Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Opis Przedmiotu Zamówienia

Rozbudowa systemu BackOffice o niezbędne funkcjonalności dla procesu atestacji W1 (rozbudowa) oraz W2

SPIS TREŚCI

1. Definicje

Administrator IT – Użytkownik Wewnętrzny z najwyższymi uprawnieniami do Systemu, umożliwiającymi dostęp do wszystkich funkcjonalności Systemu.

Administrator Konta Klienta – osoba upoważniona do administrowania Kontem Klienta w tym nadawania uprawnień oraz tworzenia nowych kont dla Pracowników Klienta. Posiada wszystkie uprawnienia Pracownika Klienta.

Aplikacja mobilna – aplikacja działająca na urządzeniach przenośnych, natywna lub PWA, dostępna dla urządzeń z systemem Android oraz IOS (obsługiwane wszystkie aktualne wersje systemów)

Błąd krytyczny - całościowy brak dostępu do Systemu lub jego kluczowych podzespołów uniemożliwiający jakąkolwiek pracę z Systemem bądź zatrzymanie lub poważne zakłócenie pracy Systemu, polegające na niemożliwości wykonania jednej z funkcji mającej wpływ na kluczowe procesy biznesowe aplikacji bez możliwości obejścia problemu, kontynuowania prac.

Błąd niekrytyczny – błąd mający wpływ na działanie funkcji Systemu, jednak nie ograniczający jego zdolności operacyjnych i nie mający wpływu na kluczowe procesy biznesowe Systemu.

Błędy - każda nieprawidłowość w działaniu Systemu, w szczególności wobec wymagań opisanych w niniejszym dokumencie i załącznikach, w tym w OPZ.

Certyfikat – Atest lub Świadectwo Jakości Zdrowotnej wydawane dla produktu/grupy produktów przez Narodowy Instytut Zdrowia Publicznego PZH – Państwowy Instytut Badawczy.

Dokumentacja - Wszelka dokumentacja dotycząca Systemu, kodów źródłowych lub jakichkolwiek innych rezultatów prac Wykonawcy, w tym też ich zmiany lub modyfikacji, która powstanie i zostanie przekazana Zamawiającemu w ramach realizacji Umowy. Dokumentacja obejmuje w szczególności: dokumentację administratora, dokumentację techniczną, dokumentację użytkownika, dokumentację powykonawczą politykę bezpieczeństwa oraz dokumentację w wersji elektronicznej wbudowaną w System, dotyczącą stworzonego i wdrożonego Systemu. Szczegółowe wymagania dla Dokumentacji są uszczegółowione w rozdziale 14. Dokumentacja.

Dystrybutor – podmiot gospodarczy, który odpowiada za dostępność produktu na rynku.

Dzień roboczy - Dzień od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczpospolitej Polskiej.

Firmowy Adres Email – adres email firmy podany w rejestrach publicznych

Klient – osoba zarejestrowana do Systemu, posiadająca konto w Systemie. Może to być Producent, Dystrybutor lub pełnomocnik (Producenta/Dystrybutora)

Komponent – część składowa realizowanego Systemu

Konto Klienta – konto z danymi Klienta, z przypisanymi dostępami Administratora Konta Klienta, Pracowników Klienta.

Modyfikacje Systemu - zmiana Systemu wynikająca ze zmian powszechnie obowiązujących przepisów prawnych, prawnych regulacji dotyczących Zamawiającego, prawnych regulacji do których Zamawiający się stosuje oraz dodania nowych funkcjonalności na wniosek Zamawiającego

Numer CAS – oznaczenie numeryczne przypisane substancji chemicznej przez amerykańską organizację Chemical Abstracts Service (CAS), pozwalające na identyfikację substancji.

Oprogramowanie dedykowane - Oprogramowanie Systemu, stworzone i wdrożone na potrzeby realizacji Umowy, obejmujące też wszelkie modyfikacje i rozszerzenia Oprogramowania Standardowego (może być indywidualizowane), lecz nie będące Oprogramowaniem Standardowym. Jeżeli dane Oprogramowanie nie zostało przypisane do Standardowego oprogramowania systemowego lub Standardowego oprogramowania aplikacyjnego uważa się je za Oprogramowanie dedykowane.

Oprogramowanie standardowe - Oprogramowanie niezbędne do zbudowania, uruchomienia i przetestowania Systemu oraz zagwarantowania prawidłowego funkcjonowania środowiska Systemu, które musi być zapewnione przez Wykonawcę w ramach wykonywania Umowy celem prawidłowego działania Systemu, zgodnie z wszelkimi wymaganiami Zamawiającego. Za Oprogramowanie Standardowe uznaje się również oprogramowanie niezbędne do zbudowania, uruchomienia i przetestowania Wdrożenia oraz zagwarantowania prawidłowego funkcjonowania środowiska Systemu, wytworzone przez Wykonawcę, posiadające oznaczenia: nazwę producenta, numer wersji, nazwę handlową lub znak towarowy, jak też to, które było oprogramowaniem skutecznie wdrożonym i opisanym w dokumentacji technicznej, w tym użytkownika i administratora, udostępnionej na każde wezwanie Zamawiającego, jak też będące w obrocie w wersji pierwotnej przed zawarciem Umowy. Do Oprogramowania Standardowego jest zapewniona pełna dostępność usług z nim związanych na zasadach rynkowych, poprzez powszechnie jawne informacje.

Podmiot, dla którego został wydany Certyfikat – podmiot gospodarczy, mogący korzystać z wydanego Certyfikatu (np. Użytkownik produktu, Dystrybutor, Producent)

Pracownik Klienta – wskazany przy rejestracji Konta Klienta pracownik firmy.

Producent – podmiot gospodarczy, który prawnie odpowiada za wytworzenie produktu.

PWA - Progressive web application – progresywna aplikacja internetowa uruchamiana tak jak zwykła strona internetowa, ale umożliwiająca stworzenie wrażenia działania jak natywna aplikacja mobilna lub aplikacja desktopowa

System W1 (rozbudowa) i W2, System – rozbudowa systemu BackOffice o niezbędne funkcjonalności dla procesu atestacji – W1 (rozbudowa) oraz W2. System zaprojektowany, zbudowany i wdrożony w ramach przedmiotu umowy, w skład którego wchodzą:

- Panel Klienta – responsywny portal dostępny w przeglądarce internetowej na desktopie i urządzeniu przenośnym (tablety, smartfony, itp.), dostępny dla Użytkowników Zewnętrznych w zakresie obsługi procesu atestacji (złożenie wniosku o atestację, płatność, kontrolowanie certyfikowanych produktów, uzyskanie Certyfikatu).
- Panel administratora – responsywny portal dla Użytkowników Wewnętrznych służący do administrowania komponentami Systemu
- W1 – rozbudowa warstwy wspierającej obsługę procesu atestacji, realizowanej w ramach obecnie wdrażanego projektu BackOffice

Usprawnienia Systemu - zmiana Systemu wynikająca z usuwania Błędów, dodawania/zmiany funkcjonalności, dostosowania do aktualnych regulacji wewnętrznych NIZP PZH-PIB i prawnych

Użytkownik produktu –Klient, który w swojej działalności wykorzystuje produkt, na który chce uzyskać Certyfikat.

Użytkownik Wewnętrzny – pracownik Zamawiającego posiadający uprawnienia do pracy w Systemie

Użytkownik Zewnętrzny – Klient zarejestrowany (posiadający odpowiednie konto) w Systemie

Wersje Systemu - zmiana Systemu wynikająca z postępu technologicznego i technicznego

Wnioskodawca – podmiot gospodarczy który składa wniosek (np. Użytkownik produktu, Dystrybutor, Producent, Pełnomocnik). Może składać wniosek w imieniu własnym lub w imieniu Zleceniodawcy (np. Producenta, Dystrybutora).

Zleceniodawca – podmiot gospodarczy zlecający Wnioskodawcy złożenie Wniosku o certyfikację, wersję w języku obcym/kopię/duplikat lub zmianę.

2. Wprowadzenie

Rozbudowany System BackOffice (W1 i W2) będzie wspierał:

- Proces atestacji realizowany przez Użytkowników wewnętrznych (W1 wraz z rozbudową), tj. obsługę Wniosku od momentu złożenia go przez Klienta (zapis Wniosku w bazie danych, rejestracja Wniosku, komunikacja z Klientem, zmiany we Wniosku (rejestracja zmian, historia zmian), polecenie zapłaty, obsługa płatności, zarejestrowanie sprawy, dekretacja, realizacja (statusy), wystawienie Certyfikatu/ negatywne zakończenie atestacji (odpowiednie zapisy dotyczące Certyfikatu w bazie danych), przekazanie Certyfikatu i faktury do W2.
- Proces uzyskiwania Certyfikatu przez Klienta – Panel Klienta W2 (założenie Konta na Panelu Klienta, wypełnienie i złożenie Wniosku (odpowiednie zapisy w bazie danych), wprowadzanie zmian we Wniosku, wprowadzanie Produktów, dodawanie załączników, komunikacja z Użytkownikami Wewnętrznymi).

Projektowany System w zakresie W1 (rozbudowa) i W2 będzie obejmował:

1. **W1 –** warstwa wspierająca obsługę procesu atestacji, realizowana w ramach obecnie wdrażanego projektu BackOffice w oparciu w szczególności o oprogramowanie enova365 i EZD PUW - rozbudowywana w niniejszym postępowaniu.
2. **W2** – responsywny Panel Klienta wraz z Panelem Administracyjnym - objęty niniejszym postępowaniem przetargowym.
3. **W3** – aplikacja mobilna i portal www służące głównie do sprawdzania czy dany produkt posiada Certyfikat/zawiera niebezpieczne substancje chemiczne - będzie przedmiotem osobnego postępowania przetargowego.

Objęty niniejszym zamówieniem System W1 (rozbudowa) i W2 zawiera:

- Komponent udostępniany publicznie - responsywny Panel Klienta
- Komponent wspierający - Panel Administratora
- Komponenty wewnętrzne stanowiące rozbudowę systemu BackOffice.

Powyższe komponenty zostaną zintegrowane poprzez szynę danych zewnętrzną/wewnętrzną z elementami systemów planowanych do wdrożenia, wdrażanych lub użytkowanych obecnie w NIZP PZH-PIB.

We wszystkich zapisach SWZ oraz jej załącznikach, w tym w niniejszym OPZ, w których Zamawiający odwołuje się do norm, aprobat, specyfikacji technicznych lub systemów odniesienia Zamawiający dopuszcza rozwiązania równoważne. W przypadku, gdy w opisie przedmiotu zamówienia podano nazwy rozwiązań, oprogramowania lub urządzeń konkretnych producentów to należy traktować to jedynie jako określenie pożądanego standardu i jakości. We wszystkich takich sytuacjach Wykonawca może zaoferować równoważne rozwiązania o co najmniej takich samych parametrach. Przez równoważność rozumie się zaoferowanie rozwiązania, którego parametry techniczne i funkcjonalności są co najmniej takie same jak opisanych w SWZ. W przypadku zaoferowania rozwiązania równoważnego, Wykonawca zobowiązany jest wykazać równoważność zastosowanych rozwiązań. Wdrożenie rozwiązania równoważnego wymaga zatwierdzenia przez Zamawiającego.

3. Zakres zamówienia

Zaprojektowanie, wybudowanie i wdrożenie oprogramowania spełniającego wskazane w niniejszym dokumencie i załącznikach wymagania funkcjonalne i poza funkcjonalne.

Oprogramowanie dedykowane będzie wdrożone na platformie oprogramowania/podsystemów/bibliotek zgodnych z wymaganiami wskazanymi w niniejszym opracowaniu. Wykonawca przekaże pełne niezaciemnione (ang. „obfusscation") kody źródłowe Oprogramowania dedykowanego opisanego wraz z nieusuniętymi komentarzami oraz autorskie prawa majątkowe w zakresie pól eksploatacji i na zasadach określonych w Umowie.

Zakres zamówienia obejmuje:

1. Wykonanie szczegółowego Projektu Technicznego
2. Wykonanie Projektu Graficznego Systemu.
3. Budowę i dostarczenie Systemu W1 (w zakresie rozbudowy/uzupełnienia obecnie realizowanego w ramach BackOffice procesu PB2.Sprzedaż i P.3.18 Atesty) i Panelu Klienta wraz z Panelem Administracyjnym (W2)
4. Dostarczenie Oprogramowania dedykowanego wraz kodami źródłowymi i prawami autorskimi.
5. Dostarczenie Oprogramowania standardowego wraz z odpowiednimi licencjami.
6. Wdrożenie Systemu W1 (rozbudowa) i W2.
7. Migrację danych
8. Dostawę dokumentacji (szczegółowy opis znajduje się w rozdziale 13) dostarczanego Systemu
9. Przeprowadzenie Szkoleń dla Użytkowników Wewnętrznych i Administratorów.
10. Przygotowanie e-learningu i testów wiedzy
11. Przeprowadzenie Audytu bezpieczeństwa Systemu (w tym Testów penetracyjnych Systemu) i przygotowanie raportu
12. Przeprowadzenie Testów użyteczności (UX) i przygotowanie raportu
13. Przeprowadzenie audytu dostępności cyfrowej (WCAG) i przygotowanie raportu zgodnego z Ustawą z dnia 4 kwietnia 2019 o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.
14. Asystę Techniczną i Usługi Rozwojowe dla Systemu W1 (rozbudowa) i W2 w wymiarze 500 roboczogodzin realizowaną na zlecenie Zamawiającego bez dodatkowych kosztów .
15. Udzielenie Gwarancji na wdrożony System i świadczenie usług w zakresie Gwarancji:
    a. Okres gwarancji minimum 24 miesięcy od zakończenia wdrożenia (Odbioru końcowego Systemu)
    b. W każdym przypadku, w którym będzie to możliwe, Wykonawca będzie świadczył opiekę serwisową/gwarancyjną w sposób zdalny.
    c. Usługi gwarancyjne świadczone na zasadach SLA określonych w Umowie
16. Dostarczanie nowych wersji Systemu w okresie gwarancji wraz z ich instalacją i konfiguracją w celu zapewnienia zgodności z Regulaminem procesu atestacji NIZP PZH-PIB i aktualnym stanem prawnym.
17. Aktualizację dokumentacji będącą wynikiem aktualizacji komponentów Systemu.
18. Usługi rozwojowe w okresie gwarancji w wymiarze co najmniej 1000 roboczogodzin oraz stawka za roboczogodzinę po przekroczeniu puli godzin dostępnych w ramach zamówienia (zamówienie objęte prawem opcji).

