Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

Znak sprawy: BA.WZP.26.25.2023

Załącznik nr 1 do SWZ

Opis Przedmiotu Zamówienia w postępowaniu pn. „Zaprojektowanie, budowa, dostarczenie i wdrożenie Rozbudowy Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej oraz świadczenie usług wsparcia ”

Warszawa, 30 czerwca 2023 r.

Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

Spis treści

1. Słownik pojęć

Pojęcie	Opis
Administrator UKE/ Administrator Systemu	Administrator IT i/lub administrator merytoryczny **Administrator IT** – zarządza Użytkownikami i uprawnieniami (również administratorów merytorycznych). Posiada uprawnienia do konfiguracji harmonogramu zasileń, zarządzania liczbą wątków oraz przeglądania dziennika błędów; **Administrator merytoryczny** – ma zapewnione funkcjonalności dostępne dla Użytkownika oraz możliwość zarządzania elementami z części portalu mapowego GIS oraz możliwość przeglądania między innymi magazynu raportów, rejestru zasileń czy statystyk dotyczących aktywności Użytkowników
API	API (z ang. Application Programming Interface) oznacza Interfejs Programowania Aplikacji. To sposób komunikacji między aplikacjami sieciowymi a składnikami oprogramowania oraz wymiany informacji pomiędzy odrębnymi systemami.
Architektura mikroserwisów	Styl tworzenia architektury aplikacji komputerowych implementujący wzorzec architektury zorientowanej na usługi, który aranżuje aplikację jako zbiór luźno połączonych ze sobą niewielkich serwisów komunikujących się poprzez lekkie protokoły komunikacyjne. Celem jest zapewnienie niezależności poszczególnych komponentów, które mogą być rozwijane niezależnie od pozostałych elementów składowych systemu oraz wyraźny podział komponentów tak, by realizowały jedną, konkretną logikę biznesową lub programową.
Architektura zorientowana na usługi (SOA)	Koncepcja tworzenia systemów informatycznych, w której główny nacisk stawia się na definiowanie usług, które spełnią wymagania użytkownika. Pojęcie SOA obejmuje zestaw metod organizacyjnych i technicznych mający na celu powiązanie biznesowej strony organizacji z jej zasobami informatycznymi.
Awaria	Błąd powodujący nieprawidłowości w funkcjonowaniu systemu PUE niezgodnie z dokumentacją lub specyfikacją wymagań, powodujące niemożność lub utrudnienia w eksploatacji Systemu
Błąd	Niedziałanie lub nieprawidłowe działanie Rozbudowanego Systemu niezależnie od przyczyny takiej nieprawidłowości. W szczególności Błędem jest działanie Systemu PUE niezgodnie z Dokumentacją. Błędom przypisane są kategorie. Szczegółowa klasyfikacja poszczególnych kategorii błędów znajduje się w rozdziale Wymagania w zakresie Gwarancji i Usług Wsparcia.
Błąd regresji	Błąd w Oprogramowaniu, występujący po zmianie części kodu źródłowego, na skutek, którego dochodzi do błędnego działania funkcji Oprogramowania, która przed dokonaniem tej zmiany działała prawidłowo.

