiać weryfikację podpisu złożonego przy pomocy podpisu osobistego
WF.WP.13	Moduł ma umożliwiać weryfikację podpisu złożonego z wykorzystaniem profilu zaufanego
WF.WP.14	Moduł umożliwia logowanie zdarzeń związanych z: • uruchamianiem i zatrzymywaniem usługi • zweryfikowanymi podpisami • wydanymi odpowiedziami OCSP • czynnościami administracyjnymi
WF.WP.15	Moduł umożliwia przesyłanie logowanych zdarzeń do modułu logowania zdarzeń
WF.WP.16	Moduł ma umożliwiać dostęp administracyjny w celu konfiguracji poszczególnych usług i repozytoriów.
WF.WP.17	Administrator korzystając z modułu, ma mieć możliwość: dodawania, aktywacji/dezaktywacji, usuwania i modyfikacji punktów zaufania oraz ustawienia harmonogramu częstotliwości wykrywania zmian.

WF.WP.18	Moduł ma utrzymywać Repozytorium list CRL i TSL dla zdefiniowanych punktów zaufania. Punktem zaufania jest odwołanie do listy TSL lub usługi weryfikacji ważności certyfikatów (CRL lub OCSP)
WF.WP.19	Moduł ma dawać możliwość określenia okresu czasu i liczby przechowywanych list CRL i TSL w Repozytorium dla poszczególnych punktów zaufania
WNF.WP.1	Dla formatu podpisu XAdES i CAdES system ma umożliwić weryfikację podpisu za pośrednictwem interfejsu zgodnego ze specyfikacją OASIS Digital Signature Services w wersji 1.0
WNF.WP.2	Dla formatu podpisu PAdES dopuszczalne jest udostępnienie interfejsu WebService służący do weryfikacji
WNF.WP.3	Udostępniany interfejs OCSP ma umożliwiać komunikację zgodnie ze standardem RFC 2560

4. Znakowanie Czasem (TSP)

4.1 Usługa znakowania czasem (ang. TSA – Time Stamp Authority) realizuje znakowanie czasem zgodnie z protokołem TSP (ang. Time Stamp Protocol). Znakowanie jest wykonywane na podstawie czasu koordynowanego UTC udostępnianego przez wewnętrzne zegary czasu NTP. Usługa znakowania czasem zrealizowana jest za pomocą odrębnego modułu aplikacyjnego TSA wykorzystującego oddzielny moduł kryptograficzny HSM (ang. Hardware Security Module) o wysokiej wydajności, pozwalający na generowanie wystarczającej ilości znaczników czasu w ciągu sekundy, w celu zaspokojenia potrzeb wydajnościowych systemu. Moduł serwera TSA stosuje odrębne klucze RSA do generowania znaczników czasu zgodnie z RFC 3161. Klientem serwera znakowania czasem mają być inne moduły P2, jednak podstawowym klientem serwera TSA będzie moduł WS (webservices) odpowiedzialny za tworzenie postaci archiwalnej podpisu. Moduł WS komunikuje się z serwerem znakowania czasem zgodnie ze specyfikacją DSS.

4.2 Usługa znakowania czasem musi spełniać następujące wymagania:

Identyfikator	**Wymaganie**
WF.TSP.1	Moduł ma umożliwić uzyskanie znacznika czasu zgodnego z bieżącym czasem systemu (polska strefa czasowa).
WF.TSP.2	Moduł ma synchronizować czas z zaufanym źródłem czasu
WF.TSP.3	Moduł ma współpracować ze sprzętowym modułem kryptograficznym (HSM) w celu przechowywania kluczy
WF.TSP.4	moduł ma pozwalać na uzyskanie znacznika czasu przy zastosowaniu protokołu TSP zgodnego z RFC 3161
WF.TSP.5	Moduł ma pozwalać na uzyskanie znacznika czasu przy zastosowaniu protokołu zgodnego z OASIS DSS Timestamp Profile

5. Moduł Logowania Zdarzeń

5.1 Moduł Logowania Zdarzeń podsystemu podpisu elektronicznego (PPE) odpowiedzialny jest za zbieranie logów zdarzeń w PPE i przekazywanie ich do Podsystemu Raportowania i Logowania.

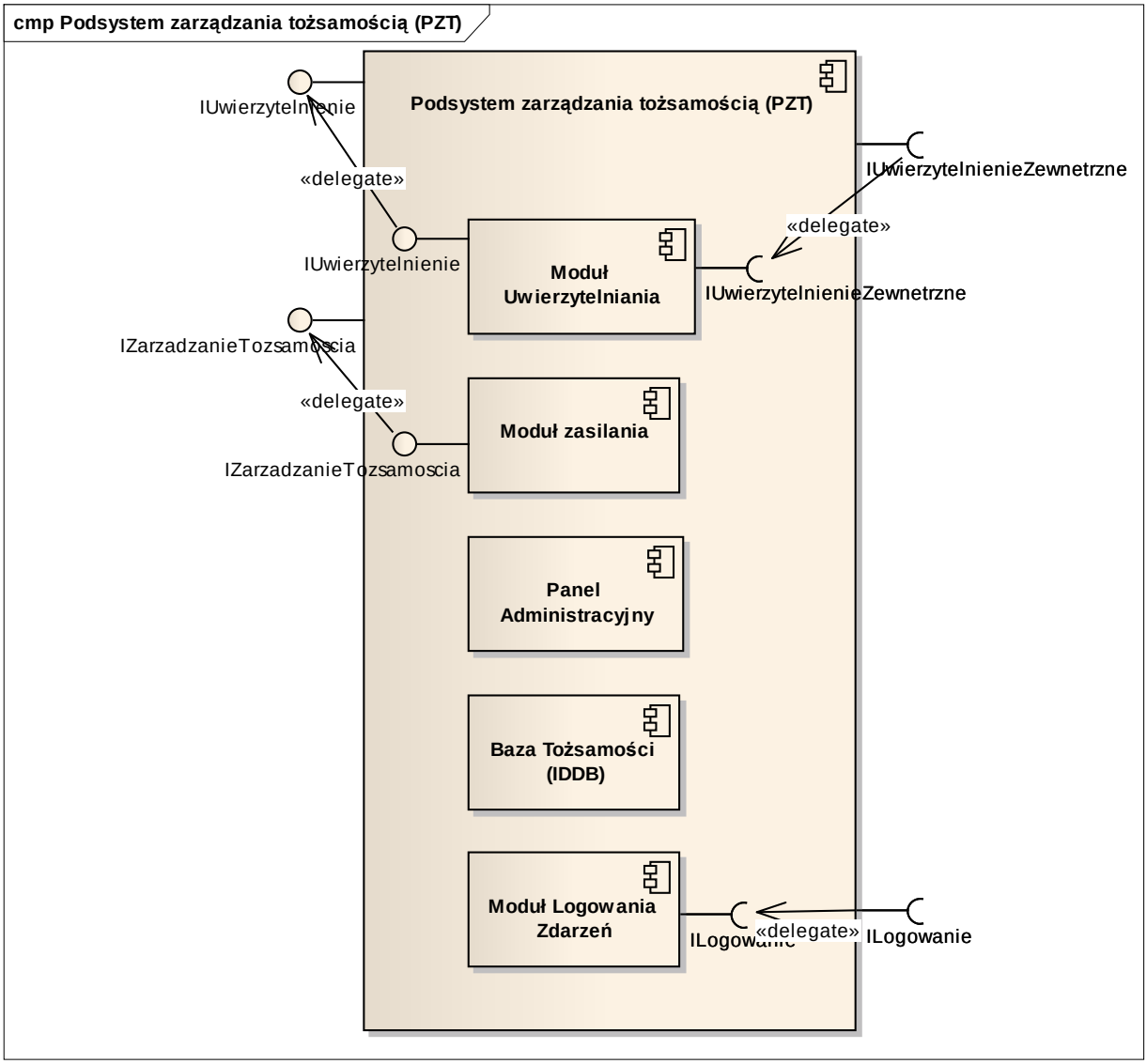
5.2 Moduł logowania zdarzeń musi spełniać następujące wymagania:

Identyfikator	**Wymaganie**

WF.MLZ.1	Moduł umożliwia odbiór informacji z modułów podsystemu podpisu elektronicznego
WF.MLZ.2	Moduł umożliwia przetworzenie zdarzeń do formatu akceptowalnego przez podsystem raportowania i logowania
WF.MLZ.3	Moduł umożliwia przesłanie odebranych zdarzeń do podsystemu raportowania i logowania

D. Podsystem zarządzania tożsamością (PZT)

Podsystem Zarządzania Tożsamością ma udostępniać interfejs umożliwiający uwierzytelnianie użytkowników. Głównym zadaniem tego podsystemu jest gromadzenie i zarządzanie informacjami o tożsamościach użytkowników.



Rysunek 5 – Podsystem zarządzania tożsamością

1. Baza Tożsamości (IDDB)

W Bazie Tożsamości (IDDB) przechowywane są informacje umożliwiające identyfikację wszystkich użytkowników systemu SIOZ. IDDB to również Repozytorium, w którym przechowywane są dane niezbędne do realizacji procesu uwierzytelniania użytkowników systemu SIOZ. Do użytkowników systemu SIOZ zalicza się:
a) osoby fizyczne

b) systemy zewnętrzne

2. Moduł Logowania Zdarzeń

Moduł Logowania Zdarzeń podsystemu zarządzania tożsamością (PZT) odpowiedzialny jest za zbieranie logów zdarzeń w PZU i przekazywanie ich do Podsystemu Raportowania i Logowania.

3. Moduł Uwierzytelniania

Moduł uwierzytelniania umożliwia uwierzytelnienie użytkowników za pomocą strony www i webserwisów

4. Moduł zasilania

Moduł zasilania umożliwia przyjęcie dokumentu XML – wniosku podpisanego za pomocą kwalifikowanego lub osobistego podpisu elektronicznego oraz profilu zaufanego w celu założenia tożsamości.

5. Panel Administracyjny

Zadaniem panelu administracyjnego jest umożliwienie podmiotowi (lub jego właścicielowi) zarządzania tożsamością w Podsystemie Zarządzania Tożsamością, w szczególności usunięcia i edycji swojej tożsamości za pomocą dedykowanej w tym celu stronie WWW po wcześniejszym pozytywnym uwierzytelnieniu.

6. Zestawienie wymagań dla PZT:

Identyfikator	**Wymaganie**
WF.PZT.1	Podsystem ma posiadać centralne repozytorium tożsamości.
WF.PZT.2	Podsystem ma zapewnić integralność magazynu tożsamości.
WF.PZT.3	Podsystem ma zapewnić, że każdy podmiot musi być identyfikowany przez unikalny identyfikator.
WF.PZT.4	Podsystem ma zapewnić integralność informacji o podmiotach w czasie ich przetwarzania i przechowywania.
WF.PZT.5	Podsystem ma zapewnić przejrzysty panel administracyjny z poziomu którego można będzie wykonywać wszystkie czynności związane z zarządzaniem tożsamością.
WF.PZT.6	Podsystem ma zapewnić, że zarządzanie podsystemem tożsamości może być wykonywane jedynie przez uprawnione osoby.
WF.PZT.7	Podsystem ma zapewnić, że modyfikacja atrybutów tożsamości może być dokonywana wyłącznie przez uprawnione osoby.
WF.PZT.8	Podsystem musi umożliwiać tworzenie procesów związanych z zarządzaniem tożsamością – w szczególności obsługi wniosków o utworzenie tożsamości.