Termin realizacji

Projekt realizowany będzie przyrostowo w ramach wskazanych poniżej etapów.
Realizacja przedmiotu zamówienia podzielona została na następujące etapy zarządcze:

1) Etap 1 – Projekt techniczny nie później niż do 1 miesiąca od podpisania umowy.
2) Etap 2 – Budowa, wdrażanie i testy Systemu – max. do 5 miesięcy od podpisania umowy. Etap 2 realizowany będzie w formie kolejnych Wydań podlegających odbiorom. Wykonawca powinien samodzielnie określić zakres i daty Wydań, które będą odbierane przez NIZP PZH-PIB.
3) Etap 3 – Stabilizacja Systemu– do 2 miesięcy od podpisania umowy.

W ramach etapu 2 Wykonawca wskaże i uwzględni w Harmonogramie co najmniej 3 Etapy techniczne (Wydania) i wskaże w Projekcie Technicznym, które wymagania Zamawiającego zostaną zrealizowane w danym etapie technicznym (zgodnie z zapisami w rozdziale Projekt Techniczny).

5. Ogólna architektura Systemu W1 (rozbudowa) i W2

Środowisko Systemu W2 zlokalizowane będzie w wydzielonej infrastrukturze NIZP PZH-PIB.

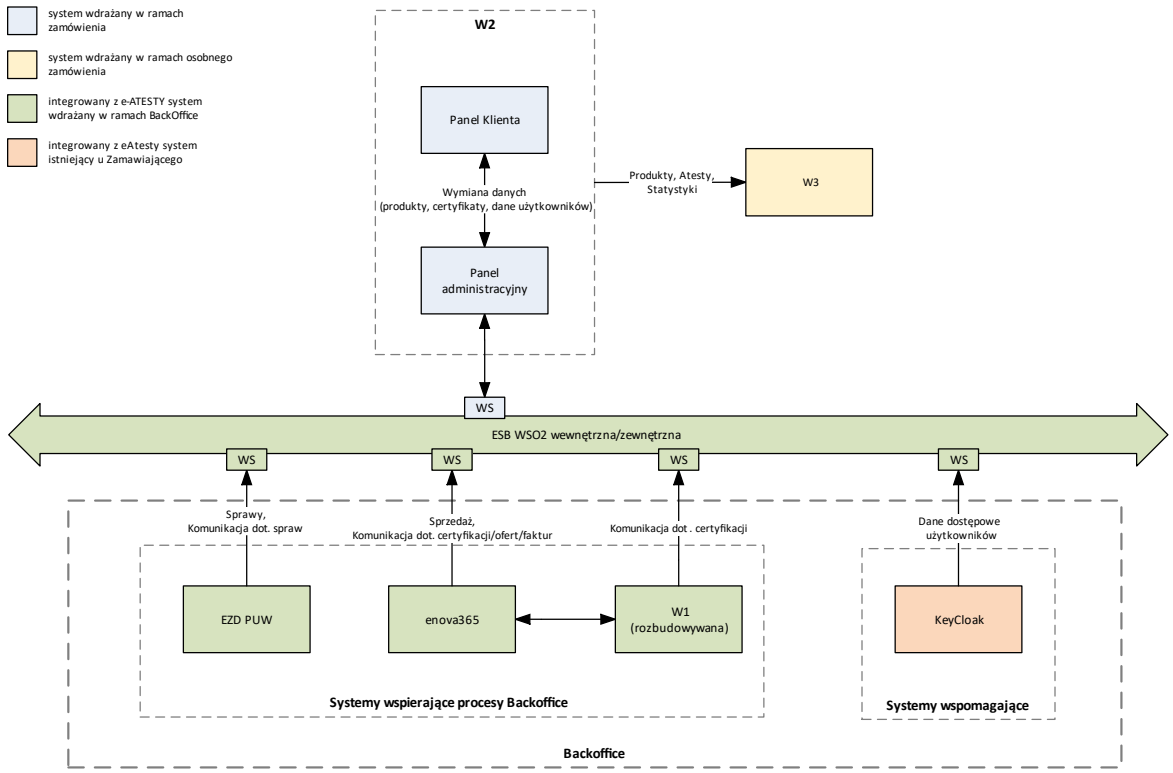
System zbudowany zostanie w oparciu o 3 elementy:

1. W1 - Realizowany obecnie w ramach projektu Dostawa i wdrożenie komponentów systemu BackOffice NIZP PZH-PIB w ramach projektu pn. "Rozwój nowoczesnych wewnętrznych technologii informacyjno-komunikacyjnych dla usług świadczonych drogą elektroniczną w Narodowym Instytucie Zdrowia Publicznego -Państwowym Zakładzie Higieny (NIZP PZH - PIB)" i rozbudowywany w ramach niniejszego OPZ
2. W2 – objęty niniejszym OPZ planowany do realizacji w ramach projektu pn. "Rozwój nowoczesnych wewnętrznych technologii informacyjno-komunikacyjnych dla usług świadczonych drogą elektroniczną w Narodowym Instytucie Zdrowia Publicznego - Państwowym Zakładzie Higieny (NIZP PZH - PIB)"
3. W3 - planowany do realizacji (osobne postepowanie) w ramach projektu pn. „E-ATESTY uruchomienie e-usługi za pośrednictwem dedykowanej aplikacji mobilnej wspieranej interoperacyjną platformą informatyczną" współfinansowanego ze środków EFRR w ramach POPC na lata 2014-2020, Oś Priorytetowa nr 2 „E-administracja i otwarty rząd" Działanie nr 2.4 „Tworzenie usług i aplikacji wykorzystujących e-usługi publiczne i informacje sektora publicznego"

System W2 będzie zintegrowany z systemami NIZP PZH-PIB zgodnie z architekturą zorientowaną na usługi (SOA). Integracje pomiędzy systemami odbywają się w oparciu o:

1. Wymianę usług poprzez usługi sieciowe (Web Serwisy) udostępniane przez poszczególne systemy na szynach danych ESB WSO2:
   a. wewnętrznej (LAN) – dla usług wykorzystywanych przez Użytkowników Wewnętrznych – pracowników NIZP PZH-PIB
   b. zewnętrznej (DMZ) – dla usług wykorzystywanych przez systemy dostępne na zewnątrz NIZP PZH-PIB, używane przez Użytkowników Zewnętrznych
2. Wymianę danych poprzez centralne repozytorium danych RDBMS i warstwę wirtualizacji danych

Ogólną architekturę systemów NIZP PZH-PIB zintegrowanych w ramach architektury SOA, mających wpływ na niniejsze Zamówienie przedstawiono na poniższym diagramie:



Elementy przedstawione na diagramie architektury to:

1. Komponenty Systemu W2:
   a. Panel Klienta – dostępny dla Klientów responsywny portal w przeglądarce internetowej służący przede wszystkim do obsługi procesu atestacji (złożenia wniosku, płatność, kontrolowanie certyfikowanych produktów, uzyskanie Certyfikatu) oraz do pozyskiwania informacji w szczególności na temat atestacji.
   b. Portal administracyjny – portal dla Użytkowników Wewnętrznych służący do administrowania komponentami Systemu W2
2. Pozostałe elementy architektury:
   a. W1 – obsługa procesu atestacji przez Użytkowników wewnętrznych (podlega rozbudowie w ramach obecnego postępowania)
   b. W3 – aplikacja mobilna i portal www służący do sprawdzania czy produkt posiada Certyfikat, W3 zasilany będzie niezbędnymi danymi z W2.
   c. System obiegu dokumentów EZD PUW
   d. Integracyjna szyna danych ESB WSO2 (wewnętrzna i zewnętrzna)
   e. KeyCloak - system zarządzania dostępem i uwierzytelniania użytkowników
   f. Oznaczenie „WS” oznacza usługę sieciową (Webservice), odpowiedzialną za przekazywanie danych zaznaczonych na strzałce prowadzącą od systemu do szyny danych.

Informacje szczegółowe na temat koncepcji integracji poszczególnych komponentów Systemu z systemami NIZP PZH-PIB znajdują się w rozdziale Integracje.

Szczegółowy zakres danych i usług udostępnianych przez System będzie uzgodniony i opracowany na etapie Projektu Technicznego.

System operacyjny

Oprogramowanie musi zostać zainstalowane na udostępnionej przez Zamawiającego platformie sprzętowo-programowej opartej o jeden ze wskazanych niżej systemów operacyjnych:

1. Linux – preferowany przez Zamawiającego
2. Windows Server – Zamawiający posiada licencje na system operacyjny Windows Server

Wykorzystanie baz danych

W przypadku korzystania przez System z platformy bazy danych będzie ona oparta o jedną ze wskazanych niżej platform danych w wersji stabilnej i najbardziej aktualnej na dzień zawarcia Umowy:

1. MySQL,
2. PostgreSQL,
3. MongoDB,
4. Microsoft SQL Server.

Wykorzystanie serwerów WWW

Dla elementów Systemu stosować można alternatywnie następujące serwery w wersji stabilnej i najbardziej aktualnej na dzień zawarcia Umowy:

1. Nginx
2. WildFly,
3. Apache / Tomcat
4. IIS Microsoft,

6. Wymagania dla Systemu

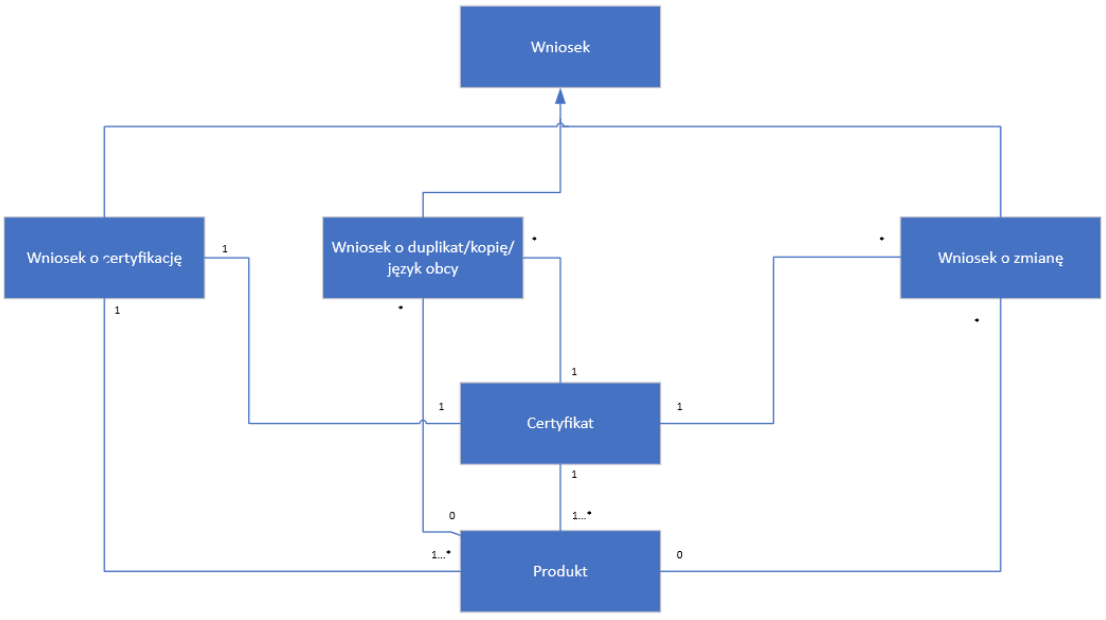
Poszczególne elementy Systemu powinny spełniać poniższe wymagania:

1. **Modułowość** pozwalająca na wyłączenie bądź zastąpienie poszczególnych modułów Systemu bez utraty integralności danych oraz w sposób zapewniający poprawność działania pozostałych modułów Systemu.
2. **Trójwarstwowa architektura** z wydzieloną warstwą interfejsu użytkownika (front-end), warstwą logiki biznesowej (middleware) i warstwą danych (database).
3. **Udokumentowane interfejsy programistyczne** (API) pozwalające na integrację poszczególnych systemów i ich modułów w ramach architektury usługowej przez niezależnych dostawców (integratorów).
4. **Udokumentowana struktura bazy danych** pozwalająca na dostęp do danych przechowywanych w warstwie bazodanowej poszczególnych systemów na potrzeby ich wirtualizacji i wykorzystania przez systemy zewnętrzne.
5. **Interfejs webowy** pozwalający na dostęp przez najbardziej popularne przeglądarki internetowe (Microsoft Edge, Chrome, Mozilla Firefox, Opera, Safari) spełniający wymagania dla osób z dysfunkcjami. Dostęp realizowany przez szyfrowane połączenie HTTPS zabezpieczony powszechnie rozpoznawalnym certyfikatem SSL.
6. **Responsywność** – System musi być responsywny, a więc taki który dostosowuje swoją zawartość do urządzenia na jakim jest wyświetlany, ze szczególnym uwzględnieniem rozdzielczości ekranów urządzeń mobilnych (smartfonów i tabletów).
7. **Interfejs GUI** Systemu musi być w polskiej i angielskiej wersji językowej. GUI będzie zgodny z Księgą Marki NIZP PZH-PIB lub ze wskazaną przez Instytut kolorystyką.
8. **Autentykacja** pomiędzy Systemem a serwerami danych i usług zaplecza powinna odbywać się w sposób zapewniający bezpieczny delegowany dostęp zgodnie ze standardem OAuth w wersji 2.0 (lub nowszej) lub równoważnym dla wybranej technologii.
9. **Otwartość Systemu** umożliwiająca jego skalowalność poprzez rozbudowę funkcjonalności.
10. Zgodność z normą europejską **WCAG** (Web Content Accessibility Guidelines) w obowiązującej na dzień odbioru Systemu wersji oraz Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych z późniejszymi zmianami.
11. Zgodność ze standardami - System zostanie wykonany z zastosowaniem najlepszych praktyk w dziedzinie budowania witryn WWW i w zgodności z najnowszymi standardami, wyznaczonymi przez W3C. Wymagana jest prawidłowa walidacja tworzonego kodu HTML i CSS za pomocą udostępnionego na stronach W3C walidatora (http://validator.w3.org)
12. **SLA** – dostarczony System powinien być objęty umową SLA. Zakres SLA opisany w rozdziale Asysta i Konserwacja Techniczna.
13. **Kopie zapasowe** zapewnienie przez Wykonawcę rozwiązania pozwalającego na tworzenie kopii zapasowych danych gromadzonych w Systemie z wykorzystaniem istniejącego u Zamawiającego narzędzia Veeam Enterprise Edition. Rozwiązanie powinno realizować następujące wymagania:
    a. możliwość zabezpieczenia danych przed ich celowym lub przypadkowym usunięciem
    b. zarządzanie kopiami zapasowymi z poziomu konsoli fizycznej (wiersz polecenia) oraz poprzez graficzny interfejs
    c. możliwość odtworzenia Systemu lub jego elementów po błędach.

d. wykonywanie kopii zapasowych plików konfiguracyjnych, logów systemowych oraz dzienników zdarzeń.
e. w ramach Dokumentacji Administratora, Wykonawca opracuje i przekaże instrukcję odtwarzania Systemu lub jego części na podstawie kopii zapasowych. W Dokumentacji Technicznej powinien znaleźć się proces tworzenia kopii zapasowych.
f. podczas wykonywania kopii zapasowej będą tworzone każdorazowo po dwie kopie, które będą przechowywane w miejscach wskazanych przez Zamawiającego, w miejscu bezpiecznym, zapewniającym ochronę przed dostępem osób nieuprawnionych, modyfikacją, uszkodzeniem, zniszczeniem oraz wpływem środowiska.
g. kopie zapasowe Systemu należy tworzyć przynajmniej w następującym cyklu:
   - pełny backup - raz w tygodniu
   - backup przyrostowy lub różnicowy – raz dziennie;
h. kopie zapasowe powinny być zabezpieczone przed nieuprawnionym dostępem.
i. okres przechowywania kopi zapasowych wynosi 3 miesiące od wytworzenia. Po ustaniu użyteczności kopii zapasowych są one usuwane. Po upływie okresu przechowywania nośnik może być wykorzystany ponownie po wcześniejszym upewnieniu się, iż wcześniejsze dane zostały w sposób trwały usunięte. Wykorzystując ponownie ten sam nośnik należy bezwzględnie weryfikować poprawność zapisu i możliwość odczytania jego zawartości. Za procedurę tworzenia kopii zapasowych i wady kopii zapasowych powstałe na skutek błędnej procedury, Wykonawca ponosi odpowiedzialność na zasadzie ryzyka.
j. Wykonawca określi procedury wykonywania i odtwarzania kopii zapasowych. Zamawiający zgodnie z przekazaną Dokumentacją Administratora będzie wykonywał kopie zapasowe oraz okresowo sprawdzał poprawność wykonania kopii zapasowych.