Pojęcie	Opis
CSU	Centralny System Uwierzytelniania Urzędu Komunikacji Elektronicznej zrealizowany w oparciu o WSO2IS dostępny pod adresem csu.uke.gov.pl.
ESOD	Elektroniczny System Obiegu Dokumentów funkcjonujący w Urzędzie.
Hot-fix	Poprawka naprawiająca konkretny błąd w systemie
JIRA	Oprogramowanie do śledzenia postępu realizacji projektu i obsługi zgłoszeń serwisowych dostępne pod adresem jira.uke.gov.pl
Mikroserwisy	Małe aplikacje wykonujące jedno powierzone im zadanie w oparciu o niezależne od siebie komponenty lub procesy stanowiące oddzielne części tej samej aplikacji.
POPC	Program Operacyjny Polska Cyfrowa
Projekt	Realizowany przez Zamawiającego projekt p.n. w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", działanie 2.2 „Cyfryzacja procesów back-office w administracji rządowej", na podstawie porozumienia o dofinansowanie nr POPC.02.02.00-00-0045/22-00
PUE	Platforma Usług Elektronicznych Urzędu Komunikacji Elektronicznej dostępna pod adresem pue.uke.gov.pl
RODO	Rozporządzenie 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)
Rozbudowany System	System teleinformatyczny obejmujący istniejące (system PUE) i rozbudowane rozwiązanie dotyczące Platformy Usług Elektronicznych, spełniający wymagania określone w OPZ. Ilekroć w OPZ jest mowa o Rozbudowanym Systemie należy przez to rozumieć również Rozbudowaną Część Systemu (SSO i MOUM).
SLA	gwarantowany poziom świadczenia usług, ang. Service Level Agreement, zgodnie z wymaganiami OPZ. Zapewnienie realizowane w okresie gwarancji lub prawa opcji na podstawie art. 441 ustawy Pzp, w przypadku skorzystania przez Zamawiającego z tego prawa.
SSO	System pojedynczego logowania, ang. Single Sign-On, w UKE zrealizowany jako Centralny System Uwierzytelniania (CSU)
System/PUE	System informatyczny pod nazwą: Platforma Usług Elektronicznych dostępny pod adresem pue.uke.gov.pl.
UKE	Urząd Komunikacji Elektronicznej

Pojęcie	**Opis**
Użytkownik	Każda osoba uprawniona do wykonywania czynności w Rozbudowanym Systemie, różnych w zależności od roli definiującej zakres tych uprawnień, w tym m.in. zasilania, przetwarzania, analizowania i eksportowania danych.
WCAG	Wytyczne dotyczące dostępności treści internetowych, ang. Web Content Accessibility Guidelines, zgodnie ze standardem w wersji 2.1

2. Wstęp

Przedmiot zamówienia obejmuje w szczególności następujące elementy:

2.1. Zaprojektowanie, budowę, dostarczenie i wdrożenie Rozbudowy Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej obejmującego nowy wygląd i zmiany UX;

2.2. Zaprojektowanie, budowę, dostarczenie i wdrożenie Modułu SSO;

2.3. Zaprojektowanie, budowę, dostarczenie i wdrożenie Modułu digitalizacji i zarządzania umowami;

2.4. Przeprowadzenie badań użytkowników dotyczących interfejsu;

2.5. Opracowanie i dostarczenie Analizy przedwdrożeniowej zawierającej opis koncepcji rozbudowy Systemu wraz z uwzględnieniem wszystkich obecnych funkcjonalności oraz opisem sposobu realizacji wszystkich wymagań wynikających z opisu przedmiotu zamówienia, a także opis infrastruktury udostępnionej przez Zamawiającego do rozbudowy Systemu PUE oraz ewentualnej jej rozbudowy w celu spełnienia wymagań SLA;

2.6. Zaprojektowania, budowy, dostarczenia i wdrożenia w oparciu o technologię mikroserwisów wyposażonych w API nowej architektury Platformy Usług Elektronicznych.

W ramach wykonania przedmiotu zamówienia Wykonawca zapewni:

2.7. Wykonanie i dostarczenie Dokumentacji Technicznej, Dokumentacji Testowej, Dokumentacji Użytkownika, Dokumentacji Instruktażowej, Dokumentacji Administratora Systemu oraz jej aktualizacja;

2.8. Przygotowanie, zorganizowanie i przeprowadzenie instruktaży dla Użytkowników oraz Administratorów Rozbudowanego Systemu po stronie UKE oraz opracowanie materiałów instruktażowych, w tym modułów szkoleniowych;

2.9. Zasilenie Rozbudowanego Systemu wszystkimi danymi znajdującymi się obecnie w Systemie PUE oraz danymi, którymi będzie zasilony System PUE do czasu uruchomienia Rozbudowanego Systemu;

2.10. Zapewnienie stabilnej, wydajnej i zgodnej z dokumentacją pracy Rozbudowanego Systemu;

2.11. Gwarancję w okresie 3 miesięcy,

2.12. Usługi Wsparcia w liczbie 100 roboczogodzin, realizowane do dnia podpisania Protokołu Odbioru Rozbudowanego Systemu.