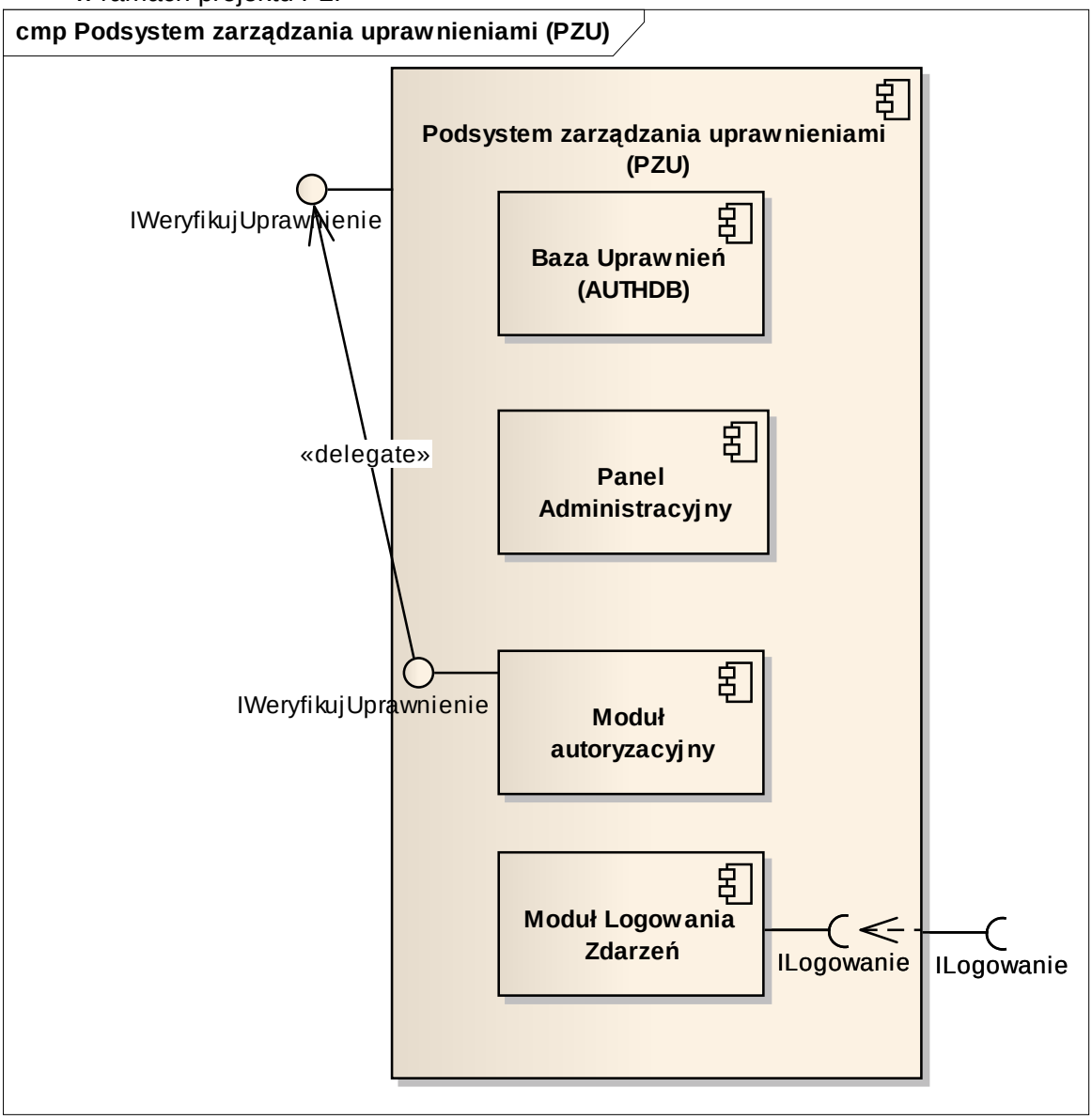
WF.PZT.9	Podsystem ma posiadać mechanizm wykrywania, blokowania i usuwania nieużywanych tożsamości. Decyzję o usunięciu wymagają ingerencji operatora.
WF.PZT.10	Podsystem ma zapewnić mechanizm wykrywania różnych tożsamości tego samego podmiotu.
WF.PZT.11	Podsystem ma udostępniać użytkownikom funkcję samoobsługowego resetowania i zmiany haseł poprzez interfejs webowy.
WF.PZT.12	Podsystem ma zapewnić ze tożsamość osoby/systemu ma zawierać następujące atrybuty: • unikalny identyfikator nadawany przez system, • imię/nazwę systemu, • nazwisko/nazwę organizacji, • PESEL/numer paszportu, (NIP, REGON), • nazwa użytkownika, • identyfikator administratora/właściciela sytemu lub identyfikator grupy administratorów/właścicieli (pole opcjonalne), • skrót hasła (pole opcjonalne), • certyfikat/y (pole opcjonalne), • identyfikator zaufanego profilu (pole opcjonalne), • identyfikator konta ePUAP (pole opcjonalne), • datę utworzenia, • datę wygaśnięcia liczoną od daty ostatniego zalogowania, • adres email podmiotu (administratora, jeśli podmiotem jest system). • Inne cechy określone w trakcie analizy szczegółowej dla realizacji projektu techniczne
WF.PZT.13	Podsystem ma uniemożliwić założenie konta bez podania wszystkich wymaganych atrybutów.
WF.PZT.14	Podsystem ma umożliwić przerwanie zakładania tożsamości na życzenie podmiotu.
WF.PZT.15	Podsystem nie może przechowywać haseł w postaci jawnej.

WF.PZT.16	Podsystem musi uwierzytelniać podmioty za pomocą: • identyfikatorów i haseł, • certyfikatów, • podpisanego tokenu za pomocą zaufanego profilu, • mechanizmu ograniczonej identyfikacji (pl.ID).
WF.PZT.17	Podsystem musi uwierzytelniać podmioty za pomocą nadsyłanych dokumentów na podstawie: • podpisu weryfikowanego kwalifikowanym certyfikatem, • podpisu osobistego, • podpisu złożonego za pomocą zaufanego profilu.
WF.PZT.18	Podsystem musi umożliwiać rozszerzenie metod uwierzytelnienia o inne niż wymienione powyżej, np. hasła jednorazowe.
WF.PZT.19	Podsystem musi tworzyć zapisy z każdego użycia tożsamości i zarządzania tożsamością.
WF.PZT.20	Podsystem ma zapewnić, że usunięcie tożsamości nie może powodować skuteczne usunięcie wszystkich atrybutów tożsamości z podsystemu.
WF.PZT.21	Podsystem ma zapewnić, aby usunięte unikalne identyfikatory nadawane przez podsystem nie mogły być ponownie wykorzystane.
WF.PZT.22	Podsystem ma zapewnić możliwość zawieszania tożsamości podmiotu przez administratora w przypadku podejrzenia nadużyć związanych z jej wykorzystaniem lub na życzenie podmiotu.
WF.PZT.23	Podsystem ma zapewnić, że aktywacja tożsamości może być dokonana wyłącznie po zatwierdzeniu przez administratora podsystemu.
WF.PZT.24	Podsystem ma umożliwiać założenie tożsamości po złożeniu wniosku - dokumentu XML podpisanego za pomocą podpisu kwalifikowanego lub osobistego podpisu elektronicznego oraz profilu zaufanego.
WF.PZT.25	Podsystem ma zapewnić panel administracyjny, dla podmiotu lub jego właściciela (w przypadku systemów), który będzie umożliwiał usunięcia i edycje swojej tożsamości za pomocą dedykowanej w tym celu strony WWW po wcześniejszym pozytywnym uwierzytelnieniu.
WF.PZT.26	Podsystem ma udostępniać mechanizm uwierzytelnienia podmiotów - systemów teleinformatycznych przy użyciu technologii WSS (WS-Seciruty).
WF.PZT.27	Podsystem ma zapewnić mechanizm wprowadzania nowego hasła lub zmiany hasła z możliwość weryfikacji np. przez podwójne wprowadzenie nowego hasła.
WF.PZT.28	Podsystem ma zapewnić, że zmiana hasła przez użytkownika ma być poprzedzona podaniem dotychczas używanego hasła.
WF.PZT.29	Podsystem ma zapewnić, że administrator będzie miał możliwość zresetowania hasła użytkownika. Hasło tymczasowe ma być automatycznie wysłane do użytkownika.

WF.PZT.30	Podsystem ma zapewnić, że po uwierzytelnieniu za pomocą hasła tymczasowego podmiot nie może mieć dostępu do żadnej funkcjonalności systemu zarządzania tożsamością poza zmianą hasła. Dostęp do pozostałych funkcjonalności ma być możliwy wyłącznie po udanym uwierzytelnieniu przy pomocy nowego hasła.
WF.PZT.31	Podsystem ma umożliwić wymuszenie polityki bezpiecznych haseł: • Zmiana hasła po określonym czasie. • Historia haseł. • Minimalna i maksymalna liczba znaków w haśle. • Uniemożliwienie wprowadzeni hasła identycznego z dowolnym atrybutem w podsystemie zarządzania tożsamością. • Złożoność haseł: o minimalnej i maksymalnej liczby znaków w haśle o minimalnej liczby cyfr w haśle o maksymalnej liczby powtarzających się znaków o zestawu wymaganych znaków o zestawu zabronionych znaków
WF.PZT.32	Podsystem ma umożliwić powiadomienie podmiotu o wygasającym haśle.
WF.PZT.33	Podsystem ma dostarczyć administratorom możliwość definiowania listy zakazanych haseł.
WF.PZT.34	Podsystem powinien posiadać mechanizm czasowego blokowania możliwości uwierzytelnienia po zdefiniowanej przez administratora liczbie nieudanych prób uwierzytelnienia. Blokowanie konta powinno być rejestrowane.
WF.PZT.35	Podsystem ma doprowadzić procedurę uwierzytelnienia do końca mimo wykrywanych błędów w trakcie jej trwania (w przypadku uwierzytelnienia wieloetapowego przeprowadzał procedurę do końca).
WF.PZT.36	Podsystem ma umożliwić podmiotowi wyświetlenie statystyk uwierzytelnienia w szczególności czas ostatniej udanej próby uwierzytelnienia oraz liczbę nieudanych uwierzytelnień od czasu ostatniego udanego uwierzytelnienia.
WF.PZT.37	Podsystem ma zapewnić, że ani prawidłowe ani nieprawidłowe hasła nie mogą być rejestrowane w podsystemie rejestracji logów.
WF.PZT.38	Podsystem nie może wyświetlać znaków hasła na wejściu.

E. Podsystem zarządzania uprawnieniami (PZU)

Podsystem zarządzania uprawnieniami realizuje funkcjonalności związane z przyznawaniem, odbieraniem i weryfikacją uprawnień do zasobów udostępnianych przez systemy realizowane w ramach projektu P2.



Rysunek 6 – Podsystem zarządzania uprawnieniami

1. Baza Uprawnień (AUTHDB)

Repozytorium, w którym przechowywane są informacje o uprawnieniach użytkowników do poszczególnych usług zlokalizowanych w P2. W repozytorium są również przechowywane informacje pozwalające skojarzyć dany formularz elektroniczny z konkretną usługą.

2. Moduł autoryzacyjny

Moduł autoryzacyjny Odpowiedzialny jest za weryfikację uprawnień dla użytkowników usług zlokalizowanych w P2.

3. Moduł Logowania Zdarzeń

Moduł Logowania Zdarzeń podsystemu zarządzania uprawnieniami (PZU) odpowiedzialny jest za zbieranie logów zdarzeń w PZU i przekazywanie ich do Podsystemu Raportowania i Logowania.

4. Panel Administracyjny

Zadaniem panelu administracyjnego jest umożliwienie podmiotowi (lub jego właścicielowi) zarządzania uprawnieniami w Podsystemie Zarządzania Uprawnieniami. Panel administracyjny umożliwia wykonywanie wszystkich czynności związanych z zarządzaniem uprawnieniami.

5. Zestawienie wymagań dla PZU

Identyfikator	**Wymaganie**
WF.PZU.1	Podsystem ma posiadać centralne repozytorium uprawnień.
WF.PZU.2	Podsystem ma umożliwić definiowanie ról i przypisanie ich do usług wewnętrznych P2. Przykłady ról: Redaktor rejestru (przykładowe uprawnienia: dokonanie wpisu do rejestru, modyfikacja wpisu w rejestrze, itp.) Administrator uprawnień (przykładowe uprawnienia: dodaj użytkownika do roli, utwórz grupę użytkowników).
WF.PZU.3	Podsystem ma umożliwić tworzenie grup ról.
WF.PZU.4	Podsystem ma umożliwiać konfiguracja użytkownika w bazie uprawnień na podstawie bazy tożsamości systemu SA.
WF.PZU.5	Podsystem ma umożliwić grupowanie użytkowników.
WF.PZU.6	Podsystem ma umożliwić przypisanie ról do użytkowników i grup użytkowników.
WF.PZU.7	Zarządzanie podsystemem autoryzacji może być wykonywane jedynie przez uprawnione osoby.
WF.PZU.8	Podsystem musi logować zdarzenia dotyczące procesu zarządzania uprawnieniami.
WF.PZU.9	Podsystem ma udostępniać listę uprawnień na podstawie identyfikatora użytkownika.
WNF.PZU.10	Podsystem ma zapewnić przejrzysty, graficzny panel administracyjny z poziomu, którego można będzie wykonywać wszystkie czynności związane z zarządzaniem uprawnieniami.
WNF.PZU.11	Szczegółowy zakres realizacji wymagań zostanie doprecyzowany podczas analizy szczegółowej realizowanej na potrzeby stworzenia projektu technicznego systemu.

F. Interfejsy udostępniane

1. ILogowanie

Zadaniem interfejsu jest udostępnienie możliwości zapisu informacji o wygenerowanych zdarzeniach do podsystemu raportowania i logowania. Interfejs ma umożliwiać wyłącznie zapis zdarzeń do podsystemu.