Główne obiekty danych w Systemie

Poniższy diagram przedstawia główne obiekty danych, które będą przetwarzane w Systemie.



1. Wniosek - obiekt danych zawierający metadane opisane w wymaganiach oraz dane wypełniane przez Użytkowników Zewnętrznych w formularzach. Wniosek jest podzielony na rodzaje:
    a. Wniosek o certyfikację - dotyczy wniosków o wydanie Certyfikatu dla Produktu/ów
    b. Wniosek o zmianę - dotyczy wniosków o zmianę już wydanego przez Instytut Certyfikatu
    c. Wniosek o Certyfikat w języku obcym/o wydanie duplikatu/o wydanie kopii – dotyczy wniosków o wydanie Certyfikatu w języku obcym, kopii lub duplikatu Certyfikatu dla ważnego/aktywnego Certyfikatu dla produktu/ów
2. Wniosek o certyfikację jest rodzajem Wniosku oraz jest powiązany z:
    a. Certyfikat - Wniosek o certyfikację zawsze dotyczy jednego Certyfikatu
    b. Produkt - Wniosek o certyfikację dotyczy jednego lub wielu Produktów
3. Wniosek o zmianę jest rodzajem Wniosku oraz jest powiązany z:
    a. Certyfikat - Wniosek o zmianę zawsze dotyczy jednego Certyfikatu
4. Produkt - Wniosek o zmianę może dotyczyć bezpośrednio jednego lub więcej Produktów.
5. Wniosek o Certyfikat w języku obcym/wydanie kopii Certyfikatu/wydanie duplikatu Certyfikatu jest rodzajem Wniosku oraz jest powiązany z:
    a. Certyfikat - Wniosek o Certyfikat w języku obcym/wydanie kopii Certyfikatu/wydanie duplikatu Certyfikatu zawsze dotyczy jednego Certyfikatu. Nigdy nie powoduje zmiany Certyfikatu.
    b. Produkt - Wniosek o Certyfikat w języku obcym/wydanie kopii Certyfikatu/wydanie duplikatu Certyfikatu nigdy nie dotyczy bezpośrednio Produktu.
6. Certyfikat jest powiązany z:
    a. Wniosek o certyfikację - Certyfikat jest powiązany zawsze z jednym wnioskiem o certyfikację
    b. Wniosek o zmianę - Certyfikat może być powiązany z od zera do wielu Wnioskami o zmianę
    c. Wniosek o Certyfikat w języku obcym/wydanie kopii Certyfikatu/wydanie duplikatu Certyfikatu - Certyfikat może być powiązany z od zera do wielu Wnioskami o Certyfikat w języku obcym/wydanie kopii Certyfikatu/wydanie duplikatu Certyfikatu
    c. Produkt - Certyfikat może być powiązany z od jednego do wielu Produktów
7. Produkt jest powiązany z:
    a. Wniosek o certyfikację - Produkt może być powiązany z od zera do wielu Wniosków o certyfikację
    b. Wniosek o zmianę - Produkt może być powiązany z od zera do wielu Wniosków o zmianę
    c. Wniosek o Certyfikat w języku obcym/wydanie kopii Certyfikatu/wydanie duplikatu Certyfikatu – Produkt może być powiązany z od zera do wielu Wniosków o Certyfikat w języku obcym/wydanie kopii Certyfikatu/wydanie duplikatu Certyfikatu
    d. Certyfikat - Produkt może być powiązany z od zera do wielu Certyfikatów

Wymagania dla Panelu Klienta

Id wymagania	Treść wymagania
Ogólne wymagania dla Panelu Klienta	
PK.1	Panel klienta musi być dostępny z oficjalnej strony NIZP PZH – PIB w formie zachęty dla Klientów do przeprowadzenia atestacji: 1. ze strony głównej https://www.pzh.gov.pl/ 2. ze strony dot. atestacji https://www.pzh.gov.pl/uslugi/atestacja-atestation/ i/lub innej wskazanej przez Instytut Linki powinny przekierowywać na ekran startowy, ekran logowania, ekran rejestracji, dla zalogowanych bezpośrednio do ich Panelu Klienta. Wykonawca powinien zaproponować najlepszy wg jego wiedzy sposób przekierowania do Panelu Klienta. Sposób musi zostać zatwierdzony przez Zamawiającego. Zamawiający przekaże Wykonawcy dostępy do oficjalnej strony, które umożliwią wdrożenie przekierowania do Panelu Klienta.
PK.2	W Panelu musi być dostępna „Deklaracja dostępności" zgodnie z WCAG 2.1 (lub nowszym) i Ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych z późniejszymi zmianami.
PK.3	Panel musi wspierać mechanizm powiadomień: 1. w Panelu 2. email (poprzez integrację z enova365). W tym w szczególności powiadomienia o zmianach statusów Wniosków, Certyfikatów, Produktów. Komunikacja powiadamiania i przekazywania email ma być zgodna ze standardem SMTP.
Zakładanie Konta Klienta – Proces PeA.1	
PK.4	Rejestracja Klienta za pomocą NIP, Firmowy Adres Email oraz hasła.
PK.5	Podczas rejestracji firmy po wpisaniu NIP dane firmy są zaczytywane z REGON a dla firm zagranicznych z EU VIES. Następuje również weryfikacja adresu email (domeny) firmy.
PK.6	Możliwość dodania Pracowników Klienta, Administratora Konta Klienta, podczas rejestracji Konta Klienta.
PK.7	Podczas rejestracji Konta Klienta wymagane jest podanie przynajmniej jednego konta Administratora Konta Klienta.
PK.8	Założenie konta powinno zostać ostatecznie potwierdzone przez weryfikację emaila
PK.9	Możliwość zdefiniowania uprawnień dla ról – Pracownik, Administrator
PK.10	Klient powinien mieć możliwość zdecydowania czy chce otrzymywać powiadomienia dotyczące atestacji poprzez email. Klient powinien mieć możliwość cofnięcia zgody i ponownego jej wyrażenia.
Zarządzanie Kontem Klienta – Proces PeA.6	
PK.11	Administrator Konta Klienta powinien mieć możliwość zmiany danych Konta Klienta

PK.12	Administrator Konta Klienta powinien mieć możliwość zmiany uprawnień dla Pracowników Klienta w tym dostępu do Produktów i Certyfikatów Klienta
PK.13	Administrator Konta Klienta powinien mieć możliwość usunięcia Konta Klienta (dezaktywacja konta – konto archiwalne).
PK.14	Administrator Konta Klienta powinien mieć możliwość zmiany Administratorów Konta Klienta, Pracowników Klienta poprzez ich dodanie, usunięcie lub modyfikację.
PK.15	Administrator Konta Klienta powinien mieć możliwość zmiany danych dostępowych Pracownika Klienta.
PK.16	Administrator Konta Klienta powinien mieć możliwość zmiany danych osobowych Pracownika Klienta.
Płatności	
PK.17	Obsługa płatności elektronicznych (koszty dot. obsługi płatności po stronie Zamawiającego).
PK.18	Po upłynięciu terminu zapłaty Wniosek powinien zostać anulowany.
PK.19	Integracja z enova365 w zakresie obsługi płatności (dokumenty, powiadomienia, płatności internetowe)
Formularze	
PK.20	System posiada zdefiniowane formularze dla: • wniosków o Certyfikację dla różnych typów grup produktowych (w szczególności różniących się w zakresie koniecznych załączników i listy dodatkowych pytań), • wniosków o wprowadzenie zmiany Certyfikatu • wniosku o wydanie duplikatu Certyfikatu • wniosku o wydanie kopii Certyfikatu • wniosku o wydanie Certyfikatu w j. obcym. Łącznie 12 przygotowywanych na etapie wdrożenia formularzy opisanych w załączniku nr. 5 (do 40 pól na formularzu)
PK.21	Definicja formularzy może obejmować następujące elementy: 1. Pola tekstowe 2. Pola numeryczne 3. Pola dat 4. Listy jednokrotnego wyboru 5. Listy wielokrotnego wyboru 6. Sekcje z możliwością dodania załącznika 7. Pola wymagane/opcjonalne 8. Relacje w polu formularza z Certyfikatem / Wnioskiem / Produktem 9. Tabele dla podania składu chemicznego Produktu 10. Pola pozwalające wpisać formułę (np. do wyliczania cen) Każdy element formularza posiada etykietę i opis będący instrukcją wypełnienia pola.
PK.22	Możliwość oznaczania załączników/pól w Formularzach jako poufne. Poufność powinna skutkować między innymi tym, że: • dane pole/załącznik nie będzie przekazywane do zasilenia systemu W3, tj. nie będzie udostępniany Konsumentom. Szczegóły integracji z systemem W3 w rozdziale Integracje.

	• Dane pole/załącznik będzie widoczne dla uprawnionych Użytkowników Wewnętrznych
Wniosek – Proces PeA.2 i Proces PeA.8	
PK.23	Możliwość realizacji przebiegu procesu zgodnie z modelem PeA.2. oraz modelem PeA.8.
PK.24	Możliwość autouzupełniania danych Klienta we wniosku na podstawie danych Konta Klienta z możliwością edycji.
PK.25	Możliwość wygenerowania nowego Wniosku (z nowym numerem i bieżącą datą) z uzupełnionymi danymi i załącznikami z poprzedniego wniosku powiązanego z Kontem Klienta.
PK.26	Możliwość wygenerowania częściowo uzupełnionych Wniosków dla wybranych Certyfikatów (ponowna certyfikacja, zmiana, itd.). Wygenerowane Wnioski są dostępne na koncie Klienta ze statusem „nowy”.
PK.27	Wniosek powinien podlegać przepływowi pracy zgodnie z modelem PeA.2 oraz PeA.8 zapewniając możliwość prośby o korektę wniosku przez Użytkownika Wewnętrznego na każdym etapie procesu. Złożona przez Klienta korekta zostanie uznana za słuszną po akceptacji Użytkownika Wewnętrznego.
PK.28	Podpowiedzi kontekstowe na etapie wypełniania Wniosku
PK.29	Możliwość zmiany wszystkich udostępnionych do modyfikacji (według zdefiniowanego formularza) danych we Wniosku (w tym załączników). Możliwość modyfikacji pola musi być możliwa do sterowania przez Użytkownika Wewnętrznego w celu udostępnienia do modyfikacji tylko tych pól, które aktualnie wymagają poprawy. Celem jest brak konieczności przeglądania całości wniosku ponownie przez pracownika Instytutu oraz ułatwienie Klientowi wprowadzenia zmian.
PK.30	Wniosek powinien umożliwiać wybranie (np. z listy rozwijalnej z wyszukiwaniem) Produktu Klienta, który ma być zgłoszony do certyfikacji lub utworzenie nowego Produktu z poziomu Wniosku.
PK.31	Złożony Wniosek wraz z podpisanym dokumentem Wniosku jako załącznikiem powinien być przekazany do realizacji w W1.
PK.32	Złożony Wniosek powinien być dostępny dla Klienta do wglądu, modyfikacji i ponownego przekazania do W1.
PK.33	W procesie przetwarzania Wniosku przez Instytut powinna być możliwość przyjęcia komentarza / opinii do Wniosku / dokumentów z systemu enova365/ Panelu Klienta.
PK.34	Proces powinien umożliwiać złożenie Wniosku przez Wnioskodawcę w imieniu własnym lub w imieniu Zleceniodawcy.
PK.35	Wniosek nie może być modyfikowany od momentu, w którym został wydany na jego podstawie Certyfikat.
PK.36	Musi być możliwość pobrania wypełnionego Wniosku celem podpisania go (poza Panelem Klienta) podpisem elektronicznym lub profilem zaufanym i ponowny zapis Wniosku podpisanego do Panelu Klienta (jako załącznik do Wniosku).
PK.37	Możliwość komunikacji z Użytkownikiem Wewnętrznym w zakresie: • Wymiany informacji • Wskazówek do sposobu wypełnienia wniosku