2.13. W ramach prawa opcji Wykonawca zapewni świadczenie:

a) Usług wsparcia w liczbie 500 roboczogodzin,

b) Usług Rozwoju Rozbudowanego Systemu w liczbie 1 000 roboczogodzin,

realizowanych od dnia podpisania Umowy do końca okresu Gwarancji.

Skorzystanie przez Zamawiającego z Prawa Opcji uzależnione jest od potrzeb Zamawiającego stwierdzonych na etapie eksploatacji Rozbudowanego Systemu oraz posiadania przez Zamawiającego środków finansowych przeznaczonych na realizację Umowy.

Zamówienie opcjonalne nie stanowi zobowiązania Zamawiającego do jego udzielenia, jak również nie stanowi podstawy do dochodzenia przez Wykonawcę roszczeń odszkodowawczych z tytułu niezrealizowania tego zamówienia.

2.14. Realizacja przedmiotu zamówienia podzielona zostanie na następujące etapy:

a) Etap I – SSO

b) Etap II – MOUM

c) Etap III – Rozbudowa Systemu PUE

Etap	Zadania do realizacji przez Wykonawcę w ramach Etapu
Etap I SSO	1. Przeprowadzenie badania UX w zakresie Rozbudowanej Części Systemu (SSO), 2. Przygotowanie analizy przedwdrożeniowej obejmującej swoim zakresem wyniki badania UX oraz szczegółowy opis Etapu I, 3. Opracowanie dokumentacji dla Etapu I, 4. Budowa Rozbudowanej Części Systemu (SSO), 5. Integracja i wdrożenie Rozbudowanej Części Systemu (SSO), 6. Testy wydajności SSO, 7. Testy bezpieczeństwa SSO, 8. Przedstawienie Rozbudowanej Części Systemu (SSO) do odbioru, 9. Przygotowanie materiałów szkoleniowych dla administratorów w zakresie Rozbudowanej Części Systemu (SSO) oraz przeprowadzenie szkoleń. 10. Start produkcyjny SSO
Etap II MOUM	1. Przeprowadzenie badania UX w zakresie Rozbudowanej Części Systemu (MOUM) 2. Przygotowanie analizy przedwdrożeniowej obejmującej swoim zakresem wyniki badania UX oraz szczegółowy opis Etapu II i aktualizację opisu Etapu I (jeśli dotyczy), 3. Opracowanie dokumentacji dla Etapu II, 4. Budowa Rozbudowanej Części Systemu (MOUM), 5. Dostarczenie narzędzia do digitalizacji umów międzyoperatorskich., 6. Integracja i wdrożenie Rozbudowanej Części Systemu (MOUM), 7. Testy wydajności MOUM, 8. Testy bezpieczeństwa MOUM, 9. Przedstawienie Rozbudowanej Części Systemu (MOUM) do odbioru, 10. Przygotowanie materiałów szkoleniowych dla użytkowników i administratorów w zakresie Rozbudowanej Części Systemu (MOUM) oraz przeprowadzenie szkoleń. 11. Start produkcyjny MOUM
Etap III	1. Przeprowadzenie badania UX w zakresie Rozbudowanego Systemu 2. Przygotowanie analizy przedwdrożeniowej obejmującej swoim zakresem wyniki badania UX oraz szczegółowy opis Etapu III i aktualizację opisu Etapu I (jeśli dotyczy) lub Etapu II (jeśli dotyczy),