2. IOCSP

Zadaniem usługi jest udostępnianie informacji o ważności zaufanych certyfikatów na potrzeby usług weryfikacji certyfikatów oraz usługi archiwizacji podpisu.

Interfejs ma udostępniać informacje o ważności przy użyciu protokołu OCSP zgodnego z RFC 2560.

3. IPodpisDSS

Interfejs implementujący wymianę komunikatów zgodnych ze standardem Oasis Digital Signature Services Core (OASIS DSS Core specification; http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html)
Interfejs ma implementować profile:
a) DSS Asynchronous profile

b) DSS AdES profile w zakresie formatu XadES

c) Zakres implementowanych funkcjonalności ma obejmować:

- Złożenie i aktualizację podpisu dla następujących rodzajów podpisu zaawansowanego:

Rodzaj podpisu	**URI**
XAdES-BES	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES
XAdES-EPES	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:EPES
XAdES-T	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T
XAdES-A	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-A

Interfejs usługi umożliwiającej składanie podpisu elektronicznego zgodnie ze specyfikacją DSS. Interfejs ma dać możliwość złożenia podpisu na podstawie przesłanego wniosku zawierającego tylko skrót dokumentu wraz z pozostałymi atrybutami - bez konieczności przesyłania całej treści dokumentu.

4. IUstalenieTozsamosciPodpisujacego

4.1 Interfejs ma udostępniać funkcjonalności:
a) Ustalenia tożsamości podpisującego na podstawie przesłanego podpisu dokumentu (informacje o użytkowniku są pobierane z certyfikatu/zaufanego profilu)

b) Ustalenia identyfikatora użytkownika na podstawie przesłanego podpisu dokumentu (identyfikator użytkownika jest wyszukiwany w podsystemie zarządzania tożsamością na podstawie informacji pobranych z certyfikatu/zaufanego profilu)

4.2 Parametrami wejściowymi są:
a) Podpis w formatach XadES, CadES, PadES, podpis złożony zaufanym profilem

4.2 Parametrami wyjściowymi są:
a) Identyfikator użytkownika (w przypadku funkcjonalności ustalenia identyfikatora użytkownika)

b) Zestaw danych: imię, nazwisko, PESEL/numer paszportu (w przypadku funkcjonalności ustalenia tożsamości użytkownika), inne dane określone w trakcie realizacji projektu technicznego systemu

4.3 Funkcje mają być udostępniane za pomocą interfejsu zgodnego z Web Services

W ramach interfejsu realizowane są następujące metody ustalenia tożsamości z wykorzystaniem kluczy publicznych do uwierzytelniania użytkowników na podstawie podpisanego dokumentu:

- o podpis elektroniczny (certyfikat podpisu osobistego z pl.ID),
- o podpis elektroniczny (certyfikaty niekwalifikowane zgodne z określonymi politykami certyfikacji),
- o profil zaufany ePUAP,
- o bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu,
- o podpis cyfrowy wykonany przez systemy informatyczne,
- o pieczęć elektroniczna (dla uwierzytelnienia podmiotów i tworzonych przez nie dokumentów),

5. IUwierzytelnianie

5.1 W ramach interfejsu realizowane są następujące metody uwierzytelniania:

a) z wykorzystaniem kluczy publicznych (ang. Public Key-Based Client Authentication) do bezpośredniego uwierzytelniania użytkowników podczas logowania:

- o podpis elektroniczny (certyfikat podpisu osobistego z pl.ID),
- o podpis elektroniczny (certyfikaty niekwalifikowane zgodne z określonymi politykami certyfikacji),
- o profil zaufany ePUAP,

b) z wykorzystaniem kluczy publicznych do uwierzytelniania użytkowników na podstawie podpisanego dokumentu:

- o podpis cyfrowy wykonany przez systemy informatyczne,
- o pieczęć elektroniczna (dla uwierzytelnienia podmiotów i tworzonych przez nie dokumentów),

c) z wykorzystaniem nazwy użytkownika i hasła do bezpośredniego uwierzytelniania użytkowników podczas logowania:

- o nazwa użytkownika i hasło

5.2 Funkcjonalność uwierzytelniania ma być realizowana za pomocą:

a) usługi sieciowej (ang. webservices) która będzie umożliwiała przekazanie danych przez system zewnętrzny.

5.3 Interfejs udostępnia usługę zgodnie ze standardem SAML 2.0

6. IWeryfikacjaDSS

6.1 Interfejs udostępniany zgodnie ze specyfikacją DSS związaną z protokołem weryfikacji podpisu (OASIS DSS Core specification; http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html). Interfejs obsługuje komunikaty dostarczone w odpowiednio przygotowanej strukturze XML.

6.2 Interfejs ma implementować profile:

a) DSS Asynchronous profile

b) DSS AdES profile w zakresie formatów XAdES, CAdES, także znajdujących się w strukturach dokumentów PDF

7. IWeryfikujUprawnienie

Interfejs udostępnia usługę weryfikacji uprawnienia zgodnie ze standardem SAML 2.0. Szczegółowy zakres parametrów usługi zostanie doprecyzowany w trakcie realizacji projektu technicznego systemu.

8. IZarzadzanieTozsamoscia

8.1 Interfejs udostępnia funkcjonalności związane z zarządzaniem tożsamością w tym:

a) Dodanie tożsamości

b) Usunięcie tożsamości

c) Modyfikację tożsamości

d) Wyszukanie tożsamości po identyfikatorze

e) Wyszukanie tożsamości na podstawie wybranego atrybutu konta (PESEL/numer paszportu, imię, nazwisko, email)

8.2 Interfejs jest udostępniany w formie usługi WebService.

9. IZnakowanieCzasemDSS

Interfejs udostępniany na potrzeby komunikacji z modułem WS i realizowany zgodnie ze specyfikacją XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0.

10. IZnakowanieCzasemRFC

Interfejs udostępniany na potrzeby komunikacji z innymi systemami P2 i realizowany zgodnie ze specyfikacją RFC 3161.

11. IZarzadzanieLogami

Interfejs odpowiada za wyszukiwanie informacji w repozytorium logów i umożliwia archiwizację informacji znajdujących się w Repozytorium Logów.

G. Interfejsy udostępnione z systemów zewnętrznych.

1. CRL

Do pobierania informacji o unieważnieniach, publikowanych przez zewnętrzne urzędy CA konieczne jest udostępnienie przez nie interfejsu pozwalającego na pobranie takiej informacji. Jedną z metod udostępniania informacji o unieważnieniach jest okresowe generowanie listy CRL. System zewnętrzny powinien udostępniać usługę poprzez protokół HTTP.

2. ITSL

Do ustalenia informacji o zaufaniu usługi wykorzystywane są listy TSL. Do wykorzystania listy TSL przez system administracji konieczne jest udostępnienie jej przy użyciu protokołu HTTP.

3. IUwierzytelnienieZewnetrzne

System Administracji ma posiadać funkcjonalność wykorzystania systemu zewnętrznego (ePUAP) w celu uwierzytelnienia użytkownika. W tym celu system zewnętrzny ma udostępniać interfejs zgodny ze standardem SAML 2.0

4. OCSP

Jednym ze sposobów pozyskiwania informacji o ważności certyfikatów wydanych przez zewnętrzne CA (np. centrum wydające certyfikaty kwalifikowane) jest pozyskanie odpowiedzi OCSP. W celu wykorzystania usług OCSP przez system administracji konieczne jest, aby usługa była udostępniana zgodnie ze specyfikacją RFC 2560

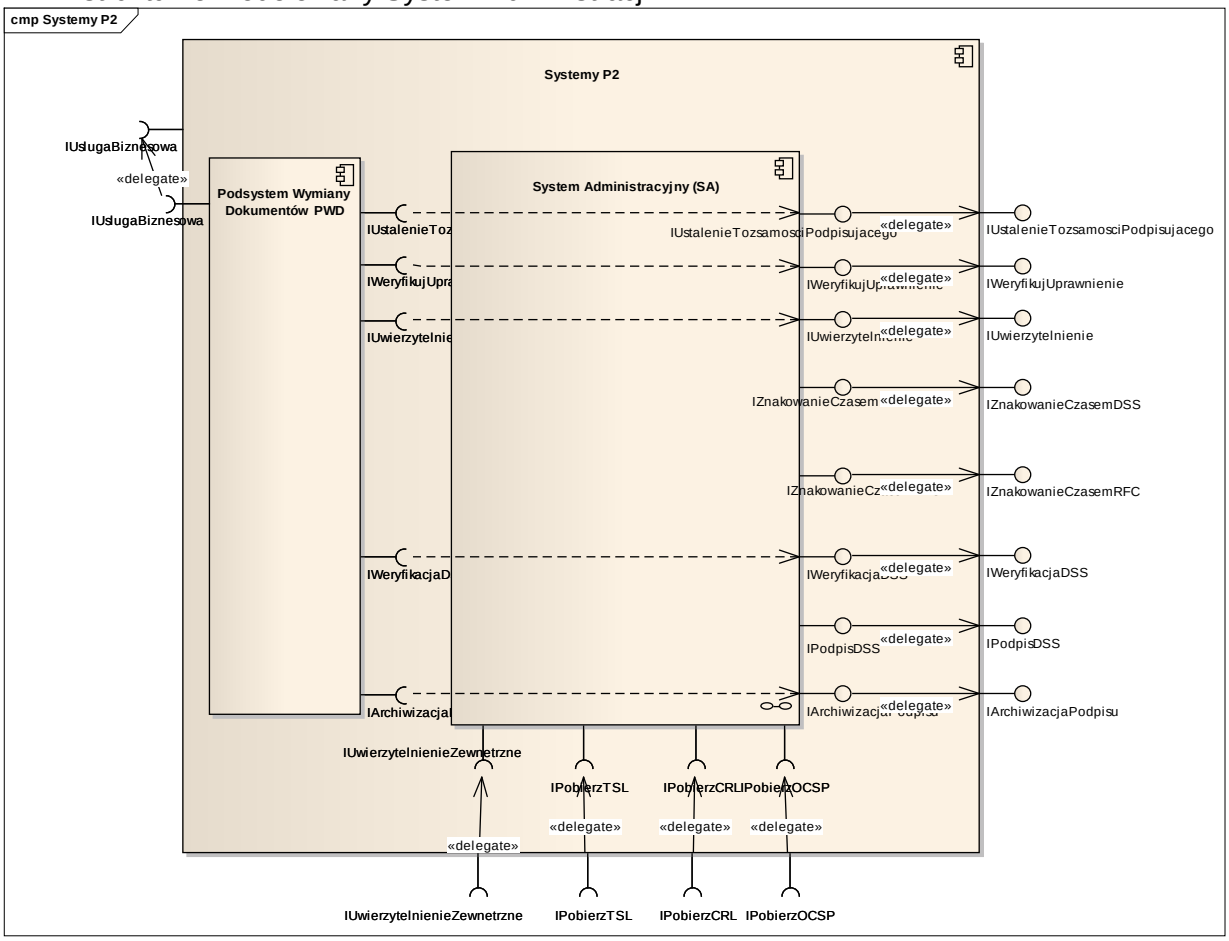
VI. Systemy Zewnętrzne

A. Rejestr

Komponent rejestru reprezentuje dowolny rejestr medyczny udostępniany za pomocą szyny P1

B. Systemy P2

Komponent P2 reprezentuje systemy i funkcjonalności udostępniane w ramach projektu P2 "Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych" przez CSIOZ. Komponent P2 jest komponentem zawierającym w swojej strukturze modelowany System Administracji.



Rysunek 7 – Systemy P2

1. Podsystem Wymiany Dokumentów PWD

Podsystem wymiany dokumentów jest komponentem realizowanym w ramach projektu P2 odpowiedzialnych za przekazywanie dokumentów pomiędzy systemami zewnętrznymi a systemem szyny ESB realizowanym w ramach projektu P1 (Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o zdarzeniach medycznych). Podsystem ten jest podsystemem zewnętrznym w stosunku do Systemu Administracji.

C. Szyna P1

Szyna usług P1 pełni rolę dodatkowej warstwy pośredniej w architekturze systemu informatycznego umożliwiającej przyłączanie oraz odłączanie usług i elementów będących częścią systemu teleinformatycznego systemu ochrony zdrowia. Adaptery pełnią funkcję interfejsów umożliwiających łączenie poszczególnych systemów informatycznych. W ramach szyny usług działają adaptery umożliwiające komunikację z istniejącymi obecnie systemami informatycznymi, w szczególności z systemami płatników, usługodawców oraz rejestry ochrony zdrowia.
Szyna usług nie realizuje funkcjonalności bezpośrednio dla użytkowników końcowych, jest natomiast kluczowym elementem architektury wdrażanych systemów i zapewnia interoperacyjność rozwiązania.