	• Przesyłania Wniosku (dane) z komentarzami • Przesyłania dokumentów (dodatkowe wymagane, potwierdzenie zapłaty)
Wnioski	
PK.38	Możliwość wyszukiwania, sortowania i filtrowania Wniosków co najmniej wg. 1. Wnioskodawca 2. Numer sprawy 3. Osoba rozpatrująca sprawę, 4. Status Wniosku 5. Rodzaj Wniosku 6. Tryb realizacji sprawy 7. Numer faktury 8. Powiązany Certyfikat 9. Powiązane Produkty 10. Producent
PK.39	Widok listy Wniosków z możliwością wyszukiwania, sortowania i filtrowania wg.: 11. Wnioskodawca 12. Numer sprawy 13. Osoba rozpatrująca sprawę, 14. Status Wniosku 15. Rodzaj Wniosku 16. Tryb realizacji sprawy 17. Numer faktury 18. Powiązany Certyfikat
PK.40	Możliwość przejścia z listy Wniosków do widoku szczegółów Wniosku, który będzie przedstawiał bieżące informacje na temat przetwarzanego Wniosku bądź podsumowanie Wniosku, dla którego przetwarzanie zostało zakończone. W widoku powinny znaleźć się dane wprowadzone na Wniosku, informacje od Instytutu, załączniki do pobrania, historia komunikacji, dane nt. płatności.
PK.41	Pracownik Klienta domyślnie powinien mieć dostęp tylko do złożonych przez siebie Wniosków.
PK.42	Wniosek na każdym etapie można pobrać jako plik (.pdf) do druku.
Produkt	
PK.43	Pracownik Klienta powinien mieć widok Produktów zgłoszonych do certyfikacji i pozostałych.
PK.44	Możliwość wyszukiwania, sortowania i filtrowania Produktów wg.: 1. Nazwa Produktu 2. Nazwa Producenta 3. Status Produktu – czy jest w trakcie certyfikacji czy posiada już Certyfikat/nie posiada Certyfikatu 4. Numer kodu kreskowego 5. Numer Certyfikatu 6. Data wydania Certyfikatu 7. Data ważności Certyfikatu 8. Grupa produktowa

	9. Powiązane Certyfikaty z możliwością wyświetlenia dokumentu Certyfikatu 10. Powiązane Wnioski 11. Statystki wyszukiwania produktu
PK.45	Widok listy Produktów z możliwością wyszukiwania, sortowania i filtrowania wg.: 1. Nazwa Produktu 2. Nazwa Producenta 3. Status Produktu – czy jest w trakcie certyfikacji czy posiada już Certyfikat/nie posiada Certyfikatu 4. Numer kodu kreskowego 5. Grupa produktowa
PK.46	Widok szczegółów Produktu zawierający: 1. Nazwa Produktu 2. Grupa produktowa 3. nazwa Producenta (czasem stosowany jest zapis np. "Wyprodukowano w Chinach/UE dla...") 4. Status Produktu – czy jest w trakcie certyfikacji czy posiada już Certyfikat/nie posiada Certyfikatu 5. Numer kodu kreskowego Produktu 6. skład chemiczny Produktu – składa się z numeru CAS, nazwy związku chemicznego, wartości % związku w składzie wyrobu. 7. lista aktualnych i nieaktualnych Certyfikatów Produktu. Domyślnie najpierw aktualne Certyfikaty sortowane po dacie wydania malejąco. Informacje, które mają zostać wyświetlone na Certyfikacie będącym na liście: a. Typ (Atest/Świadectwo) i numer Certyfikatu b. Informacja o aktualności wraz z informacją do kiedy Certyfikat jest aktualny lub nieaktualności c. Data wydania d. Data ważności e. Dokument Certyfikat do podglądu i pobrania (w przypadku zgody na udostępnienie przez Klienta) f. Przejście do szczegółowego widoku Certyfikatu 8. Powiązane z Produktem Wnioski 9. Statystki wyszukiwania produktu
PK.47	Integracja z W3 – wyświetlanie danych statystycznych dotyczących wyszukiwania produktu
PK.48	Na podstawie widoku listy Produktów Klient powinien mieć możliwość uwzględnienia w swojej analizie danych o Produktach (np. czy mam aktywne Certyfikaty na podobne produkty, jak wyglądają statystyki/ilość wyszukiwań w ostatnim miesiącu/roku, czy produkty z Certyfikatem sprzedają się lepiej niż analogiczne bez (w zestawieniu z danymi wewnętrznymi Klienta, itp.) i określenia czy warto zgłosić Produkt do certyfikacji.
PK.49	Możliwość wyświetlenia widoku statystyki wyszukiwania Produktów przez Klientów w kontekście Produktów i grup produktowych.
PK.50	Pracownik Klienta domyślnie powinien mieć widok tylko dodanych przez siebie Produktów.

PK.51	Możliwość dodawania, modyfikacji, usuwania Produktów przez Pracownika Klienta. Modyfikacja/usuwanie tylko wtedy, gdy dany Produkt jest możliwy do edycji tj. jego dane nie będą przetwarzane przez pracowników Instytutu w celu certyfikacji (złożony Wniosek) i/lub nie istnieje powiązany z Produktem Certyfikat.
PK.52	Brak możliwości edycji i usuwania Produktu z powiązanym Certyfikatem.
PK.53	W przypadku złożenia Wniosku o zmianę istnieje możliwość zmiany nazwy Produktu na Certyfikacie (skutkuje to: zmianą Certyfikatu, zmianą Produktu – pole nazwa Produktu) po przeprocesowaniu zmiany przez Instytut. Zmiany Produktu zostają zachowane w historii zmian Produktu.
PK.54	Jeśli dla Produktu nie ma ważnego Certyfikatu: 1. a był już kiedyś wystawiony Certyfikat dla tego Produktu, Produkt można modyfikować, ale pozostaje odnotowana informacja o zmianie i w przypadku korzystania z poprzedniego Wniosku przy tworzeniu Wniosku o nowy Certyfikat, wyświetla się informacja o zmianie 2. i nigdy nie było Certyfikatu lub Klient nie korzysta z poprzedniego Wniosku, to Produkt można modyfikować.
Certyfikat	
PK.55	Możliwość wyszukiwania, sortowania i filtrowania Certyfikatów wg.: 1. Numer Certyfikatu 2. Nazwa certyfikowanego wyrobu/produktu 3. Osoba rozpatrująca sprawę 4. Zleceniodawca 5. Data wydania Certyfikatu 6. Data ważności Certyfikatu 7. Status Certyfikatu 8. typ Certyfikatu (Atest/Świadectwo)Powiązane Produkty 9. Powiązane Wnioski
PK.56	Widok listy Certyfikatów z możliwością wyszukiwania, sortowania i filtrowania wg.: 1. Numer Certyfikatu 2. Nazwa certyfikowanego wyrobu/produktu 3. Data wydania Certyfikatu 4. Data ważności Certyfikatu 5. Status Certyfikatu 6. typ Certyfikatu (Atest/Świadectwo)
PK.57	Widok szczegółów Certyfikatu: 1. Numer Certyfikatu 2. typ Certyfikatu (Atest/Świadectwo) 3. Status Certyfikatu 4. Data wydania Certyfikatu 5. Data ważności Certyfikatu 6. dane podmiotu, dla którego został wydany Certyfikat, 7. Nazwa certyfikowanego Produktu 8. Powiązane Produkty 9. Powiązane Wnioski

PK.58	Pracownik Klienta domyślnie powinien mieć widok tylko Certyfikatów powiązanych z dodanymi przez siebie Produktami i Wnioskami.
PK.59	Pracownik Klienta, z poziomu listy Certyfikatów bądź widoku konkretnego Certyfikatu, powinien mieć możliwość zgłoszenia Certyfikatu bądź wielu Certyfikatów do odnowienia (ponownej certyfikacji powiązanych Produktów) zgodnie z procesem PeA.4 Monitorowanie statusu istniejących Certyfikatów.
PK.60	Pracownik Klienta może wyświetlić lub pobrać dokument Certyfikatu z widoku Produktu, listy Certyfikatów, widoku Certyfikatu.
PK.61	Pracownik Klienta może wyświetlić lub pobrać dokument Certyfikatu z widoku Wniosku.
PK.62	Zachowanie historii zmian Certyfikatu na podstawie Wniosków o zmianę.
PK.63	Administrator Konta Klienta powinien mieć możliwość konfiguracji powiadomień o zbliżającym się terminie końca ważności Certyfikatów.
Pozyskiwanie informacji o certyfikacji – Proces PeA.7	
PK.64	Wbudowany formularz kontaktowy z opcjonalną możliwością wpisania numeru telefonu. Formularz dostępny tylko dla zalogowanych Użytkowników Zewnętrznych. Historia komunikacji dostępna dla Klienta i Użytkownika Wewnętrznego.
PK.65	Klienci mogą otrzymywać od NIZP PZH-PIB dedykowane informacje w formie powiadomień w Panelu Klienta oraz e-mail, informujące o zmianach w procesie atestacji, zmianach w Panelu Klienta, informacje dot. składu chemicznego Produktów i inne związanych z atestacją. Dedykowane wiadomości są przygotowywane przez Użytkowników Wewnętrznych w systemie enova365. Wiadomości są przekazywane do Klientów poprzez integrację.

Wymagania dla Panelu Administratora

Id wymagania	Treść wymagania
Ogólne	
PA.1	System powinien umożliwiać jednoczesną pracę dla minimum 10 Użytkowników Wewnętrznych.
PA.2	Możliwość ograniczenia dostępu do Panelu Administratora dla konkretnych adresów IP.
PA.3	Panel Administratora wyłączony z wyszukiwania w wyszukiwarkach internetowych.
PA.4	Odseparowanie funkcji administracyjnych (moduł zarządzania uprawnieniami, logami i konfiguracją, szablony raportów) od funkcji związanych z pracą merytoryczną.
PA.5	Możliwość konfiguracji Systemu i jego poszczególnych elementów w tym słowników (np. słownik grup produktowych) oraz modyfikacji treści komunikatów/zgód (np. RODO, zgoda na otrzymywanie wiadomości email, itd.).
Monitorowanie komunikatów, logów, usług sieciowych	
PA.6	Komunikaty oraz logi systemowe muszą umożliwić Zamawiającemu przede wszystkim identyfikację i naprawę błędów dotyczących wydajności i bezpieczeństwa Systemu oraz monitorować aktywność w Systemie. Ponadto zgodnie z regulacjami wprowadzanymi przez ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, logi muszą umożliwiać identyfikowanie incydentów bezpieczeństwa oraz klasyfikację tych incydentów na podstawie: • liczby użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług • czas trwania incydentu • zasięg geograficzny obszaru, którego dotyczy incydent • zakres zakłócenia funkcjonowania usługi • zakres wpływu incydentu na działalność gospodarczą i społeczną
PA.7	Logowanie żądań przychodzących i wychodzących z Systemu oraz odpowiedzi do żądań. Mechanizm umożliwiający trwałe zapisywanie wszystkich lub wybranych logów.
PA.8	Obsługa logów, wyszukiwanie wg ustalonego kryterium, prezentacja rezultatów wyszukiwania w przejrzysty sposób.
PA.9	System umożliwia monitorowanie, powiadamianie i raportowanie incydentów zachodzących w Systemie.
PA.10	System posiada mechanizm audytowania zdarzeń, zapewnia logowanie wszystkich informacji z działalności Użytkowników Wewnętrznych i Zewnętrznych ze szczególnym uwzględnieniem dostępu do danych wrażliwych oraz umożliwia przygotowanie raportów w celu przeprowadzania audytów dotyczących danych wrażliwych.
Zarządzanie kontami	
PA.11	Integracja z KeyCloak w celu zarządzania dostępami dla Użytkowników Zewnętrznych i Użytkowników Wewnętrznych.

PA.12	Mechanizm nadawania dostępów i uprawnień do Panelu Administracyjnego.
PA.13	Zakładanie konta dla Użytkownika Zewnętrznego przez Administratora IT po stronie Instytutu (oprócz zakładania z poziomu KeyCloak)
PA.14	System będzie posiadał mechanizmy tworzenia i wymuszania polityki tworzenia haseł dostępowych umożliwiające tworzenie takich polityk oddzielnie dla różnych grup użytkowników, w szczególności dla Administratorów (wymuszona złożoność, cykliczność zmiany)
PA.15	Definiowanie ról dostępu do Systemu dla Użytkowników Wewnętrznych na poziomie: • Administrator IT - rola umożliwia dostęp do wszystkich funkcjonalności Systemu związanych z administrowaniem Systemem i zarządzaniem uprawnieniami Użytkowników oraz do związanych z tym słowników i parametrów (np. modyfikacja opisu roli, okresowe raporty kont i przyznanych im ról, dostęp do logów, zarządzanie parametrami, weryfikacja nieautoryzowanych dostępów), • Analityk - rola dająca dostęp do wszystkich funkcjonalności związanych z merytoryczną obsługą certyfikacji, w tym zarządzeniem uprawnieniami Użytkowników Zewnętrznych. • Obserwator – rola umożliwiająca wyłącznie podgląd danych i statystyk bez jakichkolwiek zmian • Redaktor – dodawanie, edycja komponentów i treści
PA.16	Powinna być możliwość przypisania jednemu Użytkownikowi Wewnętrznemu dowolnej ilości ról.
Dane Produktów	
PA.17	Widok szczegółów Produktów oraz listy Produktów analogiczny jak w Panelu Klienta określony w wymaganiach **PK.45** i **PK.46**
PA.18	Możliwość wyszukiwania Produktów - analogicznie jak w Panelu Klienta, wymaganie **PK.44**
PA.19	Możliwość dodawania, modyfikacji, usuwania Produktów. Ostrzeżenie w przypadku, jeśli zmiana może naruszyć strukturę danych bądź zakłócić procesy w Systemie.
Dane Certyfikatów	
PA.20	Widok szczegółów Certyfikatów oraz listy Certyfikatów analogiczny jak w Panelu Klienta określony w wymaganiach **PK.56** i **PK.57**.
PA.21	Możliwość wyszukiwania Certyfikatów - analogicznie jak w Panelu Klienta, wymaganie **PK.55**.
PA.22	Możliwość dodawania, modyfikacji, usuwania Certyfikatów. Ostrzeżenie w przypadku, jeśli zmiana może naruszyć strukturę danych bądź zakłócić procesy w Systemie.
PA.23	Możliwość przypisania istniejących Certyfikatów do Konta Klienta.
Dane Wniosków	
PA.24	Możliwość wyszukiwania Wniosków - analogicznie jak w Panelu Klienta, wymaganie **PK.38**.
PA.25	Widok szczegółów Wniosków oraz listy Wniosków analogiczny jak w Panelu Klienta określony w wymaganiach **PK.39** i **PK.40.**