Rozbudowa Systemu PUE	3. Opracowanie dokumentacji dla Etapu II, 4. Budowa Rozbudowanego Systemu, 5. Integracja i wdrożenie Rozbudowanego Systemu, 6. Testy wydajności, 7. Testy bezpieczeństwa, 8. Przedstawienie Rozbudowanej Systemu do odbioru, 9. Przygotowanie materiałów szkoleniowych dla użytkowników i administratorów w zakresie Rozbudowanego Systemu oraz przeprowadzenie szkoleń. 10. Start produkcyjny PUE

3. Przepisy i wymogi prawne

3.1. Rozbudowany System musi być zgodny w szczególności z następującymi aktami prawnymi:

3.1.1. Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2021 r. poz. 777 z późn. zm.);

3.1.2. Ustawa z dnia 30 sierpnia 2019 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz. U. z 2019 r., poz. 1815);

3.1.3. Ustawa z dnia 28 kwietnia 2022 r. o zmianie niektórych ustaw w związku z rozwojem publicznych systemów teleinformatycznych (Dz.U, z 2022, poz. 1022);

3.1.4. Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2022 r., poz. 1648 z późn. zm.);

3.1.5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023r., poz. 57);

3.1.6. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781);

3.1.7. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2021 r., poz. 386, z późn. zm.);

3.1.8. Ustawa o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. z 2020r., poz. 1173, z późn. zm.);

3.1.9. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020r., poz. 2176);

3.1.10. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2019. poz. 848, z późn. zm.);

3.1.11. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. poz. 948);

3.1.12. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski Kodeks Łączności Elektronicznej (Dz. Urz. UE L Nr 321, str. 36);

3.1.13. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. (eIDAS) w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE z dnia 23 lipca 2014 r. (Dz. Urz. UE. L Nr 257, str. 73);

3.1.14. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L 119/1);

3.2. Wykonawca jest zobowiązany do monitorowania i analizy zmian w przepisach prawa mających wpływ na wymagania opisane w SWZ.

3.3. Wykonawca jest zobowiązany do zapewnienia zgodności dokumentu Analizy Przedwdrożeniowej z przepisami prawa obowiązującymi na terytorium Polski w dniu podpisania

umowy (w tym takich, co do których wiadomo, że w dniu Odbioru Końcowego będą miały zastosowanie w przyszłości, np. znajdują się w okresie vacatio legis).

3.4. Wykonawca jest zobowiązany do zapewnienia zgodności Rozbudowanego Systemu z przepisami prawa obowiązującymi na terytorium Polski w dniu przekazania Rozbudowanego Systemu do Odbioru Końcowego.

4. Warunki równoważności

4.1. Jeżeli Zamawiający określił w SIWZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

4.2. W przypadku dostarczania, oprogramowania, szkoleń lub innych produktów równoważnych względem wyspecyfikowanych przez Zamawiającego w SWZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane produkty spełniają wszystkie wymagania i warunki określone SWZ, w szczególności w zakresie:

4.2.1. warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które nie mogą być gorsze niż dla produktu wymienionego w SIWZ,

4.2.2. funkcjonalności równoważnej produktu, która nie może być gorsza od funkcjonalności produktu wymienionego w SWZ,

4.2.3. oprogramowania, które muszą być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego,

4.2.4. oprogramowania, które nie mogą zakłócić pracy środowiska systemowo-programowego Zamawiającego,

4.2.5. oprogramowania, które muszą w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,

4.2.6. oprogramowania, które muszą zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność produktu równoważnego z produktem określonym w SWZ,

4.3. W przypadku zaoferowania przez Wykonawcę produktu równoważnego Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania produktu równoważnego w środowisku sprzętowo-programowym Zamawiającego.

4.4. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty.