D. System Zewnętrzny P1

Przez system zewnętrzny P1 należy rozumieć taki system, który pozostaje poza kontrolą systemu P1 i korzysta jedynie z usług realizowanych na szynie usług. System taki uwierzytelnia się za pomocą usługi uwierzytelnienia realizowanej przez P2.

E. Wydawca TSL

Komponent wydawcy TSL reprezentuje podmiot publikujący listy TSL służące do weryfikacji zaufania usług certyfikacyjnych

F. Zarządzanie Tożsamością ePUAP (EPUAPID)

Komponent ten reprezentuje system zarządzania tożsamością, który obsługuje system Elektronicznej Platformy Usług Administracji Publicznej (ePUAP)

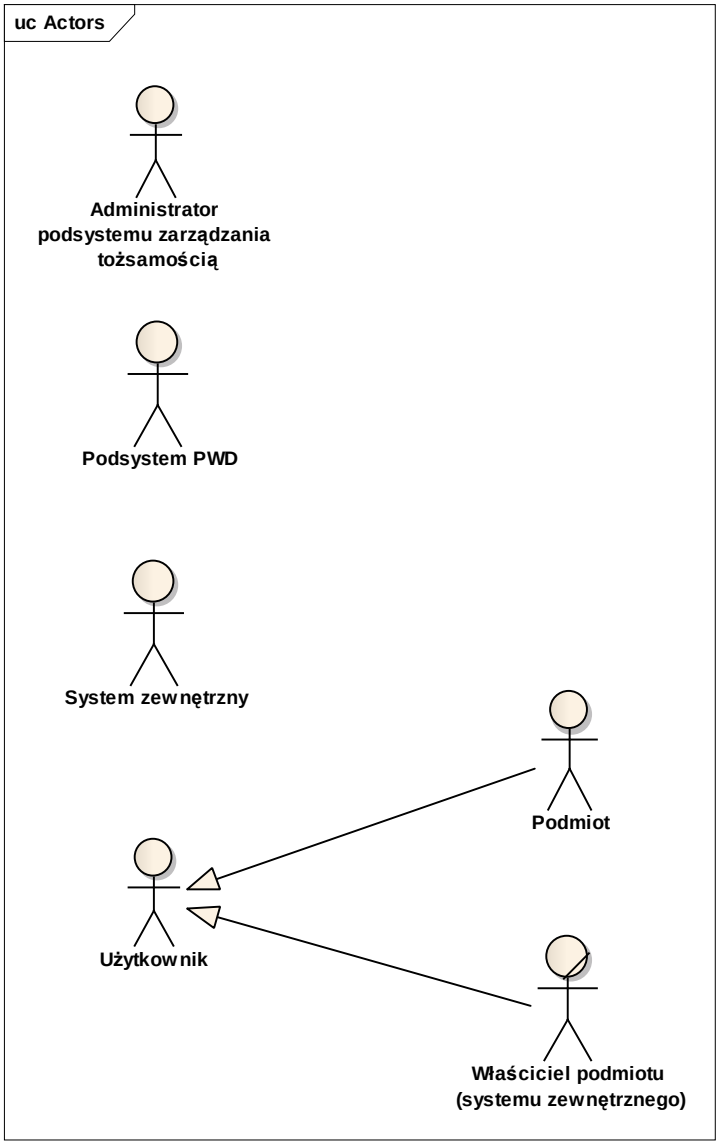
G. Zewnętrzne CA

Komponent reprezentuje dowolne centrum certyfikacji zewnętrzne w stosunku do Systemu Administracji. W szczególności takim centrum certyfikacji jest centrum wydające certyfikaty kwalifikowane. Komponent reprezentuje taką organizację, która będzie traktowana jako zaufana w procesie weryfikacji certyfikatu.

VII.Przypadki użycia systemu administracji

W systemie administracji mają być zaimplementowane między innymi przypadki użycia przedstawione poniżej. W trakcie realizacji projekt technicznego systemu mogą zostać zdefiniowane inne przypadki użycia.

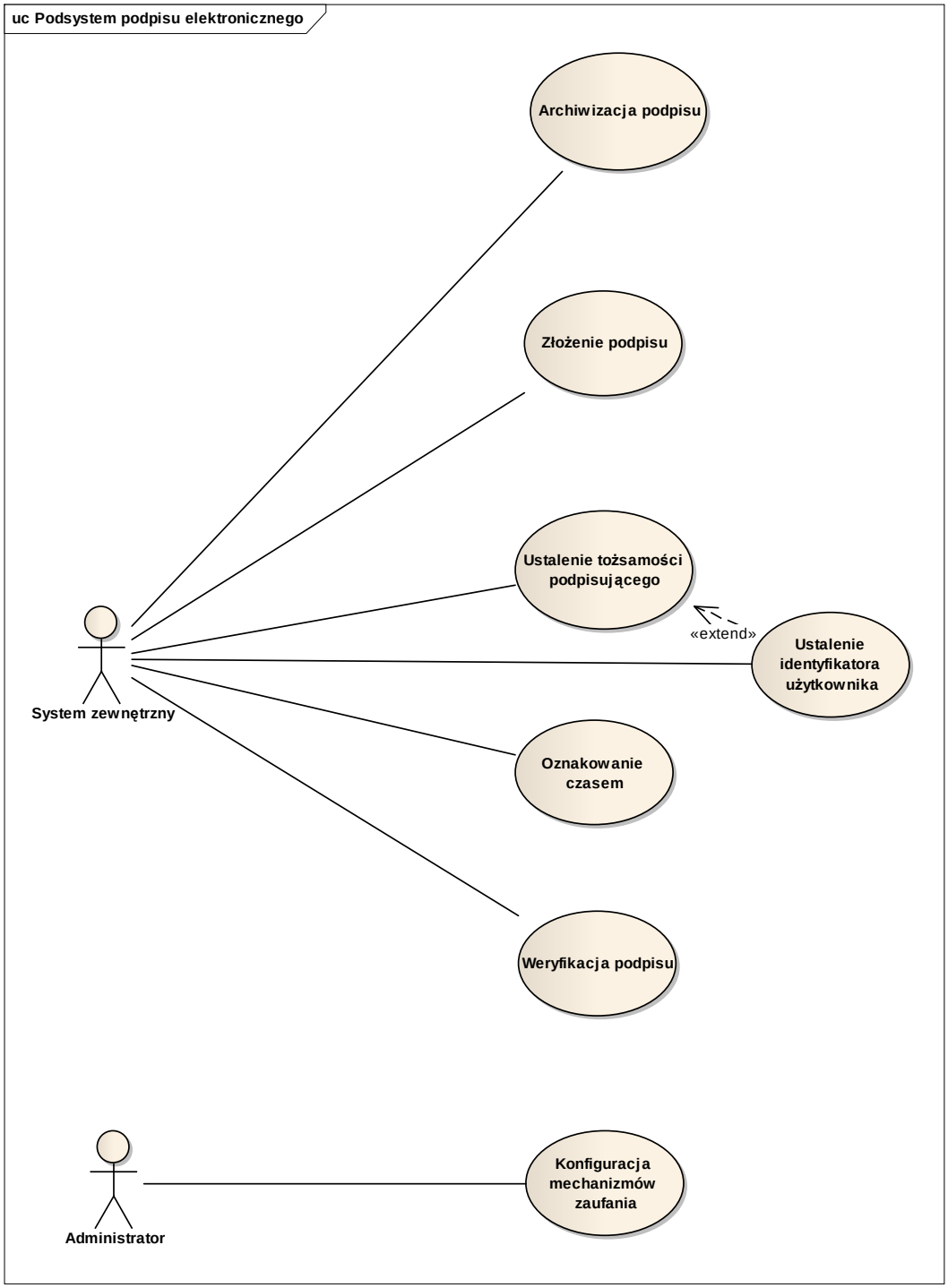
Aktorzy



Rysunek 8 – Aktorzy

A. Podsystem Podpisu Elektronicznego

Podsystem Podpisu elektronicznego ma realizować przypadki użycia wyszczególnione na poniższym diagramie.



Rysunek 9 – Podsystem podpisu elektronicznego.

Aktor	System Zewnętrzny
Numer UC	**1.1**
Nazwa UC	**Archiwizacja podpisu**
Warunki wejścia do UC	Wywołanie przez system zewnętrzny usługi archiwizacji podpisu. Przekazanie poprawnego podpisu XadES.

Okres wystąpienia	-
Opis	1. Usługa archiwizacji pobiera podpis dokumentu 2. Usługa archiwizacji ustala format podpisu 3. Usługa archiwizacji weryfikuje czy certyfikat jest zaufany 4. Usługa archiwizacji pobiera odpowiedź OCSP dla certyfikatu, którym weryfikowany jest podpis 5. Usługa archiwizacji dołącza odpowiedź OCSP do struktur podpisu 6. Usługa archiwizacji znakuje czasem podpis 7. Usługa archiwizacji przekazuje wygenerowany podpis systemowi zewnętrznemu 2a. Usługa archiwizacji ustala że format podpisu jest nieobsługiwany 3. Usługa archiwizacji zgłasza błąd z przyczyną: nieobsługiwany format podpisu 3a. Usługa archiwizacji ustala, że certyfikat użyty do złożenia podpisu jest nie zaufany 4. Usługa archiwizacji przesyła błąd z określeniem przyczyny 4a. Usługa archiwizacji nie może pobrać odpowiedzi OCSP 5 Usługa archiwizacji przesyła błąd z określeniem przyczyny 6a. Usługa nie może pobrać znacznika czasu 7. Usługa archiwizacji przesyła błąd z przyczyną: błąd wewnętrzny – znakowanie czasem niedostępne
Cechy informacyjne	[Podpis w formacie XadES, znacznik czasu, odpowiedź OCSP]
Dodatkowe dane	-
UWAGI	

Aktor	System Zewnętrzny
Numer UC	**1.2**
Nazwa UC	**Złożenie podpisu**
Warunki wejścia do UC	Wywołanie przez system zewnętrzny usługi składania podpisu. Przekazanie jako parametru wniosku o złożenie podpisu zawierającego: • Wartość skrótu z podpisywanego dokumentu \podpisywany dokument • Opcjonalnie informację o kluczu, którym ma być podpisany dokument
Okres wystąpienia	-

Opis	1. System zewnętrzny wysyła żądanie złożenia podpisu pod dokumentem/funkcją skrótu 2. Usługa składania podpisu weryfikuje poprawność żądania 3. Usługa składania podpisu składa podpis w formacie XAdES-BES 4. Usługa archiwizacji przekazuje wygenerowany podpis systemowi zewnętrznemu 2a. Usługa archiwizacji ustala, że żądanie złożenia podpisu jest nieprawidłowe 3. Usługa archiwizacji zwraca odpowiedź z kodem błędu określającym jego przyczynę.
Cechy informacyjne	[dss:SignRequest, dss:SignResponse]
Dodatkowe dane	-
UWAGI	

Aktor	System Zewnętrzny
Numer UC	**1.3**
Nazwa UC	**Ustalenie tożsamości podpisującego**
Warunki wejścia do UC	Wywołanie przez system zewnętrzny funkcji z przekazaniem parametrów: • Wartość podpisu
Okres wystąpienia	-
Opis	1. System zewnętrzny wysyła żądanie ustalenia tożsamości podpisującego na podstawie podpisu 2. System rozpoznaje rodzaj podpisu jako podpis weryfikowany certyfikatem 3. System weryfikuje poprawność struktury podpisu i zaufane certyfikatu 4. System pobiera certyfikat podpisującego 5. System z certyfikatu pobiera informacje o podpisującym (imę nazwisko, pesel/numer paszportu 6. System przekazuje wartości: imię, nazwisko, pesel/numer paszportu do systemu zewnętrznego 2a. System nie rozpoznaje rodzaju podpisu 3. System zwraca odpowiedź z kodem błędu określającym jego przyczynę 2b. System rozpoznaje podpis jako podpis profilem zaufanym

	3. System weryfikuje poprawność struktury podpisu i zaufanie certyfikatu 4. System pobiera struktury podpisu profilem zaufanym 5. System pobiera informacje o podpisującym ze struktur podpisu profilem zaufanym (imię nazwisko, pesel) 7. System przekazuje wartości: imię, nazwisko, pesel/numer paszportu do systemu zewnętrznego 3a. System wykrywa brak poprawności struktury podpisu 4. System zwraca odpowiedź z kodem błędu określającym jego przyczynę 4a. System nie może pobrać certyfikatu podpisującego 5. System zwraca odpowiedź z kodem błędu określającym jego przyczynę 5a. System nie może pobrać z certyfikatu wymaganego zakresu informacji 6. System zwraca odpowiedź z kodem błędu określającym jego przyczynę
Cechy informacyjne	[podpis XadES, podpis CadES, podpis profilem zaufanym, imię nazwisko, pesel/nr paszportu]
Dodatkowe dane	-
UWAGI	