PA.26	Możliwość dodawania, modyfikacji, usuwania Wniosków. Bez możliwości usuwania/edycji Wniosków, dla których został wydany/zmodyfikowany Certyfikat, wydany duplikat/kopia/Certyfikat w języku obcym. Ostrzeżenie w przypadku, jeśli zmiana może naruszyć strukturę danych bądź zakłócić procesy w Systemie.
PA.27	Wersjonowanie Wniosków. Możliwość przeglądania historii zmian.
Zarządzanie danymi	
PA.28	Obsługa replikacji danych do narzędzi BI, które posiada Zamawiający, wraz z przygotowaniem 3 przykładowych widoków. Zakres widoków zostanie określony w ramach prac analitycznych.
PA.29	Zapewnienie spójności danych pomiędzy W1, W2 i W3.
PA.30	Dostępne mechanizmy kontroli spójności danych dla Użytkowników Wewnętrznych.
PA.31	Możliwość wyeksportowanie danych zbieranych w Systemie do formatu .xlsx, .csv, .pdf
Logi audytu	
PA.32	System musi posiadać rejestry audytowe, umożliwiać ich przeglądanie, sortowanie, filtrowanie, wyszukiwanie danych po dowolnych polach.
PA.33	System musi zawierać mechanizm do przeglądania logów bieżących (wstępnie wszystkie do 6 miesięcy; okres ustawiany parametrem) i archiwalnych (wstępnie wszystkie powyżej 6 miesięcy; okres ustawiany parametrem) w tym zapewniający możliwość: 1. wyszukiwania 2. filtrowania po wybranych przez Użytkownika typach zdarzeń i ich cechach. 3. sortowania po wybranych przez Użytkownika typach zdarzeń i ich cechach. oraz musi zapewnić mechanizm eksportu pliku logów do serwera zewnętrznego przy użyciu standardowych protokołów i mieć możliwość synchronizacji z serwerem czasu (protokół NTP).
PA.34	W zakresie przeglądania logów musi być możliwość dostępu co najmniej do następujących danych: 1. Historii zmian uprawnień Użytkowników (z dokładnością do roli): login, nazwisko, imię, komórka organizacyjna, rola, data nadania roli, data odebrania roli. 2. Historia Lista sesji Użytkowników: zawierać będzie listę wszystkich sesji Użytkowników, wraz z informacjami: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina początku sesji, data i godzina zakończenia sesji (jeżeli sesja już została zakończona), adresie IP komputera, na którym powstała sesja. 3. Listy otwartych sesji: Login, nazwisko, imię, jednostka, komórka organizacyjna, data /godzina początku sesji (musi być możliwość wylogowania wszystkich Użytkowników). 4. Historii logowań: login, nazwisko, imię, komórka organizacyjna, data i godzina zalogowania, data i godzina wylogowania, czas logowania. 5. Kont Użytkowników Systemu: login, nazwisko, imię, komórka organizacyjna, data założenia konta, data

	dezaktywacji konta, czy aktywne, data ostatniego logowania. 6. Historii zmian dotyczących kont Użytkowników: zawiera wszystkie atrybuty konta Użytkownika (login, nazwisko, imię, komórka organizacyjna, data założenia konta, data zablokowania konta, czy aktywne) oraz powiązań konta Użytkownika z innymi obiektami (np. uprawnienia, sesje), wraz z datą i godziną zmiany oraz informacją o tym kto zmianę wykonał. 7. Listy aktywnych Użytkowników wraz z przypisanymi rolami (imię. nazwisko, login, komórka organizacyjna, rola). 8. Listy osób, które w zadanym okresie miały nadane uprawnienia, przy czym powinna być możliwość wyszukiwania po parametrach: • okres (od, do) wraz z możliwością wyszukania listy osób, które miały nadane uprawnienia przez cały okres jak i w jego fragmencie, • rola (możliwe zaznaczenie kilku), • Lista osób powinna zawierać następujące informacje: login, nazwisko, imię, data nadania uprawnienia, data odebrania uprawnienia. 9. Zakres powyższych logów powinien zostać ostatecznie przedstawiony i uzgodniony z Zamawiającym.
PA.35	Wszystkie wskazane powyżej widoki muszą posiadać: 1. nagłówek zawierający tytuł raportu. 2. zadane parametry wyszukiwania dla których został wygenerowany raport. 3. część zasadniczą z wygenerowanymi danymi wraz z nagłówkami kolumn. 4. możliwość wyszukiwania. 5. możliwość filtrowania po wybranych przez Użytkownika wartościach. 6. możliwość sortowania po wybranych przez Użytkownika wartościach.
PA.36	W Systemie muszą być logowane zdarzenia z dokładnością do każdego parametru określonego w **PA.34**. Komunikaty zdarzeń muszą być opisane w sposób czytelny dla Użytkownika.
PA.37	W Systemie muszą być rejestrowane działania Użytkowników oraz zdarzenia związane z bezpieczeństwem informacji. Dane te muszą być przechowywane przez określony przez Zamawiającego czas dla potrzeb przyszłych postępowań wyjaśniających oraz monitorowania kontroli dostępu. Logi bieżące mają być przechowywane w Systemie, natomiast kwestie związane z przechowywaniem logów archiwalnych zostaną omówione na etapie Projektu Technicznego.
PA.38	W przypadku, gdy w Aplikacji jest realizowany interfejs integracyjny obligatoryjne jest odnotowywanie działań związanych z uruchamianiem funkcji interfejsu integracyjnego wraz z możliwością włączenia powiadamiania mailowego o błędach.

PA.39	System musi umożliwiać eksport wyników wyszukiwania do plików formatu np. xlsx, csv w zależności od zapotrzebowania Użytkownika.
PA.40	W Systemie konieczne jest przygotowywanie raportu dostępu do danych osobowych zgodnie z obowiązującymi regulacjami prawnymi.
PA.41	Raport dostępu do danych osobowych musi zawierać: 1. Informację o okolicznościach kiedy konkretny zestaw danych osobowych został wprowadzony do Systemu. Musi być rejestrowana co najmniej 'Data i godzina wprowadzenia danych', 'Operator który dane wprowadził' (wystarczy login, np. testowy), 'Źródło danych' (wystarczy skrót identyfikujący inny system, np. enova365 moduł CRM, w przypadku wprowadzenia danych przez operatora może być pustym polem), 'zakres wprowadzonych danych' (np. 'imię: Jan, nazwisko: Testowy, adres zameldowania: ul. Testowa 1, pesel: 1234567890'). 2. Informację o udostępnieniu danych osobowych – 'zakres udostępnionych danych' (np. 'imię, nazwisko, adres zameldowania, pesel'), 'operator który wykonał udostępnienie' (wystarczy login, np. testowy), 'data i godzina udostępnienia danych', 'podmiot dla którego udostępnia' (powinien móc uzupełnić pole z informacją komu udostępnia dane). 3. Informację o źródle pozyskania danych osobowych w przypadku, gdy dane pozyskano z innego źródła niż osoba, której dane dotyczą, 4. Informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały, przekazane, wraz z określeniem daty i zakresu udostępnianych danych 5. zapis eksportu do edytowalnego pliku treści danych osobowych, 6. zapis daty i godziny zmiany danych w aplikacji i określenia operatora, który zmiany wprowadził, 7. zapis usunięcia danych z aplikacji, 8. zapis oznaczenia wraz z odnotowaniem daty danych, których przetwarzanie zostało ograniczone, 9. zapis oznaczenia wraz z odnotowaniem daty danych, wobec przetwarzania których wniesiono sprzeciw, 10. zapis wygenerowania i wydrukowania raportu zawierającego informacje dot. przetwarzania danych osobowych.
Formularze	
PA.42	Przygotowane formularze Wniosków powinny być możliwe do edycji i zapisu jako modyfikacja lub nowy formularz przez Użytkowników Wewnętrznych w zakresie: • Edycja wyświetlanej etykiety pola • Edycja opisu będącego instrukcją wypełnienia pola • Dodanie / usunięcie sekcji z możliwością dodania załącznika
PA.43	Zarządzanie formularzami - nadawanie uprawnień, edycja, usuwanie, przypisywanie czasu ważności formularza, itd.
PA.44	Formularze archiwalne – dostępne w Systemie, można na ich bazie budować nowe formularze, można je przeglądać, dostępna jest historia zmian formularza

Słowniki (listy jednokrotnego lub wielokrotnego wyboru)	
PA.45	Możliwość definiowania nowych słowników (dla nowych Formularzy)
PA.46	Zarządzanie słownikami – nadawanie uprawnień, edycja, usuwanie, przypisywanie czasu ważności słownika, itd.
PA.47	Słowniki archiwalne – dostępne w Systemie, można na ich bazie budować nowe słowniki, można je przeglądać, dostępna jest historia zmian słowników

Wymagania dla warstwy W1 (rozbudowa)

Id wymagania	Treść wymagania
Ogólne	
W1R.1	System powinien umożliwiać jednoczesną pracę dla minimum 80 Użytkowników Wewnętrznych.
W1R.2	System musi umożliwiać przygotowanie i przekazanie dedykowanych wiadomości do Klientów opisanych w wymaganiu **PK.65**. Wysyłanie wiadomości realizowane z wykorzystaniem obecnego modułu enova365 dot. korespondencji seryjnej. Możliwość filtrowania Klientów, do których będą wysyłane dedykowane wiadomości ze względu na: 1. Dla wszystkich Klientów 2. Nazwa Klienta 3. Grupa produktowa certyfikowanych produktów 4. Ilość Certyfikatów – czy Klient posiada X Certyfikatów? 5. Certyfikaty wystawione przez dany Zakład merytoryczny 6. Skład chemiczny Produktów – Czy Klient posiada Produkty z związkiem chemicznym X, dla których posiada Certyfikat? 7. Status Wniosków – Czy Klient posiada Wnioski w trakcie realizacji/przygotowane do złożenia?
W1R.3	Przygotowanie szablonu dedykowanej wiadomości e-mail do Klientów zgodnie z Systemem Identyfikacji Wizualnej NIZP PZH-PIB/wytycznymi Instytutu.
W1R.4	Użytkownik Wewnętrzny ma dostęp do Panelu Administratora bezpośrednio z W1.
Obsługa wniosku	
W1R.5	Możliwość zapisania złożonego Wniosku w W1 wraz z załącznikami (w tym podpisany Wniosek). Złożony Wniosek po opłaceniu jest podstawą założenia sprawy (integracja z EZD PUW)
W1R.6	Możliwość komunikacji z Klientem w zakresie: • Wymiany informacji • Wskazówek do sposobu wypełnienia wniosku • Przesyłania Wniosku (dane) z komentarzami • Przesyłania dokumentów (polecenia zapłaty)
W1R.7	Możliwość wskazania, które pola wniosku wymagają poprawy przez Użytkownika Wewnętrznego w celu udostępnienia do modyfikacji tylko tych pól, które aktualnie wymagają poprawy. Celem jest brak konieczności przeglądania całości wniosku ponownie przez pracownika Instytutu oraz ułatwienie Klientowi wprowadzenie zmian.
W1R.8	Obsługa 3 trybów realizacji sprawy (zwykły, ekspresowy, pilny). Tryby różnią się czasem realizacji przez Użytkownika Wewnętrznego, co ma wpływ na kolejność i czas trwania działań w procesie P.3.18 i pośrednio w PeA.2 i PeA.8 (tryb pilny).
W1R.9	Obsługa załączników/pól oznaczonych jako poufne.
W1R.10	Widok listy Wniosków z możliwością wyszukiwania, sortowania i filtrowania wg.: 1. Wnioskodawca

	2. Numer sprawy 3. Osoba rozpatrująca sprawę, 4. Status Wniosku 5. Rodzaj Wniosku 6. Tryb realizacji sprawy 7. Numer faktury 8. Powiązany Certyfikat
W1R.11	Możliwość przechowywania danych dotyczących składanych przez Klientów Wniosków: 1. Zleceniodawca 2. Wnioskodawca 3. Numer sprawy (z EZD PUW) 4. Osoba rozpatrująca sprawę 5. Status Wniosku 6. Tryb realizacji sprawy 7. Powiązany Produkt / Powiązane Produkty 8. Numer faktury 9. Powiązany Certyfikat 10. Inne dane wypełniane na formularzu dla Wniosku 11. Powiązane załączniki / dokumenty
W1R.12	Użytkownik Wewnętrzny może wyświetlić lub pobrać dokument Wniosku z widoku Wniosków oraz listy Wniosków.
W1R.13	Zachowanie historii zmian Wniosku.
W1R.14	Użytkownik Wewnętrzny ma możliwość wprowadzania zmian we Wniosku, komentowania pól Wniosku.
W1R.15	Wniosek podlega zatwierdzeniu przez Użytkownika Wewnętrznego. Podczas zatwierdzania we Wniosku dostępne są dodatkowe pola – co najmniej: • data wystawienia Certyfikatu • data ważności Certyfikatu • uwagi • check box: - czy treść pola uwagi ma być umieszczona na Certyfikacie tak/nie • numer Certyfikatu – pole generowane automatycznie według zadanych reguł, możliwość modyfikacji wygenerowanego numeru Rodzaj i ilość dodatkowych pól zostanie określona na etapie analizy wymagania podczas odpowiedniego Wydania.
W1R.16	Możliwość definiowania reguł numeracji Certyfikatów dla każdego Zakładu i typu Certyfikatu przez Użytkownika Wewnętrznego.
Atestacja	
W1R.17	Możliwość ręcznego i automatycznego (na podstawie określonych zdarzeń ustawia System) ustawiania statusów realizacji sprawy. Statusy i powiązane z nimi działania zostaną określone na etapie analizy wymagania podczas odpowiedniego Wydania
W1R.18	Zachowanie historii Certyfikatu (zmiany, wersje obcojęzyczne, kopie, duplikaty)