4.5. Wraz z produktem równoważnym Wykonawca jest zobowiązany do dostarczenia niżej wymienionego oświadczenia i następujących dokumentów:

4.5.1. oświadczenia dotyczącego zastosowania produktu równoważnego,

4.5.2. pełnego postanowienia licencji / sublicencji produktu równoważnego,

4.5.3. pełnego wykazu funkcjonalności produktu równoważnego,

4.5.4. wykazu miejsc użycia produktu równoważnego.

4.6. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.

5. Harmonogram realizacji zamówienia

5.1. Harmonogram realizacji zadania „Zaprojektowanie, budowa, dostarczenie i wdrożenie Rozbudowy Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej oraz świadczenie usług wsparcia" stanowi załącznik numer 5 do umowy.

5.2. Zamawiający wymaga aby produkty przekazane do odbioru były na tyle wcześnie aby zamawiający miał czas na odbiór zgodnie z tabelą określoną w załączniku nr 5 do umowy oraz Wykonawca miał czas na poprawki wraz z uwzględnieniem powtórnego odbioru od zamawiającego.

5.3. Zamawiający wymaga, aby Dokumentacja (Dokumentacja Użytkownika, Testowa, Administratora Systemu, Instruktażowa, Techniczna) została przekazana Zamawiającemu w dniu przekazania do Odbioru każdego z Etapów Rozbudowanego Systemu.

5.4. Zamawiający wymaga realizacji Przedmiotu Umowy z zachowaniem szczególnych terminów przedstawienia Produktu do Odbioru:

5.4.1. Przygotowanie, zorganizowanie i przeprowadzenie instruktaży dla użytkowników oraz administratorów Rozbudowanego Systemu po stronie Zamawiającego (poza siedzibą Zamawiającego) oraz opracowanie materiałów szkoleniowych – po zakończeniu testów,

5.4.2. Zamówienia wykonane w ramach Usług Rozwoju Rozbudowanego Systemu świadczonych od dnia podpisania Protokołu Odbioru – w terminie ustalonym zgodnie z Umową.

5.4.3. Usługi Wsparcia świadczone od dnia podpisania Protokołu Odbioru – w terminie ustalonym zgodnie z Umową.

5.4.4. Świadczenia gwarancyjne zapewnione od dnia podpisania Protokołu Odbioru - w terminie ustalonym zgodnie z Umową, nie krótszym niż 12 miesiące.

5.5. Prace polegające na realizacji opisanego Przedmiotu Zamówienia zostaną zrealizowane w terminach przedstawionych w Harmonogramie Wdrożenia, opracowanym przez Wykonawcę w ramach Analizy Przedwdrożeniowej.

6. Produkty i świadczenia Wykonawcy

6.1. W ramach realizacji Przedmiotu Zamówienia, Wykonawca zobowiązany jest do realizacji niżej wymienionych świadczeń oraz dostaw:

6.1.1. Rozbudowany System PUE,

6.1.2. Rozbudowana Część Systemu – SSO,

6.1.3. Rozbudowana Część Systemu – MOUM,

6.1.4. Analiza przedwdrożeniowa dla każdego z etapów.

6.1.5. Budowa nowego modułu kreatora formularzy do usług w PUE,

6.1.6. Przebudowa aplikacji PUE z architektury monolitycznej na architekturę mikro serwisów

6.1.7. Przebudowa frontendu PUE z zastosowaniem nowego stosu technologicznego, w oparciu o przeprowadzone badania dotyczące użyteczności tego interfejsu,

6.1.8. Implementacja mechanizmów blockchain w usługach PUE w celu zapewnienia ciągłości oraz niezaprzeczalności dokumentacji w PUE,

6.1.9. Budowa usługi blockchain API dla innych systemów UKE,

6.1.10. Budowa API do dwukierunkowej wymiany dokumentów pomiędzy PUE (dane z usług świadczonych przez UKE za pośrednictwem PUE), a innymi systemami UKE (systemy dostarczające dokumenty do klientów w PUE) w zakresie wysyłania i odbierania dokumentów,