Aktor	System Zewnętrzny
Numer UC	**1.4**
Nazwa UC	**Ustalenie identyfikatora użytkownika**
Warunki wejścia do UC	Wywołanie przez system zewnętrzny funkcji z przekazaniem parametrów: • Wartość podpisu
Okres wystąpienia	-
Opis	1. System wykonuje kroki 1-5 przypadku użycia „ustalenie tożsamości podpisującego” 2. System przesyła do podsystemu zarządzania tożsamością zapytanie o identyfikator użytkownika na podstawie danych: (imię nazwisko, pesel/nr paszportu) 3. System przesyła odpowiedź systemu zarządzania tożsamością do systemu zewnętrznego

Cechy informacyjne	[podpis XadES, podpis CadES, podpis profilem zaufanym, identyfikator użytkownika, imię nazwisko, pesel/nr paszportu]
Dodatkowe dane	-
UWAGI	

Aktor	System Zewnętrzny
Numer UC	**1.5**
Nazwa UC	**Oznakowanie czasem**
Warunki wejścia do UC	Wywołanie przez system zewnętrzny funkcji z przekazaniem parametrów: • Opcjonalnie wartość skrótu oznaczanego czasem • Opcjonalnie wartość odnawianego znacznika czasu
Okres wystąpienia	-
Opis	1. System zewnętrzny przesyła żądanie oznakowania czasem 2. System weryfikuje poprawność przesłanego żądania 3. System pobiera aktualną wartość czasu 4. System generuje znacznik czasu 5. System przesyła zwraca wartość wygenerowanego znacznika do systemu zewnętrznego 2a. przesłane żądanie jest niepoprawne 3. System zwraca odpowiedź z kodem błędu określającym jego przyczynę 4a. System nie może wygenerować znacznika czasu 5. System zwraca odpowiedź z kodem błędu określającym jego przyczynę
Cechy informacyjne	[dss:SignRequest, dss:SignResponse]
Dodatkowe dane	-
UWAGI	Żądanie ma zawierać jedną z wartości jako wartość dss:SignatureType: urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken urn:ietf:rfc:3161

Aktor	System Zewnętrzny
Numer UC	**1.6**
Nazwa UC	**Weryfikacja podpisu**
Warunki wejścia do UC	Wywołanie przez system zewnętrzny funkcji weryfikacji z przekazaniem parametrów:

	• Wartość funkcji skrótu/podpisany dokument • Podpis do weryfikacji
Okres wystąpienia	-
Opis	1. System zewnętrzny przesyła żądanie weryfikacji podpisu 2. System weryfikuje poprawność przesłanego żądania 3. System rozpoznaje rodzaj złożonego podpisu 4. System sprawdza czy podpis jest prawidłowy 5. System sprawdza czy certyfikat służący do weryfikacji podpisu jest zaufany korzystając ze skonfigurowanych mechanizmów/punktów zaufania 6. System sprawdza czy certyfikat służący do weryfikacji jest ważny 7. System przesyła odpowiedź zawierającą wynik weryfikacji podpisu 2a. przesłane żądanie jest niepoprawne 3. System zwraca odpowiedź z kodem błędu określającym jego przyczynę 3a. System nie może rozpoznać rodzaju złożonego podpisu 4. System zwraca odpowiedź z kodem błędu określającym jego przyczynę
Cechy informacyjne	[dss:VerifyRequest, dss:VerifyResponse]
Dodatkowe dane	-
UWAGI	

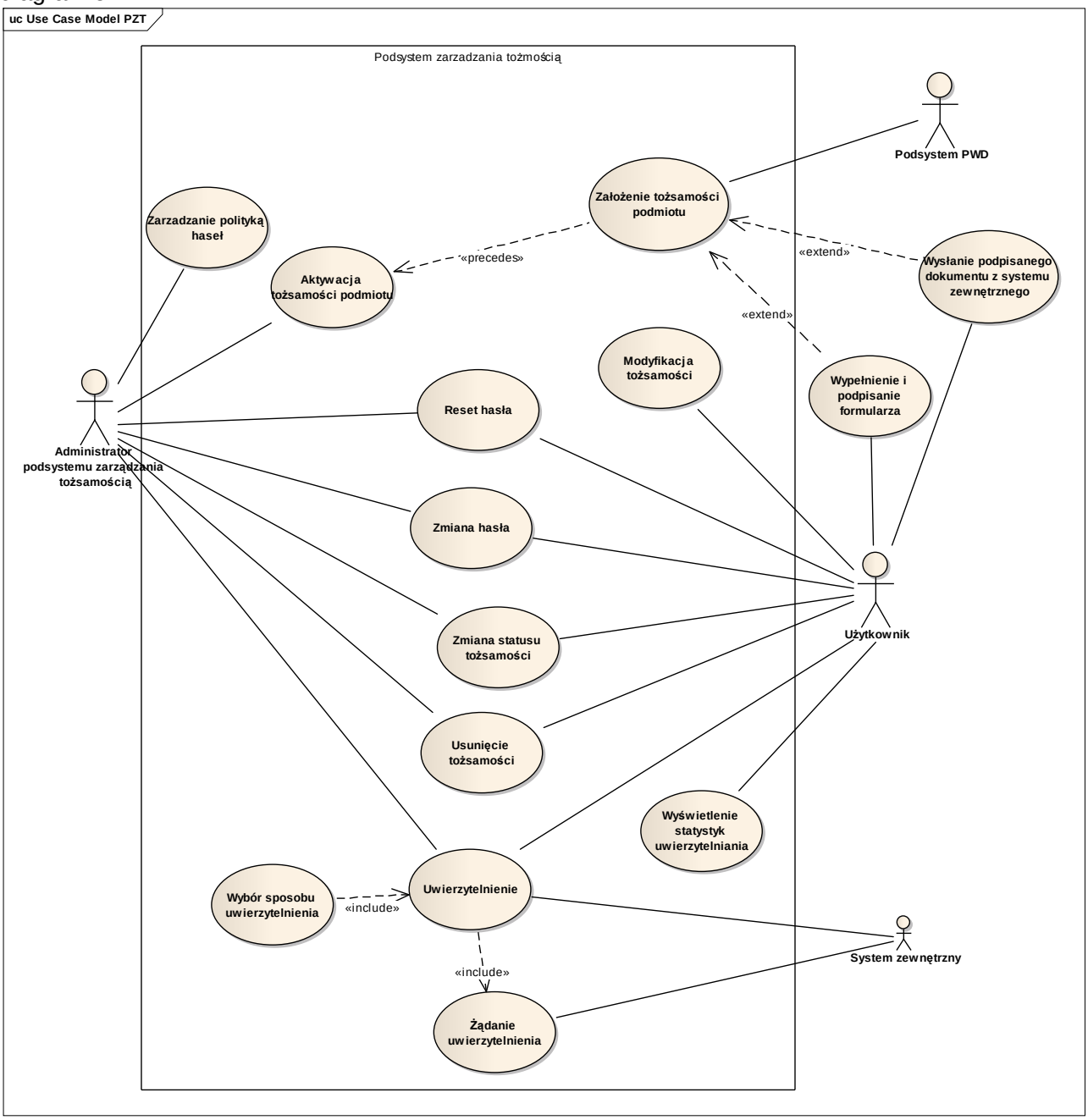
Aktor	Administrator
Numer UC	**1.7**
Nazwa UC	**Konfiguracja mechanizmów zaufania**
Warunki wejścia do UC	Uruchomienie interfejsu graficznego do konfiguracji mechanizmów zaufania
Okres wystąpienia	-
Opis	1. Administrator uwierzytelnia się w interfejscie do konfiguracji mechanizmów zaufania 2. Administrator wybiera opcję konfiguracji mechanizmów zaufania 3. Administrator wybiera opcję dodania nowego punktu zaufania

	4. Administrator podaje nazwę i opis nowego punktu zaufania 5. Administrator podaje rodzaj mechanizmu zaufania (ścieżka certyfikacji) 6. Administrator wskazuje plik zawierający certyfikaty urzędów CA 7. Dla każdego certyfikatu urzędu CA administrator wskazuje lokalizację listy CRL/usługi OCSP 8. Administrator zapisuje konfigurację punktu zaufania 9. Administrator aktywuje punkt zaufania 3a. Administrator wybiera opcję usunięcia punktu zaufania 4. Administrator wybiera z listy punktów zaufania punkt do usunięcia 5. Administrator potwierdza usunięcie punktu zaufania 3b. Administrator wybiera opcje aktywacji/dezaktywacji punktu zaufania 4. Administrator wybiera z listy punktów zaufania punkt do aktywacji/dezaktywacji 5. Administrator potwierdza aktywację/dezaktywację punktu zaufania 3c. Administrator wybiera opcję edycji punktu zaufania 4. Administrator wybiera z listy punktów zaufania punkt do edycji 5. Administrator zatwierdza chęć edycji punktu zaufania 6. Administrator zmienia wartości (dowolne spośród: nazwa, opis, certyfikat, lista tsl, rodzaj usługi weryfikacji certyfikatów, adres usługi weryfikacji certyfikatów) 7. Administrator zapisuje konfigurację punktu zaufania 8. Administrator dezaktywuje i aktywuje punkt zaufania 5a administrator podaje rodzaj mechanizmu zaufania (lista TSL) Administrator wskazuje lokalizację listy TSL 6. Administrator wskazuje częstotliwość wykrywania zmian listy TSL 7. Administrator zapisuje konfigurację punktu zaufania 8. Administrator aktywuje punkt zaufania
Cechy informacyjne	[certyfikaty CA, listy CRL, adresy list CRL, listy TSL, adresy listy TSL, nazwa punktu zaufania, opis punktu zaufania, stan punktu zaufania]

Dodatkowe dane	-
UWAGI	Punkty zaufania mają za zadanie zbudowanie bazy informacji o zaufaniu do certyfikatów, oraz zbudowanie mechanizmów do weryfikacji certyfikatów wydanych przez zaufane urzędy CA

A. Podsystem Zarządzania Tożsamością

Podsystem zarządzania tożsamością ma realizować przypadki użycia przedstawione na poniższym diagramie.



Rysunek 10 – Model przypadków użycia dla Podsystemu Zarządzania Tożsamością

Aktor	*Administrator podsystemu zarządzania tożsamością*
Numer UC	***2.1***
Nazwa UC	***Zarządzanie polityką haseł***
Warunki wejścia do UC	*Wybranie przez użytkownika, posiadającego rolę Administrator podsystemu zarządzania tożsamością, opcji „Zarządzanie polityką haseł"*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Zarządzanie polityką haseł umożliwia określenie:* • *liczby dni ważności hasła,* • *liczby haseł po których hasło może być wykorzystane ponownie* • *złożoność haseł:* o *minimalnej i maksymalnej liczby znaków w haśle* o *minimalnej liczby cyfr w haśle* o *maksymalnej liczby powtarzających się znaków* o *zestawu wymaganych znaków* o *zestawu zabronionych znaków*
Cechy informacyjne	*[minimalna liczba znaków, maksymalna liczba znaków, wymagalność cyfr, wymagalność wielkich liter, wymagalność znaków specjalnych, autor, data +godzina zmiany]*
Dodatkowe dane	-
UWAGI	-

Aktor	*Podsystem wymiany dokumentów*
Numer UC	***2.2***
Nazwa UC	***Założenie tożsamości podmiotu***
Warunki wejścia do UC	*Przygotowanie i wysłanie komunikatu zawierającego dane niezbędne do założenia tożsamości przez podsystem PWD na podstawie otrzymanego uprzednio wniosku.*
Okres wystąpienia	-
Opis	*Przysłany komunikat powoduje wpisanie do bazy tożsamości nowej tożsamości podmiotu. Komunikat powinien zawierać następujące informacje:* • *imię/nazwę systemu,* • *nazwisko/nazwę organizacji,* • *PESEL/(NIP, REGON),* • *nazwa użytkownika,* • *identyfikator administratora/właściciela sytemu lub identyfikator grupy administratorów/właścicieli (pole opcjonalne),* • *certyfikat (pole opcjonalne),* • *identyfikator zaufanego profilu (pole opcjonalne),* • *identyfikator konta ePUAP (pole opcjonalne),* • *adres e-mail podmiotu (administratora, jeśli podmiotem jest system),* • *Inne dane określone w trakcie realizacji projektu technicznego systemu.*