W1R.19	Widok listy Certyfikatów z możliwością wyszukiwania, sortowania i filtrowania wg.: 1. Numer Certyfikatu 2. Nazwa certyfikowanego wyrobu/produktu 3. Osoba rozpatrująca sprawę 4. Zleceniodawca 5. Data wydania Certyfikatu 6. Data ważności Certyfikatu 7. Status Certyfikatu 8. typ Certyfikatu (Atest/Świadectwo) 9. Powiązane Produkty 10. Powiązane Wnioski 11. Skład chemiczny Produktu (numer CAS, nazwy związku chemicznego, wartości % związku w składzie wyrobu) Wykonawca zaproponuje, które z powyższych pól powinny znaleźć się na liście, a po których będzie możliwe wyszukiwanie, aby zapewnić ergonomię użytkowania narzędzia.
W1R.20	Użytkownik Wewnętrzny może wyświetlić lub pobrać dokument Certyfikatu z widoku Certyfikatów lub listy Certyfikatów.
W1R.21	Automatyczne przesyłanie danych wystawionych Certyfikatów do W2 (integracja, przepływ danych, powiązane z Wnioskiem) dla określonego (na etapie analizy wymagania podczas odpowiedniego Wydania) statusu realizacji sprawy/statusu Certyfikatu.
W1R.22	Automatyczne przesyłanie informacji do W2 (powiązane z Wnioskiem), że Certyfikat nie zostanie wydany dla określonego statusu realizacji sprawy/statusu Certyfikatu.
W1R.23	Generowanie dokumentów (Certyfikat) – możliwość generowania dokumentu w formacie MS Word zgodnie ze zdefiniowanymi szablonami. Certyfikat generowany jest na żądanie Użytkownika Wewnętrznego. Pola szablonu wypełniane są automatycznie przez System zgodnie z danymi wskazanymi w zatwierdzonym Wniosku
W1R.24	Dla Użytkownika Wewnętrznego dostępna jest lista/widok zatwierdzonych Wniosków bez wygenerowanych Certyfikatów. Certyfikaty mogą być generowane pojedynczo lub zbiorczo (wszystkie dla zatwierdzonych Wniosków lub wybrane). Wniosek, dla którego został wygenerowany Certyfikat nie jest widoczny na liście.
W1R.25	Możliwość wygenerowania Certyfikatu w pdf.
W1R.26	Wygenerowane Certyfikaty są dostępne w systemie w postaci plików.
W1R.27	Musi być możliwość pobrania Certyfikatu celem podpisania go (poza Portalem) ręcznego, podpisem elektronicznym lub profilem zaufanym i ponowny zapis Certyfikatu podpisanego, z hologramem.
Szablony dla Certyfikatów	
W1R.28	Obsługa definicji szablonów dokumentów Certyfikatów. System posiada zdefiniowane szablony dla Zakładów: • Atestu Higienicznego • Świadectwa Jakości Zdrowotnej • Duplikatu Certyfikatu • Kopii Certyfikatu

	• Certyfikatu w języku obcym. Łącznie 12 przygotowywanych na etapie wdrożenia szablonów opisanych w załączniku nr. 6
W1R.29	Możliwość definiowania nowych szablonów dla Certyfikatów przez Użytkowników Wewnętrznych
W1R.30	Zarządzanie szablonami - nadawanie uprawnień, edycja, usuwanie, przypisywanie czasu ważności formularza, itd.
W1R.31	Szablony archiwalne – dostępne w Systemie, można na ich bazie budować nowe szablony, można je przeglądać, dostępna jest historia zmian szablonu
Słowniki (listy jednokrotnego lub wielokrotnego wyboru)	
W1R.32	Zarządzanie słownikami – nadawanie uprawnień, edycja, usuwanie, przypisywanie czasu ważności słownika, itd.
W1R.33	Słowniki archiwalne – dostępne w Systemie, można na ich bazie budować nowe słowniki, można je przeglądać, dostępna jest historia zmian słowników
Uprawnienia	
W1R.34	Możliwość definiowania ról dla Użytkowników Wewnętrznych – co najmniej Kierownik, Pracownik merytoryczny, Asystent dla każdego z Zakładów merytorycznych – zróżnicowany dostęp do Wniosków i uprawnienia w zależności od roli i Zakładu powiązanego z Użytkownikiem Wewnętrznym. Role i uprawnienia zostaną zdefiniowane na etapie analizy wymagania podczas odpowiedniego Wydania.
W1R.35	Możliwość nadania jednemu Użytkownikowi Wewnętrznemu kilku ról.

7. Integracje

Integracja systemów poprzez wymianę usług powinna być realizowana w oparciu o usługi sieciowe (Web Serwis) udostępniane na wewnętrznej i zewnętrznej szynie danych (WSO2) w oparciu o udokumentowane interfejsy programistyczne REST API lub SOAP API.
W poniższej tabeli zamieszczono listę standardowych usług charakterystycznych dla poszczególnych systemów integrowanych w ramach Backoffice.

Metadane, będące parametrami wywołania lub rezultatem wywołania poszczególnych usług powinny być zapisywane w powszechnie stosowanym standardzie przeznaczonym do otwartych typów danych (np. XML lub JSON).

Id	Usługa	Charakterystyka i rezultat
U.BO.1	getBusinessObject(ObjectId): Data	Usługa pozwalająca na pobranie danych obiektu biznesowego o zadanym identyfikatorze. Parametrem wywołania jest identyfikator obiektu, opcjonalnie wersja obiektu. Rezultatem są metadane zawierające opis obiektu w tym, jeśli obiekt biznesowy reprezentuje fizyczny plik, dynamicznie generowany adres URL pozwalający na pobranie pliku w ramach aktywnej sesji.
U.BO.2	putBusinessObject(Data): ObjectID	Usługa pozwalająca na aktualizację obiektu biznesowego. Parametrami wywołania są metadane obiektu, rezultatem – identyfikator obiektu w systemie docelowym lub kod błędu.
U.BO.3	deleteBusinessObject(ID):result	Usługa pozwalająca na usunięcie obiektu biznesowego z systemu.
U.BO.4	getObjectList(ObjectId, Type): Data	Usługa pozwalająca na pobranie listy obiektów biznesowych powiązanych z obiektem o zadanym identyfikatorze relacją zadanego typu.

Interfejsy programistyczne (API) poszczególnych systemów powinny umożliwiać implementację wymienionych wyżej usług lub ich kombinacji w postaci usług sieciowych (WS).

Przepływ danych

Przepływ danych pomiędzy integrowanymi komponentami musi odbywać się poprzez standardowe sterowniki ODBC/JDBC/ADO.NET. Integracja odbywa się sposób:

1. Synchroniczny – w czasie rzeczywistym
2. Asynchroniczny – w określonych parametrami konfiguracyjnymi odstępach czasu

Integracje z systemami wdrażanymi u Zamawiającego

W przypadku gdy któryś z planowanych do wdrożenia systemów u Zamawiającego nie będzie na etapie umożliwiającym wdrożenie integracji z Systemem, Wykonawca powinien stworzyć interfejsy symulujące integrację.

Punkty integracji pomiędzy Panelem Klienta (W2) a systemami wewnętrznymi Zamawiającego zostały oznaczone przepływami na diagramach procesów (diagramy procesów stanowią załączniki do OPZ) pomiędzy basenem „Panel Klienta (W2)" a basenem „Systemy NIZP PZH-PIB". W poniższych rozdziałach zostały opisane pozostałe ważne elementy integracji.

Replikacja danych w Platformie RDBMS

Dane zgromadzone w Systemie dotyczące w szczególności:

1. Produktów
2. Certyfikatów
3. Wniosków
4. Statystyk
5. Kont użytkowników
6. Dane audytowe

powinny być możliwe do replikacji z wykorzystaniem Platformy RDBMS oraz podłączenia do systemu wirtualizacji danych.

Integracja z systemem W1 (enova365 i EZD PUW)

Punkty integracji pomiędzy Systemem W2 a enova365 to m.in:

1. Przekazanie informacji o danych Klienta do systemu enova365 podczas rejestracji w W2.
2. Korzystanie z mechanizmu wysyłania wiadomości email z systemu enova365.
3. Obsługa wiadomości z formularza kontaktowego Systemu.
4. Obsługa Wniosku
5. Obsługa płatności
6. Obsługa faktur
7. Obsługa Certyfikatów

Całość komunikacji Użytkownika Wewnętrznego z Klientem będzie się odbywała za pośrednictwem enowa365.

Integracja W1 z EZD PUW (realizowana w ramach obecnego projektu BackOffice) - z poziomu enova365:
- zostanie utworzona sprawa w EZD PUW
- sprawa zostanie zadekretowana na odpowiednie osoby w EZD PUW
- będą nadawane statusy sprawie w EZD PUW
- zostaną przekazane do EZD PUW wszystkie niezbędne (zgodnie z Instrukcją Kancelaryjną i innymi obowiązującymi w tym zakresie w NIZP PZH-PIB regulacjami) dokumenty
- zostanie zamknięta sprawa w EZD PUW.

Integracja powinna zapewnić mapowanie statusów pomiędzy W1, EZD PUW, właściwe moduły enova365, W2 Mapowanie statusów zostanie zaproponowane przez Wykonawcę.

Integracja z systemem DMS (w ramach projektu obecnie realizowanego wdrożenia BackOffice)

Przepływy danych dotyczące wysyłania dokumentów z Systemu do DMS powinny uwzględniać możliwość oznaczenia części przesyłanych dokumentów jako poufne. Na tej podstawie system DMS umieści dokumenty w odpowiednich repozytoriach.

Integracja powinna uwzględniać możliwość dodania w Systemie hiperłącza, które umożliwia pobranie pliku z DMS. Możliwymi do pobrania plikami są:

1. Certyfikaty produktu
2. Załączniki do wniosków
3. Wnioski

Integracja z systemem uwierzytelniania i autoryzacji KeyCloak

Integracja z systemem KeyCloak polega na możliwości wydelegowania zarządzania dostępem do Systemu dla Użytkowników Wewnętrznych oraz Zewnętrznych do systemu KeyCloak. Zarządzanie dostępem do Systemu będzie możliwe z poziomu Systemu i aplikacji zewnętrznej.

Przepływy danych związane z integracją Panelu Klienta (W2) z systemem KeyCloak zostały wyszczególnione na diagramach procesów, które są załącznikiem nr 1.

Integracja z systemem W3

W2 ma za zadanie zasilanie bazy danych W3, wykorzystując przygotowane w ramach projektu W3 interfejsy programistyczne do obsługi Produktów i wydanych dla nich Certyfikatów.

Interfejsy umożliwią dodawanie, edycję i wyświetlanie jednego lub więcej obiektów biznesowych.

Integracja powinna polegać na określeniu momentów w trakcie działania W2, kiedy baza W3 powinna zostać zasilona, a następnie wdrożenie integracji. Powinna również uwzględniać poufność danych oznaczonych jako poufne przez Klientów we Wnioskach.

Dodatkowo w ramach W3 do odpowiednich Produktów i Certyfikatów będą zbierane statystyki ich wyświetlania. Dane te możliwe będą do wyświetlenia i zaimplementowania w strukturę danych W2 w celu wyświetlenia tych statystyk Klientom.

8. Migracja danych do Systemu

Wdrożenie Systemu obejmowało będzie przeprowadzenie migracji danych z różnych (osobne nieidentyczne bazy w różnych Zakładach Instytutu) baz Access, plików MS Word/MS Excel do Systemu.
Plan migracji stanowił będzie element Projektu Technicznego wdrożenia.

Szacowana liczba to ok. 30 000 rekordów.

Odpowiedzialność za wykonanie migracji danych leży po stronie Wykonawcy. Zamawiający umożliwi Wykonawcy dostęp do baz danych MS Access oraz plików MS Word/MS Excel.

Po wykonaniu importu danych na środowisko testowe Wykonawca przedstawi zaimportowane dane Zamawiającemu do akceptacji.

Zamawiający dokona przeglądu danych, naniesie konieczne korekty i dokona akceptacji danych.

Wykonawca zaimportuje zatwierdzone przez Zamawiającego dane do wdrażanego systemu na środowisku produkcyjnym.

Przeniesione mają zostać maksymalnie następujące dane:

- Wnioskodawca
- Producent
- Zleceniodawca (np. Dystrybutor) czyli podmiot, dla którego wydawany jest atest (w sytuacjach gdy w proces certyfikacji zaangażowany jest podmiot inny niż zwyczajowy Wnioskodawca i Producent)
- Adres e-mail Wnioskodawcy
- Numer Certyfikatu
- Nazwa certyfikowanego wyrobu
- Skład wyrobu /skład chemiczny wyrobu/produktu
- Zakres zastosowania
- Data wydania Certyfikatu
- Data ważności Certyfikatu
- Osoba rozpatrująca sprawę
- Numer NIP Wnioskodawcy,
- Numer kodu kreskowego lub kodów kreskowych wyrobu/wyrobów/produktów,
- Etykieta (w przypadku gdy możliwe)
- Tryb realizacji sprawy
- Numer faktury
- Powiązane zmiany Certyfikatu,
- Powiązane Certyfikaty w języku obcym
- Uwagi

Migracja powinna zostać przeprowadzona do odpowiednich struktur Systemu z uwzględnieniem charakterystyki obiektów danych i relacji pomiędzy obiektami danych.

9. Projekt Techniczny

Projekt techniczny zawierający w szczególności uzgodnione z Zamawiającym:

1. Zdalne dostępy do systemów i baz danych Zamawiającego w tym środowiska testowego oraz produkcyjnego
2. Wymagana minimalna architektura techniczna infrastruktury IT potrzebnej do wdrożenia systemu (w tym; konfiguracja logiczna sieci, konfiguracja urządzań odpowiedzialnych za bezpieczeństwo, systemy operacyjne, oprogramowanie narzędziowe, itd.)
3. Harmonogram wdrożenia Systemu
4. Szczegółowy harmonogram wdrożenia dla Wydania I Systemu (dla kolejnych Wydań harmonogramy będą przekazywane przez Wykonawcę na 2 tygodnie przed końcem Wydania poprzedzającego)
5. Narzędzia informatyczne oraz sposób komunikacji z Wykonawcą
6. Harmonogramu i zakres szkoleń dla Użytkowników Wewnętrznych
7. Zakres szkoleń (e-learning) dla Użytkowników Zewnętrznych
8. Plan testów i zakres scenariuszy testowych
9. Zakres i sposób przeprowadzenia audytu bezpieczeństwa kodu oraz testów swobodnych
10. Sposób realizacji wymagań Zamawiającego
11. Jednoznacznie ustalone zasady konfiguracji Systemu
12. Jednoznacznie określony sposób wymienionych w dokumencie integracji
13. Schemat i opis architektury logicznej i fizycznej zawierający również rozmieszczenie oraz powiązanie jej poszczególnych elementów, na poziomie sprzętowym oraz oprogramowania, z uwzględnieniem wersji produkcyjnej i testowej
14. Wykaz komponentów wchodzących w skład Systemu (w tym bibliotek zewnętrznych oraz oprogramowania firm trzecich) wraz z informacją o wersji
15. Sposób przeprowadzenia audytu pod kątem dostępności Systemu (wymagań WCAG)
16. Podział wymagań funkcjonalnych na Wydania (poszczególne elementy Projektu Funkcjonalnego muszą zawierać odwołania do konkretnych wymagań Zamawiającego wskazanych w OPZ i załącznikach)
17. Projekt Techniczny musi być aktualizowany o wprowadzone na etapie realizacji zmiany do końca czasu trwania wdrożenia tj. końca Etapu 3 Umowy.