6.1.11. Budowa API dostarczającego informacji z PUE do systemów analitycznych UKE,

6.1.12. Szkolenie pracowników UKE z obsługi rozbudowanej platformy,

6.1.13. Testy systemu PUE, o których mowa w rozdziale 10 i rozdziale 17.

6.1.14. Dokumentacja, o której mowa w rozdziale 11, w skład której wchodzą:

a. Dokumentacja Użytkownika

b. Dokumentacja Techniczna

c. Dokumentacja Instruktażowa

d. Dokumentacja Administratora

e. Dokumentacja Testowa

f. Dokumentacja Analityczna

g. Kody źródłowe

6.1.15. Instruktaże dla użytkowników i administratorów Systemu, o których mowa w rozdziale 14,

6.1.16. Świadczenia gwarancyjne i usługa wsparcia, o których mowa w rozdziale 19,

6.1.17. Usługi Rozwoju, o których mowa w rozdziale 20.

7. Systemy istniejące

7.1. Projektowany system musi współpracować z istniejącymi wewnętrznymi systemami Zamawiającego jak i zewnętrznymi systemami dostarczanymi przez podmioty trzecie, opisanymi w niniejszym Rozdziale.

7.2. Wykaz systemów wewnętrznych Zamawiającego

- UKE AD – usługa katalogowa Active Directory dostarczająca informacji o użytkownikach wewnętrznych UKE.
- SSO - Single sign-on UKE zbudowane w oparciu o WSO2IS.
- ESOD - Elektroniczny System Obiegu Dokumentów
- Business Intelligence (Oracle BI, Tableau). Rozwiązania analityki biznesowej wykorzystywane w UKE.
- Regon UKE – mikroserwis UKE dostarczający na podstawie numeru NIP, dla wewnętrznych systemów UKE informacjizwracanych przez usługę REGON BIR.
- TERYT UKE – mikroserwis UKE dostarczający informacji o danych teryt dla wskazanego adresu.

7.3. Wykaz systemów zewnętrznych

- Krajowy Węzeł Identyfikacji Elektronicznej stanowiący zewnętrznego dostawcę tożsamości dla rozwiązania SSO.

7.4. Przepływy między systemami w rozbudowanym systemie.

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ Interfejsu
1	Platforma Usług Elektronicznych	Business Intelligence (Oracle BI, Tableau)	Dane zgormadzone w usługach na Platformie Usług Elektronicznych	Kopiowanie danych z bazy PUE oraz tryb odwołań bezpośrednich	Krytyczny dla realizacji projektu	DB/REST-API
2	Platforma Usług Elektronicznych	Single sign-on	Żądanie danych uwierzytelniających użytkownika	Tryb odwołań bezpośrednich	Krytyczny dla realizacji projektu	REST-API
3	Single sign-on	Platforma Usług Elektronicznych	Dane użytkowników niezbędne do logowania na Platformie Usług Elektronicznych	Tryb odwołań bezpośrednich	Krytyczny dla realizacji projektu	REST-API
4	Platforma Usług Elektronicznych	Elektroniczny System Obiegu Dokumentów	Dane w tym formularzu zgromadzone w usługach na Platformie Usług Elektronicznych	Tryb odwołań bezpośrednich	Krytyczny dla realizacji projektu	REST-API
5	Elektroniczny System Obiegu Dokumentów	Platforma Usług Elektronicznych	Formularze zgromadzone w Elektroniczny Systemie Obiegu Dokumentów	Tryb odwołań bezpośrednich	Krytyczny dla realizacji projektu	REST-API

6.	Regon UKE	Platforma Usług Elektronicznych	Dane podmiotu na podstawie numeru NIP	Tryb odwołań bezpośrednich	Krytyczny dla realizacji projektu	REST-API
7.	TERYT UKE	Platforma Usług Elektronicznych	Dostarczanie informacji o danych teryt dla wskazanego adresu.	Tryb odwołań bezpośrednich	Krytyczny dla realizacji projektu	REST-API