	Po dokonaniu wpisu do administratora wysyłany jest komunikat o konieczności zatwierdzenia tożsamości.
Cechy informacyjne	*[imię/nazwę systemu, nazwisko/nazwę organizacji, PESEL/(NIP, REGON), nazwa użytkownika, identyfikator administratora/właściciela sytemu lub identyfikator grupy administratorów/właścicieli (pole opcjonalne), certyfikat (pole opcjonalne), identyfikator zaufanego profilu (pole opcjonalne), identyfikator konta ePUAP (pole opcjonalne), adres email podmiotu (administratora, jeśli podmiotem jest system), unikalny identyfikator w systemie (nadawany automatycznie przez system)]*
Dodatkowe dane	-
UWAGI	-

Aktor	*Administrator podsystemu zarządzania tożsamością*
Numer UC	***2.3***
Nazwa UC	***Aktywacja tożsamości podmiotu***
Warunki wejścia do UC	*Otrzymanie komunikatu wygenerowanego wyniku wykonania UC „Założenie tożsamości podmiotu”*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Administrator podsystemu zarządzania tożsamością weryfikuje dane nowej tożsamości i zatwierdza aktywację tożsamości. Podsystem generuje hasło tymczasowe i wysyła na podany adres e-mail potwierdzenie o założeniu tożsamości i konieczności zmiany hasła.*
Cechy informacyjne	*[imię/nazwę systemu, nazwisko/nazwę organizacji, PESEL/(NIP, REGON), nazwa użytkownika, identyfikator administratora/właściciela sytemu lub identyfikator grupy administratorów/właścicieli (pole opcjonalne), certyfikat (pole opcjonalne), identyfikator zaufanego profilu (pole opcjonalne), identyfikator konta ePUAP (pole opcjonalne), adres email podmiotu (administratora, jeśli podmiotem jest system), tymczasowe hasło, komunikat wysyłany do użytkownika]*
Dodatkowe dane	-
UWAGI	-

Aktor	*Użytkownik*
Numer UC	***2.4***
Nazwa UC	***Modyfikacja tożsamości***
Warunki wejścia do UC	*Wybranie przez użytkownika, opcji „Modyfikacja tożsamości haseł”*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Użytkownik może zmienić następujące pola:* • *imię/nazwę systemu,* • *nazwisko/nazwę organizacji,* • *PESEL/(NIP, REGON),* • *nazwa użytkownika,* • *identyfikator administratora/właściciela sytemu lub identyfikator grupy administratorów/właścicieli (pole opcjonalne),* • *certyfikat (pole opcjonalne),* • *identyfikator zaufanego profilu (pole opcjonalne),*

	• *identyfikator konta ePUAP (pole opcjonalne),* • *adres e-mail podmiotu (administratora, jeśli podmiotem jest system).* • *Inne dane*
Cechy informacyjne	*[imię/nazwę systemu, nazwisko/nazwę organizacji, PESEL/(NIP, REGON), nazwa użytkownika, identyfikator administratora/właściciela sytemu lub identyfikator grupy administratorów (pole opcjonalne), certyfikat (pole opcjonalne), identyfikator zaufanego profilu (pole opcjonalne), identyfikator konta ePUAP (pole opcjonalne), adres e-mail podmiotu (administratora, jeśli podmiotem jest system)]*
Dodatkowe dane	-
UWAGI	-

Aktor	*Użytkownik.* *Administrator podsystemu zarządzania tożsamością.*
Numer UC	***2.5***
Nazwa UC	***Reset hasła***
Warunki wejścia do UC	*Wybranie przez użytkownika, opcji „Zapomniałem hasła" lub przez administratora podsystemu zarządzania tożsamością opcji „Reset hasła" z menu zarządzania tożsamością.*
Okres wystąpienia	-
Opis	*Wybranie opcji powoduje wygenerowanie w podsystemie zarządzania tożsamością hasła tymczasowego i wysłanie pod adres email związany z tożsamością emaila z informacją o konieczności zmiany hasła na nowe.*
Cechy informacyjne	*[tymczasowe hasło, komunikat wysyłany do użytkownika]*
Dodatkowe dane	-

Aktor	*Użytkownik.* *Administrator podsystemu zarządzania tożsamością.*
Numer UC	***2.6***
Nazwa UC	***Zmiana hasła***
Warunki wejścia do UC	*Wybranie przez użytkownika lub przez administratora podsystemu zarządzania tożsamością opcji „Zmień hasło" z menu zarządzania własną tożsamością.*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Wybranie opcji powoduje wyświetlenie strony zmiany hasła. Użytkownik podaje stare hasło, nowe hasło, drugi raz nowe hasło w celu potwierdzenia i zatwierdza zmianę.*
Cechy informacyjne	*[stare hasło, nowe hasło]*
Dodatkowe dane	-

Aktor	*Użytkownik.* *Administrator podsystemu zarzadzania tożsamością.*
Numer UC	***2.7***
Nazwa UC	***Zmiana statusu tożsamości***

Warunki wejścia do UC	*Wybranie przez użytkownika lub przez administratora podsystemu zarządzania tożsamością opcji „Zmień status tożsamości" z menu zarządzania własną tożsamością lub panelu administratora.*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Przypadek użycia umożliwia zmianę statusu tożsamości.* *1. Wybór tożsamości w panelu administratora* *1a. Brak kroku.* *2. Wybranie opcji umożliwia wybór jednego z dwóch statusów:* • *aktywny,* • *zawieszony.*
Cechy informacyjne	*[status tożsamości]*
Dodatkowe dane	-

Aktor	*Użytkownik.* *Administrator podsystemu zarządzania tożsamością.*
Numer UC	***2.8***
Nazwa UC	***Usuniecie tożsamości***
Warunki wejścia do UC	*Wybranie przez użytkownika lub przez administratora podsystemu zarządzania tożsamością opcji „Usuń tożsamość" z menu zarządzania własną tożsamością lub panelu administratora.*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Przypadek użycia umożliwia usunięcie tożsamości.*
Cechy informacyjne	
Dodatkowe dane	-

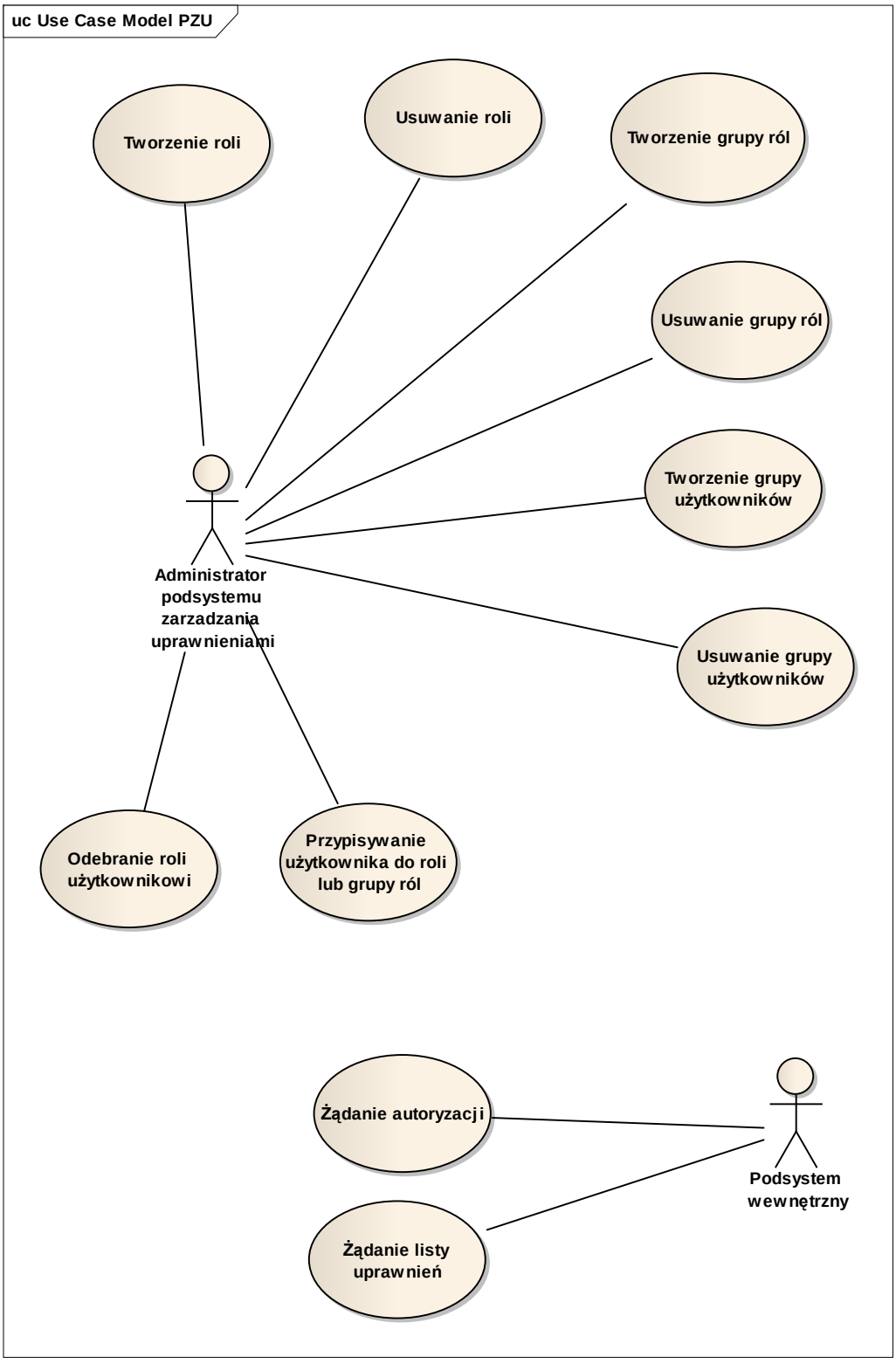
Aktor	*Użytkownik.* *Administrator podsystemu zarządzania tożsamością.* *System zewnętrzny.*
Numer UC	***2.9***
Nazwa UC	***Uwierzytelnienie***
Warunki wejścia do UC	*Wybranie przez dowolnego użytkownika SIOZ opcji „Zaloguj" lub wywołanie przez aplikację lub system usługi uwierzytelnienia z wykorzystaniem SAML.*
Okres wystąpienia	*Po aktywacji tożsamości.*
Opis	*W oknie uwierzytelnienia użytkownik może się uwierzytelnić za pomocą nazwy użytkownika i hasła lub wybrać inny sposób uwierzytelnienia.* *1a. Wybór sposobu logowania (opisane w oddzielnym przypadku użycia).* *1b. Wprowadzenie danych uwierzytelniających w postaci nazwy użytkownika i hasła.* *1c. Wywołanie procesu uwierzytelnienia przez aplikację lub system.*
Cechy informacyjne	*[dane uwierzytelniające, identyfikator sposobu uwierzytelnienia]*
Dodatkowe dane	-

Aktor	*Użytkownik* *Administrator podsystemu zarządzania tożsamością*
Numer UC	***2.10***
Nazwa UC	***Wybór sposobu uwierzytelnienia***
Warunki wejścia do UC	*Wybranie przez dowolnego użytkownika sposobu uwierzytelnienia w oknie logowania.*
Okres wystąpienia	*Po aktywacji okna uwierzytelnienia.*
Opis	*Możliwe jest wybranie jednego z dwóch sposobów uwierzytelnienia.* *1a. Wybór uwierzytelnienia przy pomocy certyfikatu.* *1b. Wybór uwierzytelnienia przy pomocy konta ePUAP z profilem zaufanym.* *2a. Podanie numeru PIN.* *2b. Wywołanie uwierzytelnienia w systemie ePUAP.* *3b. Odebranie asercji typu „SAML authentication response”.*
Cechy informacyjne	*[identyfikator sposobu uwierzytelnienia, token, klucz prywatny użytkownika służący do uwierzytelnienia, asercja typu „SAML authentication response]*
Dodatkowe dane	-

Aktor	*System zewnętrzny*
Numer UC	***2.11***
Nazwa UC	***Żądanie uwierzytelnienia***
Warunki wejścia do UC	*Wywołanie uwierzytelnienia przez system zewnętrzny, odebranie asercji typu „SAML authentication request”.*
Okres wystąpienia	
Opis	*Obsługa żądania uwierzytelnienia polega na:* *1. Uwierzytelnieniu zgodnie z przypadkiem użycia „Uwierzytelnienie”.* *2. Wysłanie asercji typu „SAML authentication response”.*
Cechy informacyjne	*[asercja typu „SAML authentication request”, asercja typu „SAML authentication response”]*
Dodatkowe dane	-

B. Podsystem Zarządzania Uprawnieniami

Podsystem zarządzania uprawnieniami ma realizować przypadki użycia przedstawione na poniższym diagramie.