Budowa dokumentu:

1. Cel i zakres
2. Wykaz dokumentów referencyjnych
3. Definicje pojęć
4. Opis rozwiązania
5. Sposób realizacji wymagań funkcjonalnych (Wydania, priorytety, ewentualne odstępstwa/zmiany z uzasadnieniem, itp.)
6. Sposób realizacji wymagań niefunkcjonalnych
7. Architektura rozwiązania
    a. Architektura systemu
    b. Metody autentykacji i autoryzacji użytkowników Wewnętrznych i Zewnętrznych
    c. Rozliczalność działań użytkowników
    d. Sposoby zapewnienia bezpieczeństwa i ochrony przed zagrożeniami
    e. Sposoby zapewnienia poufności danych
    f. Sposoby zapewnienia wysokiej dostępności Systemu

g. Disaster recovery (w tym mechanizm realizacji kopii zapasowych)
h. Wydajność
i. Standardy integracyjne i wymiana danych
j. Minimalna wymagana infrastruktura fizyczna (serwery fizyczne i wirtualne, macierze, infrastruktura sieciowa, infrastruktura wirtualna, itd.)
k. Wykaz licencji

10. Projekt Graficzny

1. Projekt Graficzny musi być sporządzony dla komponentów Systemu będących Oprogramowaniem dedykowanym.
14. Projekt graficzny W2 musi być zgodny z Systemem Identyfikacji Wizualnej NIZP PZH-PIB, wymaganiami WCAG w aktualnej wersji
2. Spójność graficzna poszczególnych modułów Aplikacji
   Projekt Graficzny musi być sporządzony dla co najmniej 3 grup urządzeń: dla komputerów, dla tabletów oraz dla smartfonów, uwzględniając wytyczne i założenia responsywnego interfejsu webowego,
3. Projekt Graficzny dla każdej z tych grup urządzeń musi zawierać wszystkie podstrony (strona główna oraz wszystkie podstrony, które wyglądają inaczej niż pozostałe)`
4. Projekt Graficzny musi zostać przygotowany i przedstawiony Zamawiającemu przez Wykonawcę oraz zaakceptowany przez Zamawiającego dla każdego Wydania, zgodnie z zakresem danego Wydania.
5. Projekt Graficzny musi zostać przygotowany przez Wykonawcę w formacie umożliwiającym nanoszenie komentarzy i próśb o zmianę przez Zamawiającego.
6. Praca z Projektem Graficznym nie może obciążać Zamawiającego koniecznością ponoszenia dodatkowych kosztów, np. przez konieczność dokupienia dodatkowych licencji na oprogramowanie. Dopuszczalne jest uwzględnienie licencji na dodatkowe oprogramowanie w ofercie.
7. Projekt Graficzny będzie zawierał pliki wyjściowe w formacie, umożliwiającym otwarcie w standardowych narzędziach systemu Windows (pakiet MS Office 365) .
8. Projekt graficzny, po zaakceptowaniu przez Zamawiającego, powinien zostać wyeksportowany do formatu raportu .docx i przekazany Zamawiającemu.
9. Projekt graficzny musi uwzględniać standardy UX Zamawiającego opisane w dokumencie będącym załącznikiem nr 4, standard **WCAG** w aktualnej wersji i odpowiednie wymagania Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

11. Harmonogram realizacji wdrożenia

1. Harmonogram musi zawierać kamienie milowe i produkty.
2. Harmonogram musi zawierać sekwencję zdarzeń.
3. Harmonogram musi uwzględniać wykorzystanie odpowiednich zasobów ludzkich po stronie Zamawiającego.
4. Harmonogram musi określać rozłożone w czasie Wydania.
5. W harmonogramie muszą zostać w szczególności uwzględnione następujące elementy:
    a. Dostarczenie Projektu Technicznego
    b. Dostarczenie planu testów i scenariuszy testowych
    c. Przygotowanie środowiska przez Wykonawcę z podziałem na środowisko testowe i produkcyjne
    d. Dostarczenie, instalacja i konfiguracja przez Wykonawcę Systemu w środowisku testowym
    e. Dostarczenie Dokumentacji
    f. Dostarczenie, instalacja i konfiguracja przez Wykonawcę Systemu w środowisku produkcyjnym
    g. Szkolenia dla Administratorów IT i Użytkowników Wewnętrznych
    h. Dostarczenie szkoleń e-learning dla Użytkowników Zewnętrznych i Wewnętrznych
    i. Rozpoczęcia i zakończenia poszczególnych Wydań
6. Harmonogram musi zawierać terminy, czas trwania poszczególnych elementów wymienionych w pkt 5. Harmonogram zostanie przedstawiony do akceptacji
7. Zamawiającego w terminie 1 tygodnia od dnia podpisania Umowy. Obustronnie zaakceptowany Harmonogram będzie stanowił część Projektu Technicznego.

Wydanie

1. Wydanie jest okresem czasu w trakcie trwania projektu wdrożenia Systemu, w którym realizowane są określone przez Wykonawcę wymagania funkcjonalne i poza funkcjonalne z zakresu wszystkich wymagań OPZ. Następnie wskazany przez Wykonawcę zakres jest odbierany przez Zamawiającego.
2. Plan wydania wskazuje, które wymagania OPZ zostaną zrealizowane w danym Wydaniu.
3. Minimalna ilość planowanych wydań w projekcie to 4. Minimalny czas trwania Wydania to 1 miesiąc. Zakres ostatniego wydania przed etapem stabilizacji Systemu może realizować maksymalnie 15% wszystkich wymagań z OPZ.
4. Wydanie składa się z odbioru następujących produktów dla określonego w wydaniu zakresu wymagań z OPZ.
    - Zaktualizowany Projekt Techniczny
    - Projekt Graficzny
    - Scenariusze testowe
    - Wdrożony testowo/produkcyjnie System
    - Procedura testów wg Planu testów w tym testy akceptacyjne Zamawiającego
5. Każde wydanie musi dostarczać działającą i możliwą do przetestowania przez Zamawiającego część Systemu.
6. Każde kolejne wydanie powinno rozwijać w sposób narastający System.

Wdrożenie

Wdrożenie Systemu musi obejmować:

1. Uruchomienie środowiska testowego z dostępem dla Zamawiającego
2. Dostarczenie Systemu.
3. Udzielenie Zamawiającemu wsparcia podczas testów Systemu przeprowadzanych przez Zamawiającego.
4. Uruchomienie produkcyjne Systemu.
5. Przeprowadzenie testów i audytów

Plan testów i audytów

Plan testów i audytów oraz scenariusze testowe:

1. Plan testów i audytów określa koncepcje wykonania testów i audytów na przestrzeni całego projektu. Natomiast w poszczególnych Wydaniach Plan testów i audytów będzie implementowany, przygotowywane będą scenariusze testowe i na ich podstawie wykonywane będą wszystkie rodzaje testów/audytów dla danego zakresu wydania.
2. Plan testów i audytów w zakresie wdrożenia Systemu musi zawierać co najmniej:
    a. Testy funkcjonalne,
    b. Testy wydajności,
    c. Testy spójności danych
    d. Testy akceptacyjne.
    e. Testy swobodne
    f. Audyt bezpieczeństwa kodu (w tym jakości i kompletności)
    g. Audyt bezpieczeństwa (w tym Testy penetracyjne)
    h. Audyt dostępności cyfrowej (WCAG)
    i. Audyt użyteczności (UX)
3. Plan testów i audytów zawiera listę wymagań funkcjonalnych i jakościowych Systemu wynikających z OPZ, które mają zostać poddane testom.
4. Wyłączenia – Zamawiający dopuszcza, aby testy nie obejmowały wybranych elementów w zakresie i obszarze testów, jednak w takiej sytuacji, fragmenty te musza być jasno i precyzyjnie określone wraz z podaniem przyczyny, dla której następuje wyłączenie. Wyłączenia muszą być zatwierdzone przez Zamawiającego. Brak zgody Zamawiającego skutkuje koniecznością przeprowadzenia testów w tym zakresie.
5. Plan testów i audytów zawiera harmonogram ich realizacji, tj. określa w jaki sposób testy będą realizowane dla poszczególnych Wydań.
6. Plan testów i audytów zawiera spis środowisk przeznaczonych do wykorzystania w trakcie testów.
7. Plan testów i audytów i scenariusze testowe zostaną opracowane przez Wykonawcę.
8. Plan testów i audytów musi zostać zaakceptowany przez Zmawiającego w zakresie zgodności z wymogami wskazanymi w Umowie.
9. Scenariusze testowe mają określone warunki, których spełnienie pozwala na rozpoczęcie testów.
10. Scenariusze testowe zawierają cel testu i zestaw kryteriów pozwalających uznać test za zakończony z wynikiem pozytywnym. Zestaw kryteriów podlega akceptacji Zamawiającego.

11. Audyt bezpieczeństwa i testy penetracyjne, audyt bezpieczeństwa kodu, audyt użyteczności i audyt dostępności cyfrowej (WCAG) zostaną zrealizowane przez Wykonawcę i zakończą się sporządzeniem odpowiednich Raportów.
12. Test spójności danych dotyczyć będzie metod i procesów wykorzystywanych do weryfikacji i zarządzania danymi oraz samą bazą danych. Celem testu będzie sprawdzenie metod dostępu do danych, sprawdzenia poprawności wdrożonych funkcji procesu i potwierdzenie, że korzystanie z bazy danych przez użytkowników zewnętrznych, nie powoduje zmiany danych, niepożądanych modyfikacji bazy oraz innych podobnych problemów. Test zakończy się sporządzeniem odpowiedniego Raportu przez Wykonawcę.
13. Zakres, wykorzystywane standardy i metody prowadzenia testów/audytów podlegają akceptacji Zamawiającego na etapie Projektu Technicznego.

12. Licencje

Wykonawca przekaże autorskie prawa majątkowe w zakresie pól eksploatacji i na zasadach określonych w Umowie na Oprogramowanie dedykowane wraz z kodami źródłowymi.

Wykonawca udzieli Zamawiającemu licencji na Oprogramowanie Standardowe w oparciu o liczbę użytkowników na moduł. Liczby użytkowników są wskazane w rozdziałach dotyczących wymagań do odpowiednich systemów. W przypadku licencji na czas inny niż nieoznaczony (zarówno licencji chmurowych jak i licencji na oprogramowanie instalowane u Zamawiającego) konieczne jest wyszczególnienie, związanych z licencjonowaniem, kosztów w czasie. Wykonawca powinien ponadto dostarczyć opis funkcjonalności, które zapewnia licencja wraz z liczbą użytkowników, którą obejmuje.

Dostarczane przez Wykonawcę licencje obejmują wszystkie komponenty i biblioteki Systemu, w tym stosowane przez Wykonawcę komponenty OpenSource i komponenty firm trzecich muszą umożliwiać integrację z nielimitowaną liczbą usług i systemów poprzez interfejsy integracyjne REST lub SOAP API oraz połączenia ODBC/JDBS/ADO.NET.

13. Dokumentacja

Ogólne

1. Dokumentacja sporządzona na potrzeby Zamówienia musi być zgodna ze stanem prawnym aktualnym na dzień przedstawienia jej do odbioru Zamawiającemu.
2. Dokumentacja powinna obejmować wszystkie komponenty Systemu
3. Dostarczona Dokumentacja musi być w języku polskim, być spójna i nie może zawierać sprzeczności. Wykonawca musi zapewnić wzajemną zgodność pomiędzy wszystkimi rodzajami informacji umieszczonymi w Dokumentacji, brak logicznych sprzeczności oraz spójność pomiędzy informacjami zawartymi w Dokumentacji.
4. Dostarczona Dokumentacja ma charakteryzować się:
    a. Jednolitą strukturą, rozumianą jako podział danego dokumentu na rozdziały, podrozdziały i sekcje w czytelny i zrozumiały sposób.
    b. Jednolitym sposobem opisywania rozumianym jako zachowanie spójnej struktury, formy i sposobu pisania.
    c. Poprawnością ortograficzną.
    d. Aktualnymi odnośnikami do innych dokumentów, rozdziałów lub fragmentów Dokumentacji.
    e. Musi w całości opisywać funkcjonalności Systemu.
    f. Musi zawierać pełne przedstawienie omawianego problemu obejmujące całość rozpatrywanego zakresu zagadnienia i nie zawierać zbędnej treści.
    g. Musi zawierać uzgodnienia poczynione z Zamawiającym w trakcie realizacji przedmiotu Umowy.
    h. Musi być spójna z Systemem Identyfikacji Wizualnej NIZP PZH-PIB.

Dokumentacja Użytkownika

Dokumentacja Użytkownika powinna zawierać:

1. Instrukcję użycia Sytemu krok po kroku dla wszystkich wymaganych funkcjonalności
2. Komplet zrzutów ekranu z komponentów Systemu dla każdego indywidualnego ekranu/okna systemu, w celu obrazowego zaprezentowania użytkownikowi koniecznych kroków
3. Wyjaśnienie zasady komunikacji systemu z użytkownikiem – kolory błędów, zasady walidacji, schemat rozwiązywania problemów
4. Opis zastosowania wszystkich użytych słowników.
5. Listę i opis ikon, przycisków i skrótów klawiaturowych.
6. Opis wszystkich parametrów Systemu związanych z jego ustawieniami i funkcjonalnościami.
7. Zawierać wykaz możliwych do przyznania uprawnień do Systemu wraz z ich opisem

Dokumentacja Administratora

Dokumentacja Administratora powinna zawierać:

1. Opis konfiguracji Systemu, w tym wykaz wdrożonych komponentów, relacji pomiędzy nimi, opis ich konfiguracji, implementacji w środowiskach, implementacji integracji.
2. Kompletną instrukcję instalacji i konfiguracji:
    a. Systemu
    b. baz danych
    c. szyny danych
    d. kolejek

3. Opis postępowania w przypadku sytuacji awaryjnych – lista poleceń potrzebnych do uruchomienia wszystkich komponentów Systemu
4. Komplet skryptów bazodanowych do odtworzenia baz danych
5. Instrukcje start/stop dla całego środowiska.
6. Instrukcje eksploatacyjne dla administratorów.
7. Instrukcje wykonywania kopii zapasowych i odtwarzania Systemu z kopii.

Dokumentacja Techniczna

Dokumentacja Techniczna powinna zawierać:

1. Specyfikacje interfejsów i funkcje API oraz strukturę baz danych wraz z referencyjnym modelem danych, elementów danych i metadanych w formacie dokumentu DOC(X) lub PDF
2. Schemat architektury Oprogramowania wraz z opisem.
3. Diagramy klas i struktura bazy danych wraz z opisem uwzględniająca powiązania i zależności między elementami w formacie zgodnym z Enterprise Architect w wersji 15 lub nowszej (XML).
4. Wymagania techniczne dotyczące sprzętu i środowiska (z dokładnością do wersji środowiska).
5. Ustawienia konfiguracyjne środowiska, w którym pracuje System, w tym również opis implementacji w środowisku wraz z procedurami start/stop dla wszystkich komponentów Systemu.
6. Opis parametrów konfiguracji Systemu i sposób ich wykorzystania.
7. Opis techniczny rodzajów i zastosowanych protokołów komunikacji (w tym certyfikatów).
8. Sposób wykonania instalacji Systemu, instalacji poprawek i kolejnych wersji.
9. Procedurę odtworzenia danych i konfiguracji.
10. Proces tworzenia kopii zapasowych.
11. Diagram przepływu danych pomiędzy Systemem, a wszystkimi aplikacjami mającymi się integrować.
12. Diagram przepływu danych pomiędzy poszczególnymi modułami wewnątrz Systemu,.
13. Instrukcję integracji, w wersji do udostępniania osobom trzecim w celu właściwego zintegrowania się z Systemem zawierającą:
    - opis usługi, interfejsów i wytyczne umożliwiające integrację Systemu
    - pliki ze schematami (WSDL, GML, itp.)
    - opis metod i struktur danych interfejsów.
14. Słownik danych – zaleca się taki, w którym dla danych w formatkach i raportach Systemu przywołano odpowiednie pole w tabeli lub widoku w bazie.
15. Wykaz danych podlegających kontroli poprawności wraz z informacją o sposobie kontroli poprawności.
16. Wykaz komunikatów diagnostycznych i standardowych błędów (opis błędu, warunki jego powstania).

Dokumentacja Powykonawcza

Dokumentacja Powykonawcza powinna zawierać:

1. Kompletny opis środowiska produkcyjnego i testowego
    a. Opis maszyn wirtualnych i irch rozmieszczenia na serwerze/serwerach
    b. Opis zainstalowanych komponentów/systemów/aplikacji, ich lokalizacji, roli, uprawnieniach

2. Spis wszystkich użytkowników administracyjnych (serwerowych, bazodanowych, aplikacyjnych itp.) wraz z danymi autoryzacyjnymi
3. Spis wszystkich utworzonych użytkowników (serwerowych, bazodanowych, aplikacyjnych itp.) z zakresem praw jakie posiadają oraz opisem
4. Raporty zawierające wyniki testów/audytów akceptacyjnych, funkcjonalnych, swobodnych, bezpieczeństwa, bezpieczeństwa kodu, penetracyjnych, użyteczności
5. Protokoły zdawczo – odbiorcze dla poszczególnych składowych systemu

Polityka bezpieczeństwa

Polityka Bezpieczeństwa musi być opracowana zgodnie z obowiązującymi przepisami prawa Rzeczpospolitej Polskiej oraz prawem Unii Europejskiej, w tym zgodnie z wymaganiami Krajowych Ram Interoperacyjności, Krajowym Systemie Cyberbezpieczeństwa, normą PN-EN ISO/IEC 27001 jak również z obowiązującymi przepisami w zakresie ochrony danych osobowych.

Polityka bezpieczeństwa musi obejmować cały wdrażany System wraz z poszczególnymi modułami. Powinna zawierać m.in:

1. Regulamin Ochrony Danych Osobowych,
2. Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji zgodne z regulacjami RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679);
3. Regulamin Ciągłości Działania,
4. Instrukcję bezpiecznego administrowania systemami teleinformatycznymi,
5. Listy wymagań minimalnych dla głównych klas zbiorów danych,
6. Instrukcję bezpiecznego użytkowania systemów teleinformatycznych,
7. Procedurę okresowych wewnętrznych audytów bezpieczeństwa,
8. Plan audytów wewnętrznych i zewnętrznych,
9. Instrukcję sporządzania cyklicznych raportów dla właścicieli kluczowych zbiorów danych i kadry zarządzającej,
10. Procedury eksploatacyjne dla głównych klas zbiorów danych,
11. Szablony rejestrów przewidzianych w regulaminach, instrukcjach i procedurach,
12. Wymagane procedury bezpieczeństwa i instrukcje wynikających z regulaminów bezpieczeństwa obszarów.
13. Określenie sposobu kwalifikacji incydentów włączając w to parametry je określające i poziomy/istotność incydentów
14. Określanie konkretnych środków i miar mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w kontekście oferowania usług objętych wdrażanym Systemem.

Wraz z Polityką bezpieczeństwa opracowana zostanie metodyka szacowania ryzyka oraz na jej podstawie przeprowadzony proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w systemie.

14. Kody źródłowe Systemu

Kody źródłowe muszą być przekazane w formie elektronicznej (przed kompilacją), umożliwiającej analizę i rozbudowę zarówno przez Zamawiającego jak i firmy trzecie działające na potrzeby Zamawiającego. Wykonawca musi przekazać informację o:

1. wszystkich bibliotekach i dodatkach niezbędnych do kompilacji i uruchomienia kodu
2. rekomendowanym środowisku programistycznym wraz ze wskazaniem niezbędnych dodatków
3. parametrach i zmiennych środowiska programistycznego koniecznych do kompilacji i uruchomienia Systemu, instrukcji minimalnych czynności pozwalających na uruchomienie Systemu (wraz z kompilacją, jeżeli jest potrzebna)
4. rekomendacji w zakresie kompilatora i jego ustawień
5. w przypadku przekazywania kodu źródłowego Systemu, musi być on przekazany w taki sposób, aby było możliwe umieszczenie kodu w lokalnym repozytorium Zamawiającego.
6. Kod skryptów do obsługi/wdrażania (CI/CD).

Kody źródłowe wytwarzane i dostarczane przez Wykonawcę będą gromadzone w repozytorium udostępnionym przez Wykonawcę. Wykonawca zapewni wymagane dostępy dla Zamawiającego do tego repozytorium.

W przypadku kodów źródłowych wytwarzanych przez Wykonawcę po ich akceptacji i/lub odbiorze przez Zamawiającego, Wykonawca zobowiązany będzie do ich utrzymywania i zapewnienia aktualności w ramach prowadzonych prac projektowych.

Kody źródłowe powinny zawierać wskazanie:

1. wersji i dystrybucji wszystkich niezbędnych komponentów
2. sposobu instalacji bibliotek i dodatków
3. sposobu ustawiania parametrów i zmiennych środowiskowych.

W celu dokonania weryfikacji kompletności i czytelności kodu źródłowego, w obecności Zamawiającego Wykonawca ma dokonać kompilacji i sprawdzenia poprawności działania kodu źródłowego o ile na etapie projektu technicznego nie zostanie ustalony inny tryb weryfikacji kodu źródłowego.

15. Asysta i Konserwacja Techniczna

1. W ramach świadczenia ATiK Wykonawca:
   a. zapewnieni prawidłowe funkcjonowanie Systemu zgodne z warunkami Umowy oraz Dokumentacją,
   b. usunie Błędy na zasadach określonych w Umowie,
   c. dostarczy Modyfikacje Systemu,
   d. dostarczy Usprawnienia Systemu,
   e. dostarczy Wersje Systemu,
   f. zapewni usługę konsultacji elektronicznych polegających na udzielaniu porad i wyjaśnień dotyczących zasad działania Systemu oraz możliwości i warunków jego rozbudowy,
   g. przeniesie dane ze struktur poprzedniej Wersji Systemu do struktur Wersji Systemu, jeżeli Wersja Systemu tego wymaga,
   h. utrzyma sprawność Systemu na co najmniej takim poziomie jaki był przed zainstalowaniem Usprawnień, Modyfikacji i Wersji Systemu, przy zabezpieczeniu przez Zamawiającego odpowiedniej konfiguracji sprzętowo-systemowej,
   i. zapewni Zamawiającemu wsparcie i pomoc w usuwaniu nieprawidłowości działania Systemu wynikających z instalacji Oprogramowania Standardowego,
   j. zapewni konserwację Systemu obejmującą prace związane z rekonfiguracją Systemu,
   k. zapewni wsparcie i pomoc w zakresie zarządzania Systemem.
2. Wykonawca zobowiązany jest do dostarczenia Modyfikacji Systemu przed terminem wejścia w życie zmian w przepisach prawnych, jeżeli zostały one opublikowane co najmniej 14 Dni roboczych przed ich wejściem w życie, a jeżeli warunek ten nie jest spełniony – w terminie 14 Dni roboczych od dnia ich opublikowania. W uzasadnionych przypadkach Strony mogą ustalić inny termin wykonania Modyfikacji Systemu.
3. Wykonawca zobowiązany jest do przeprowadzenia przed dostarczeniem do Zamawiającego testów Usprawnień Systemu, Wersji Systemu oraz Modyfikacji Systemu we własnym środowisku testowym, które składa się co najmniej z takiej samej wersji Systemu, jaką posiada Zamawiający w tym również pod kątem:
   a. poprawnego działania dostarczonego rozwiązania,
   b. poprawnego działania wszystkich pozostałych funkcjonalności Systemu, której dotyczy dostarczone rozwiązanie.
4. Wykonawca zobowiązany jest do dostarczenia Zamawiającemu do 10 Dni roboczych po instalacji każdej Modyfikacji, każdego Usprawnienia, każdej Wersji Systemu zaktualizowanej Dokumentacji (jeżeli taka aktualizacja jest konieczna) w wersji elektronicznej w formacie umożliwiającym jej wydruk i modyfikację.
5. W ramach ATiK Wykonawca przystąpi niezwłocznie do usunięcia Błędów i udzielenia odpowiedzi w ramach konsultacji elektronicznych. Powyższe czynności będą trwać nie dłużej niż:
   a. usunięcie Błędów krytycznych – do 1 Dnia roboczego od momentu zgłoszenia,
   b. usunięcie Błędów niekrytycznych – do 5 Dni roboczych od momentu zgłoszenia,
   c. udzielenie odpowiedzi w ramach konsultacji elektronicznych – do 10 Dni roboczych od momentu zgłoszenia.
6. Czas usunięcia Błędu/udzielania konsultacji elektronicznych, o którym mowa w ust. 5, jest liczony od momentu przekazania zgłoszenia Błędu/potrzeby udzielenia konsultacji

elektronicznych przez Zamawiającego do momentu usunięcia Błędu/udzielenia odpowiedzi w ramach konsultacji elektronicznej.

16. Szkolenia

1. Terminy realizacji szkoleń zostaną uzgodnione z Zamawiającym na etapie Projektu Technicznego.
2. Zakres szkoleń:
   Szkolenia Użytkowników Wewnętrznych i Administratorów IT
   - Ogólne szkolenie dla wszystkich Użytkowników Wewnętrznych Systemu (łącznie 150 osób),
   - Szkolenia z poszczególnych części Systemu dla 20 Użytkowników i dla 6 Administratorów IT
   - E-learning dla użytkowników Systemu (osobno w wersji dla Użytkowników Wewnętrznych i Zewnętrznych)- dostarczenie paczki SCORM na platformę e-learningową Zamawiającego wraz z materiałami szkoleniowymi i testami wiedzy.
   - E-learning dla Użytkowników Wewnętrznych i dla Administratorów IT - dostarczenie paczek SCORM na platformę e-learningową Zamawiającego wraz z materiałami szkoleniowymi i testami wiedzy.
   - Użytkownicy Wewnętrzni będą mieli stały dostęp do materiałów e-learning od etapu testowania produktów. Cyklicznie co pół roku przeprowadzane będą testy wiedzy.
   - Wykonawca musi uwzględnić ciągłość pracy Zamawiającego
   - Wykonawca utrwali w formie audio-video wszystkie przeprowadzone Szkolenia

17. Uwarunkowania prawne, normy i systemy

Oprogramowanie powinno spełniać obowiązujące wymagania prawne, w szczególności:

1. RODO (Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - ogólne unijne rozporządzenie zawierające przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.
2. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych – Ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. i Sprostowanie do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 23 maja 2018r.
3. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz.U. 2019 poz. 730 z późn. zm.).
4. Ustawa z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz.U. 2018 poz. 1544 z późn. zm.)
5. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości Dz.U. 2019 poz. 125Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228 z późn. zm.)
6. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019 poz. 848 z późn. zm.), w szczególności wymagania WCAG (Web Content Accessibility Guidelines) w wersji 2.1
7. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021r. poz. 670 z późn. zm.), w szczególności minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych.
8. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2022 poz. 1863 z późn. zm.).
9. Norma PN-ISO/IEC 27001:2017-06 – Systemy zarządzania bezpieczeństwem informacji
10. Norma PN-ISO/IEC 27005:2014-01 - Zarządzanie ryzykiem w bezpieczeństwie informacji
11. Standardy wynikające z wytycznych horyzontalnych MIiR.
12. Standard OWASP TOP TEN (https://www.owasp.org) - Standard Weryfikacji Bezpieczeństwa Aplikacji
13. Rozporządzenie rady ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jednolity Dz.U.2017 poz. 2247 z późn. zm.).
14. Rozporządzenie (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów,

zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE wraz z rozporządzeniami wykonawczymi KE oraz zmieniającymi go Rozporządzeniami Komisji UE i WE , jeśli dotyczy - z późniejszymi zmianami.

15. System ma być zgodny z zapisami dokumentów NIZP PZH-PIB (chyba, że OPZ stanowi inaczej):
    a. Załącznik nr 2 – Strategia bezpieczeństwa
    b. Załącznik nr 3 – Plan zapewnienia jakości
    c. Załącznik nr 4 – Rekomendacje UX

18. Załączniki do dokumentu

Załącznik nr 1 - Modele procesów (stanowią integralną część wymagań funkcjonalnych i poza funkcjonalnych) dla Panelu Klienta (W2) i pośrednio dla W1(rozbudowa):

- PeA.1 Rejestracja nowego Klienta
- PeA.2 Zgłaszanie produktu do certyfikacji (w zakresie wykraczającym poza proces PB.2 Sprzedaż i P.3.18 Atesty)
- PeA.3 Monitorowanie statusu procesu certyfikacji
- PeA.4 Monitorowanie statusu istniejących Certyfikatów
- PeA.6 Zarządzanie kontem
- PeA.7 Pozyskanie informacji o certyfikacji
- PeA.8 Wniosek o zmiany/ duplikat/Certyfikat w języku obcym (w zakresie wykraczającym poza proces PB.2 Sprzedaż i P.3.18 Atesty)
- PB.2 Sprzedaż
- P.3.18 Atesty

Załącznik nr 2 – Strategia bezpieczeństwa
Załącznik nr 3 – Plan zapewnienia jakości
Załącznik nr 4 – Rekomendacje UX
Załącznik nr 5 – Załączniki do wniosku o atest świadectwo
Załącznik nr 6 – Grupy atestowanych wyrobów i wymagania