Rysunek 11 – Model przypadków użycia dla Podsystemu Zarządzania Uprawnieniami

Aktor	*Administrator podsystemu zarzadzania uprawnieniami*
Numer UC	***3.1***
Nazwa UC	***Tworzenie roli***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „tworzenie ról”.*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Utworzenie roli polega na:* *1. Wprowadzeniu nazwy roli.* *2. Wprowadzeniu opisu.* *3. Określeniu obszaru dostępu (usługi)* *4. Zdefiniowaniu poziomu uprawnień.* *5. Dodanie identyfikatorów użytkowników i grup użytkowników.*
Cechy informacyjne	*[identyfikator roli, nazwa roli, opis roli, obszar dostępu (usługi), identyfikator usługi szyny P2, identyfikatory użytkowników i grup użytkowników]*
Dodatkowe dane	*-*

Aktor	*Administrator podsystemu zarządzania uprawnieniami*
Numer UC	***3.2***
Nazwa UC	***Usuwanie roli***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „usuwanie ról”.*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Usunięcie roli polega na:* *1. Wyborze roli do usunięcia.* *2. Usunięciu wskazanej roli.*
Cechy informacyjne	*[identyfikator roli]*
Dodatkowe dane	*-*

Aktor	*Administrator podsystemu zarządzania uprawnieniami*
Numer UC	***3.3***
Nazwa UC	***Tworzenie grupy ról***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „tworzenie grup ról”.*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Utworzenie grupy ról polega na:* *1. Wprowadzeniu nazwy grupy ról.* *2. Wprowadzeniu opisu.* *3. Określeniu ról przynależnych do grupy.* *4. Dodanie identyfikatorów użytkowników i grup użytkowników.*

Cechy informacyjne	*[identyfikator grupy ról, nazwa grupy ról, opis grupy ról, identyfikatory ról, identyfikatory użytkowników i grup użytkowników]*
Dodatkowe dane	-

Aktor	*Administrator podsystemu zarządzania uprawnieniami*
Numer UC	***3.4***
Nazwa UC	***Usuwanie grupy ról***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „usuwanie grup ról".*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Usunięcie grupy ról polega na:* *1. Wyborze grupy ról do usunięcia.* *2. Usunięciu wskazanej grupy ról.*
Cechy informacyjne	*[identyfikator grupy ról]*
Dodatkowe dane	-

Aktor	*Administrator podsystemu zarządzania uprawnieniami*
Numer UC	***3.5***
Nazwa UC	***Tworzenie grupy użytkowników***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „tworzenie grup użytkowników".*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Utworzenie grupy użytkowników polega na:* *1. Wprowadzeniu nazwy grupy użytkowników.* *2. Wprowadzeniu opisu.* *3. Określeniu użytkowników przynależnych do grupy.*
Cechy informacyjne	*[identyfikator grupy użytkowników, nazwa grupy użytkowników, opis grupy użytkowników, identyfikatory użytkowników przynależnych do grupy]*
Dodatkowe dane	-

Aktor	*Administrator podsystemu zarządzania uprawnieniami*
Numer UC	***3.6***
Nazwa UC	***Usuwanie grupy użytkowników***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „usuwanie grup użytkowników".*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Usunięcie grupy użytkowników polega na:* *1. Wyborze grupy użytkowników do usunięcia.* *2. Usunięciu wskazanej grupy użytkowników.*

Cechy informacyjne	*[identyfikator grupy użytkowników]*
Dodatkowe dane	-

Aktor	*Administrator podsystemu zarządzania uprawnieniami*
Numer UC	***3.7***
Nazwa UC	***Przypisywanie użytkownika do roli lub grupy ról***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „zarządzaj uprawnieniami".*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Przypisywanie użytkownika do roli lub grupy ról polega na:* *1. Wyborze roli lub grupy ról do przypisania użytkowników.* *2. Wskazaniu użytkowników i/lub grup użytkowników, którzy mają być dodani do roli lub grupy ról. Opcjonalnie wskazanie użytkowników spełniających wskazane kryteria np. (wszyscy użytkownicy zalogowani). Szczegółowy zakres kryteriów zostanie określony w trakcie realizacji projekty technicznego systemu.* *3. Zatwierdzeniu wyboru wskazanych użytkowników.*
Cechy informacyjne	*[i[identyfikator roli, identyfikator grupy ról, identyfikatory użytkowników i grup użytkowników]*
Dodatkowe dane	-

Aktor	*Administrator podsystemu zarządzania uprawnieniami*
Numer UC	***3.8***
Nazwa UC	***Odebranie roli użytkownikowi***
Warunki wejścia do UC	*Wybranie przez administratora podsystemu zarządzania uprawnieniami opcji „zarządzaj uprawnieniami".*
Okres wystąpienia	*Po uwierzytelnieniu w systemie.*
Opis	*Odebranie roli polega na:* *1. Wyborze roli lub grupy ról do usunięcia użytkowników.* *2. Wskazaniu użytkowników i/lub grup użytkowników, którzy mają być usunięci z roli lub grupy ról.* *3. Zatwierdzeniu usunięcia wskazanych użytkowników.*
Cechy informacyjne	*[identyfikator roli, identyfikator grupy ról]*
Dodatkowe dane	-

Aktor	*Podsystem wewnętrzny*
Numer UC	***3.9***
Nazwa UC	***Żądanie autoryzacji***
Warunki wejścia do UC	*Żądanie autoryzacji przez podsystem wewnętrzny, odebranie asercji typu „SAML authorization request".*
Okres wystąpienia	
Opis	*Żądanie weryfikacji czy użytkownik ma uprawnienia do danej usługi polega na:*

	1. Weryfikacja uprawnień dla żądania. *2. Wysłanie asercji „SAML authorization response”.*
Cechy informacyjne	*[asercja typu „SAML authorization request”, asercja typu „SAML authorization response”] – szczegółowy zakres przekazywanych parametrów zostanie określony w trakcie realizacji projektu technicznego systemu.*
Dodatkowe dane	*-*

Aktor	*Podsystem wewnętrzny*
Numer UC	***3.10***
Nazwa UC	***Żądanie listy uprawnień***
Warunki wejścia do UC	*Żądanie listy uprawnień dla określonego podmiotu przez podsystem wewnętrzny.*
Okres wystąpienia	
Opis	*Podsystem wewnętrzny żąda podania listy usług do których podmiot ma uprawnienia:* *1. Odebranie żądania z identyfikatorem użytkownika.* *2. Utworzenie listy usług do których uprawniony jest podmiot.* *3. Wysłanie listy usług do których uprawniony jest podmiot.*
Cechy informacyjne	*[identyfikator użytkownika, lista uprawnień] – szczegółowy zakres przekazywanych parametrów zostanie określony w trakcie realizacji projektu technicznego systemu.*
Dodatkowe dane	*-*

VIII. Dostawy systemu

A. Dostawa Systemu na zakończenie realizacji umowy

Dostawa systemu na zakończenie realizacji ma zawierać wszystkie komponenty niniejszego Opisu Przedmiotu Zamówienia (OPZ) wraz z kartą opisu dostawy, w której będą wskazane odwołania do poszczególnych opisów komponentów Systemu w niniejszym OPZ.

.

B. Dostawy Systemu w okresie gwarancji

W okresie gwarancji dostawy systemu każdorazowo powinny zawierać komplet nośników zgodnie z procedurą „modyfikacji oprogramowania” wypracowaną wspólnie z Zamawiającymi i zaakceptowaną przez Zamawiającego w tym między innymi komplet aktualnych plików zawierający:

1. Numer wersji systemu lub modułu systemu, który jest dostarczany.
2. Opis ograniczeń i wymagań wersji dla innych systemów, które powinny współpracować z SA – ograniczenia nie mogą być sprzeczne z wymaganiami zawartymi w SIWZ
3. Instrukcja instalacji i konfiguracji systemu lub modułu, który ulega aktualizacji.
4. Dokumentacja instalacji i konfiguracji serwerów oraz pozostałych części składowych infrastruktury systemu, odpowiadająca pełnemu zakresowi prac niezbędnych do wykonania przed instalacją i konfiguracją systemu zgodnie z instrukcją instalacji systemu lub modułu (pkt. 3).
5. Karta opisu dostawy zawierająca wykaz wszystkich niezbędnych elementów dostawy z dokładnością do nazw plików, obecnych na nośniku zawierającym dostawę, niezbędnych do instalacji, konfiguracji, kompilacji Systemu, oraz wykaz pozostałej dokumentacji obecnej na nośnik. Każdy plik na nośniku dostawy powinien posiadać wskazaną datę wersji pliku.

6. Komplet aktualnych testów akceptacyjnych Systemu, obejmujących komplet funkcji systemu.
7. Plan testów akceptacyjnych, pokrywający wykorzystanie wszystkich testów akceptacyjnych, o których mowa w pkt. 6.

IX. Normy i standardy

Ilekroć w dokumencie następuje odwołanie do standardu należy rozumieć standard wymieniony w niniejszej części lub nowszy. System ma być stworzony zgodnie z obowiązującymi normami i standardami.

1. Standardy Europejskiego Komitetu Normalizacyjnego

CEN CWA 14167-1:2003	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
CEN CWA 14167-2:2004	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)
CEN CWA 14167-4:2004	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP
CEN CWA 14169:2004	Secure Signature-creation devices "EAL 4+"
CEN CWA 14170:2004	Security requirements for signature creation applications
CEN CWA 14171:2004	General guidelines for electronic signature verification
CEN CWA 14172-1:2004	EESSI Conformity Assessment Guidance - Part 1: General introduction
CEN CWA 14172-3:2004	EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures
CEN CWA 14172-5:2004	EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices
CEN CWA 14172-6:2004	EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified
CEN CWA 14172-7:2004	EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services
CEN CWA 14172-8:2004	EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes
CEN CWA 14355:2004	Guidelines for the implementation of Secure Signature-Creation Devices
CEN CWA 14365-1:2004	Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects
CEN CWA 14365-2:2004	Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices

2. Standardy Kryptografii Klucza Publicznego (PKCS)

PKCS#1	RSA Cryptography Standard

PKCS#3	Diffie-Hellman Key Agreement Standard
PKCS#6	Extended-Certificate Syntax Standard
PKCS#7	Cryptographic Message Syntax Standard
PKCS#10	Certification Request Syntax Standard
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Syntax Standard

Standardy European Standards Organisation

TS 102 176-1	Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms
TS 102 176-2	Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures;Part 2: Secure channel protocols and algorithms for signature creation devices
TR 102 030	Provision of harmonized Trust Service Provider status information
TR 102 040	International Harmonization of Policy Requirements for CAs issuing Certificates
TR 102 045	Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model
TR 102 047	International Harmonization of Electronic Signature Formats
TR 102 272	Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies
TS 102 023	Electronic Signatures and Infrastructures (ESI);Policy requirements for time-stamping authorities
TS 101 861	Time stamping profile.
TS 102 280	X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

3. Standardy European Standards Organisation w zakresie podpisu elektronicznego w formacie XAdES, CAdES, PAdES.

TS 101 733	CMS Advanced Electronic Signatures (CAdES)
TS 102 734	Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)
TS 101 903	XML Advanced Electronic Signatures (XAdES)
TS 102 904	Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)
TS 102 778-1	PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES
TS 102 778-2	PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1
TS 102 778-3	PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles
TS 102 778-4	PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile
TS 102 778-5	PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures

4. Specyfikacje RFC

3161	Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)

5905	Network Time Protocol Version 4: Protocol and Algorithms Specification
2560	X.509 Internet Public Key Infrastructure; Online Certificate Status Protocol - OCSP
3986	Uniform Resource Identifier (URI): Generic Syntax
2616	Hypertext Transfer Protocol -- HTTP/1.1
2818	HTTP over TLS
4346	The Transport Layer Security (TLS) Protocol Version 1.1
2821	Simple Mail Transfer Protocol

5. Specyfikacje W3

SOAP wersja 1.1 z załącznikami	http://www.w3.org/TR/soap/
WSDL wersja 2.0	http://www.w3.org/TR/wsdl20/
SOAP MTOM	http://www.w3.org/TR/soap12-mtom
WS-I Basic Profile wersja 1.0	http://lists.w3.org/Archives/Public/www-ws-desc/2003Feb/0022.html
WS Policy wersja 1.5	http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm

6. Specyfikacje OASIS

UDDI wersja 3.x	http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm
WS-Security wersja 1.1	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
OASIS Digital Signature Services wersja 1.0	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss
OASIS Digital Signature Service Asynchronous Profile wersja 1.0	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss
OASIS Digital Signature Timestamp Profile wersja 1.0	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss
SAML wersja 2.0	http://saml.xml.org/saml-specifications

7. Specyfikacje SUN

JMS wersja 1.1	http://java.sun.com/products/jms/docs.html

8. Normy ISO i BS dotyczące systemów zarządzania

PN ISO/IEC 17799	Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji
PN ISO/IEC 27001	Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania
PN-ENISO27799	Informatyka w ochronie zdrowia - Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002
PN ISO/IEC 20000-1	Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja
PN ISO/IEC 20000-2	Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania
PN ISO/IEC 24762	Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie

BS 25999	Business continuity management
Projekt ISO/IEC 22301	Societal security — Preparedness and continuity management systems — Requirements

Dopuszcza się rozwiązania równoważne do opisanych przenoszące normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego.

9.Lista procedur bezpiecznej eksploatacji, które muszą zostać wytworzone w ramach przedmiotu zamówienia

Lp.	Kategoria	Nazwa procedury	Opis
1.	Procedury administracyjne	Procedura przydzielania / odbierania uprawnień	Opisuje sposób przyznawania uprawnień w ramach systemu P2.
		Procedura zgłaszania incydentów bezpieczeństwa	Opisuje sposób zgłaszania zaobserwowanych incydentów bezpieczeństwa.
		Procedura postępowania w trakcie wystąpienia incydentu bezpieczeństwa	Procedura dedykowana dla osób zajmujących się bezpieczeństwem teleinformatycznym.
		Procedura dystrybucji dokumentów	Specyfikuje sposób dystrybucji dokumentacji technicznej
		Procedura uzupełniania dokumentów	Opisuje ścieżkę administracyjną niezbędną do wprowadzenia i zaakceptowania zmian w dokumentacji technicznej.
2.	Bezpieczeństwo osobowe	Procedura szkolenia użytkowników systemu P2	Procedura opisująca wymagany poziom kwalifikacji i wymagane szkolenia niezbędne do pracy z systemem P2.
		Procedura nadawania uprawnień do dostępu do pomieszczeń dla personelu zewnętrznego	Procedura opisująca nadawanie uprawnień dla personelu technicznego firm trzecich, personelu sprzątającego itp.
		Procedura podwójnej kontroli	Opisuje sposób przeprowadzania podwójnej kontroli wraz z wymaganymi sposobami potwierdzenia .
3.	Ochrona fizyczna	Procedura kontroli dostępu	Opisuje sposób wnioskowania, nadawania i odbierania uprawnień do systemu kontroli dostępu.
		Procedury eksploatacji systemów alarmowych	Opisuje sposoby użytkowania systemów alarmowych chroniących pomieszczenia z urządzeniami technicznymi.
		Procedura wnoszenia/wynoszenia urządzeń technicznych	Przedstawia sposoby uzyskania zgody na wniesienie, lub wyniesienie urządzeń technicznych na teren pomieszczeń administracyjnych.
		Procedura niszczenia nośników danych	Procedura niszczenia nośników zawierających dane wrażliwe.
4.	Ochrona kryptograficzna	Procedura uruchomienia urządzenia kryptograficznego	Procedura opisująca uruchomienie urządzenia kryptograficznego, aż do trybu operacyjnego.

Lp.	Kategoria	Nazwa procedury	Opis
		Procedura generacji kluczy na urządzeniu kryptograficznym	Opisuje sposób generowania kluczy na urządzeniu kryptograficznym .
		Procedura wykonania kopii bezpieczeństwa kluczy kryptograficznych z urządzenia kryptograficznego	Opisuje sposób wykonywania bezpiecznej kopii kluczy, przechowywanych przez urządzenie kryptograficzne.
		Procedura importu kopii bezpieczeństwa kluczy kryptograficznych na urządzenie kryptograficzne	Opisuje sposób odtworzenia kopii kluczy utworzonych w ramach procedury backupu
		Procedura wyczyszczenia urządzenia kryptograficznego	Opisuje sposób usunięcia zawartości urządzenia kryptograficznego.
		Inicjalizacja urządzenia kryptograficznego	Opisuje sposób przygotowania urządzenia do pracy po pierwszym uruchomieniu.
		Instalacja i konfiguracja urządzenia kryptograficznego	Opisuje podłączenie urządzenia i instalacji sterowników.
		Wymiana urządzenia kryptograficznego	Opisuje procedurę wymiany urządzenia kryptograficznego ze wskazaniem na odzyskanie kopii bezpieczeństwa.
		Odłączenie urządzenia kryptograficznego	Opisuje sposób odłączenia urządzenia kryptograficznego od usług.
		Zatrzymanie urządzenia kryptograficznego	Opisuje proces przejścia urządzenia z trybu operacyjnego do momentu wyłączenia zasilania.
		Procedura generacji kart administratora	Opisuje proces generowania kart dostępowych do obsługi administracyjnej urządzenia.
		Procedura generacji kart operatora	Opisuje proces generowania kart dostępowych do obsługi pracy urządzenia w trybie operacyjnym.
5.	Bezpieczeństwo transmisji	Procedura współpracy z operatorami sieci zewnętrznych	Opisuje sposoby komunikacji z operatorami sieci zewnętrznych.
		Procedura instalacji switcha	Opisuje proces instalacji i podłączenia urządzenia typu switch.
		Procedura instalacji zapory sieciowej	Opisuje proces instalacji i uruchomienia zapory sieciowej.
		Procedura konfiguracji dostępu do urządzenia sieciowego	Opisuje sposób zabezpieczenia urządzenia sieciowego, poprzez zapewnienie dostępu tylko uprawnionym użytkownikom.
		Konfiguracja switcha do pracy w trybie active-standby	Opisuje sposób konfiguracji pracy switcha w trybie redundancji.

Lp.	Kategoria	Nazwa procedury	Opis
		Konfiguracja zapory sieciowej do pracy w trybie active-standby	Opisuje sposób konfiguracji pracy zapory sieciowej w trybie redundancji.
		Ustawienie parametrów bezpieczeństwa dla urządzenia sieciowego	Opisuje sposób implementacji polityki bezpieczeństwa dla urządzenia sieciowego.
		Podział sieci na segmenty VLAN	Opisuje sposób przydzielania identyfikatorów sieci VLAN dla poszczególnych interfejsów switcha.
		Procedura zestawienia tunelu VPN	Opisuje proces zestawienia szyfrowanego kanału VPN pomiędzy urządzeniami sieciowymi.
6.	Bezpieczeństwo urządzeń	Procedura bezpiecznej pracy	Opisuje zalecenia dotyczące bezpiecznej pracy przy urządzeniach zainstalowanych w systemie P2.
		Procedura przeglądu i konserwacji urządzeń	Opisuje sposób i czas przeglądów okresowych dla poszczególnych urządzeń.
		Procedura naprawy urządzenia	Opisuje sposób naprawy typowych awarii urządzeń technicznych.
		Procedura planowania przeglądów i napraw	Opisuje sposób planowania przeglądów i napraw urządzeń
7.	Bezpieczeństwo oprogramowania	Procedura modyfikacji oprogramowania operacyjnego	Opisuje sposób instalacji aktualizacji systemów operacyjnych wykorzystywanych w systemie P2.
		Procedura modyfikacji oprogramowania	Opisuje sposób instalacji aktualizacji oprogramowania wykonywanych w trakcie i po okresie gwarancyjnym
		Procedura instalacji usługi znakowania czasem	Opisuje sposób utworzenia usługi znakowania czasem wraz z wydaniem dla niej certyfikatu
		Procedura instalacji usługi OCSP	Opisuje proces utworzenia usługi OCSP, łącznie z wydaniem dla niej certyfikatu
		Procedura instalacji usługi weryfikacji podpisu	Opisuje proces instalacji i konfiguracji usługi weryfikacji podpisu zakończony uruchomieniem usługi.
		Procedura usunięcia usługi znakowania czasem	Opisuje proces wycofania usługi znakowania czasem z eksploatacji
		Procedura usunięcia usługi weryfikacji podpisu	Opisuje proces wycofania usługi weryfikacji podpisu z eksploatacji
		Procedura usunięcia usługi OCSP	Opisuje proces usunięcia z eksploatacji usługi OCSP, wraz z unieważnieniem certyfikatu.
		Procedura modyfikacji oprogramowania użytkowego	Opisuje sposób instalacji poprawek w ramach oprogramowania świadczącego usługi w systemie P2
		Procedura wprowadzania nowego oprogramowania	Opisuje proces uzyskania niezbędnych pozwoleń, oraz ścieżkę zamawiania nowego oprogramowania.
		Procedura defragmentacji dysku	Opisuje sposób uruchomienia narzędzi do defragmentacji dysków

Lp.	Kategoria	Nazwa procedury	Opis
		Procedura zarządzaniem kont użytkowników systemu operacyjnego	Opisuje sposób dodawania i usuwania kont w systemach operacyjnych.
		Procedura uwierzytelnienia użytkowników	Opisuje proces uwierzytelnienia użytkowników w różnych systemach i na urządzeniach
		Procedura konfiguracji uprawnień	Opisuje sposób konfiguracji profili uprawnień, oraz przypisywania ich do poszczególnych kont użytkowników
		Procedura kontroli antywirusowej	Opisuje sposób i częstotliwość uruchomienia kontroli przed złośliwym oprogramowaniem, na stacjach i serwerach w ramach systemu P2
		Procedura kontroli antywirusowej nośników	Opisuje sposób uruchomienia skanowania zewnętrznych nośników danych.
		Procedura aktualizacji oprogramowania antywirusowego	Opisuje metody aktualizacji baz sygnatur dla oprogramowania antywirusowego
		Procedura zarządzania wersji instalacyjnych oprogramowania	Opisuje procesy obsługi biblioteki oprogramowania zawierającej zarejestrowane nośniki.
8.	Zarządzanie konfiguracją	Procedura tworzenia konfiguracji bazowej	Opisuje proces tworzenia i rejestrowania konfiguracji bazowej służącej, jako punkt odniesienia w przypadku wprowadzonych zmian.
		Procedura wprowadzania zmian w konfiguracji	Opisuje proces uzyskiwania niezbędnych pozwoleń, oraz warunki niezbędne do wykonania zmian w konfiguracji usług i urządzeń w ramach systemu P2
9.	Utrzymanie dostępności usług	Procedura tworzenia i odzyskiwania kopii zapasowych	Opisuje sposób tworzenia kopii zapasowej na żądanie użytkownika
		Procedura przełączania ośrodków	Opisuje czynności niezbędne do przeniesienia przetwarzania do ośrodka zapasowego
		Procedura odtwarzani ośrodka po awarii	Opisuje czynności wykonywane podczas odzyskiwania usług w ośrodku podstawowym.
		Procedura naprawy serwisowej	Opisuje proces zgłaszania naprawy serwisowej
		Procedura wymiany urządzenia	Opisuje warunki i czynności niezbędne do wykonania bezpiecznej wymiany urządzenia.
		Procedura wymiany podzespołu	Opisuje czynności niezbędne do wykonania wymiany podzespołu w urządzeniu działającym w systemie P2.
		Procedury zabezpieczenia zapasowych urządzeń i materiałów eksploatacyjnych	Opisuje sposób zabezpieczenia materiałów eksploatacyjnych wymaganych do wykonywania procesów realizowanych w Systemie P2

Lp.	Kategoria	Nazwa procedury	Opis
		Główna procedura obsługi incydentów bezpieczeństwa	Ogólna procedura przetwarzania i reakcji na incydenty bezpieczeństwa.
10.	Postępowanie w sytuacji kryzysowej	Procedura uruchomienia planu zachowania ciągłości działania	Zawiera kryteria uruchomienia i proces wdrożenia planu zachowania ciągłości działania.
		Procedura szkolenia z zakresu zachowania ciągłości działania	Opisuje częstotliwość i zakres przeprowadzania szkoleń z zakresu zachowania ciągłości działania po wystąpieniu sytuacji kryzysowych
11.	Rozliczalność zdarzeń i audytowanie	Główna procedura obsługi zdarzeń	Opisuje proces przetwarzania zdarzeń systemowych rejestrowanych przez system monitorujący.
		Procedura przeglądu dzienników zdarzeń	Opisuje sposób dostępu i przeglądania dzienników zdarzeń systemów i usług.
		Procedura archiwizacji dzienników zdarzeń	Opisuje proces archiwizacji i czyszczenia dzienników zdarzeń.
		Procedura dokumentowania audytów i kontroli bezpieczeństwa systemów	Opisuje proces dokumentowania przeprowadzanych kontroli i audytów bezpieczeństwa.
		Procedura kontroli aktualności oprogramowania	Opisuje sposób pozyskiwania informacji o wersjach aktualnie zainstalowanego oprogramowania, oraz skanowaniu w celu wykrycia zainstalowanych poprawek.
		Procedura monitorowania zasobów	Opisuje sposób monitorowania dostępności, oraz pojemności urządzeń działających w systemie P2

10. Serwis gwarancyjny

W ramach realizacji zamówienia Zamawiający będzie żądał po zakończeniu umowy (podpisaniu bez uwag protokołu zakończenia III etapu) 36 miesięcznego bezpłatnego serwisu gwarancyjnego świadczonego przez Wykonawcę niniejszego zamówienia.