8. Wymagania w zakresie architektury systemu

8.1. Architektura Systemu musi uwzględniać i spełniać pryncypia architektoniczne określone przez Radę Architektury Informacyjnej Państwa oraz:

8.1.1. Współdzielenie funkcji aplikacji i systemów – minimalizacja liczby serwisów,

8.1.2. Współdzielenie danych,

8.1.3. Integracja systemów z użyciem platform integracyjnych – zwiększenie niezawodności i bezpieczeństwa poprzez centralne zarządzanie bezpieczeństwem dostępu do danych i ukrycie fizycznej lokalizacji dostawcy danych.

8.1.4. Kluczowe komponenty architektury Systemu, odpowiadające przyjętej przez Wykonawcę koncepcji realizacji jego funkcjonalności muszą zostać zaprezentowane w sposób zrozumiały dla Zamawiającego.

8.1.5. Wykonawca musi przygotować Diagram kooperacji, odzwierciedlający relacje pomiędzy mikroserwisami i zintegrowanymi systemami w podziale na systemy wewnętrzne i zewnętrzne.

8.1.6. Wykonawca musi rozbudować w oparciu o architekturę mikroserwisów, gdzie każdy z nich będzie osobnym kontenerem logicznym.

8.1.7. Zastosowanie rozwiązań architektury musi umożliwić uruchamianie rozbudowanego Systemu lub jego części w wielu niezależnych środowiskach w sposób niezależny od infrastruktury realizującej środowisko uruchomieniowe.

8.1.8. Zamawiający wymaga, aby rozwiązanie zostało zaprojektowane w taki sposób, aby umożliwić dalszą rozbudowę systemu PUE.

8.1.9. Interfejsy API budowanych serwisów muszą zostać udokumentowane w sposób umożliwiający łatwą integrację. Zamawiający wymaga, aby dokumentacja ta została wykonana za pomocą szeroko przyjętych oraz wspieranych standardów jak np. OpenAPI, AsyncAPI czy Swagger.

8.1.10. Zastosowanie architektury mikroserwisów oraz tworzeniu i dokumentacji interfejsów API za pomocą szeroko przyjętych standardów ma na celu ograniczenie złożoności Systemu i możliwość łatwej jego rozbudowy w przyszłości, a także integracja zewnętrznych systemów do systemu SMJI.

8.1.11. Mikroserwisy zbudowane na potrzeby rozbudowanego systemu PUE muszą zapewniać możliwość skalowania bez potrzeby zakupu dodatkowych licencji na system.

8.1.12. Zamawiający wymaga, aby integracja mikrousług za pomocą udokumentowanych interfejsów API pozwalała na łatwą wewnętrzną integrację pomiędzy mikroserwisami oraz na łatwą integrację zewnętrznych rozwiązań.

8.1.13. Zamawiający wymaga, aby rozbudowany system PUE posiadał budowę modułową.

9. Wymagania w zakresie analizy przedwdrożeniowej

9.1. Analiza Przedwdrożeniowa musi zostać przygotowana w języku polskim w sposób przejrzysty z jasnym podziałem na elementy wymagane w przedmiocie zamówienia.

9.2. W ramach analizy muszą być opisane w szczególności:

9.2.1. szczegółowy projekt modyfikacji architektury Rozbudowanego Systemu,

9.2.2. szczegółowy dobór technologii dla Rozbudowanego Systemu,

9.2.3. opis planowanych operacji przetwarzania danych osobowych w ramach Rozbudowanego Systemu,

9.2.4. ocenę ich niezbędności oraz proporcjonalności w stosunku do celów realizowanych przez Rozbudowany System,

9.2.5. ocenę ryzyka naruszenia praw lub wolności osób których dane dotyczą, a także środki planowane w celu zaradzenia temu ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych,

9.2.6. analizę ryzyka na potrzeby bezpieczeństwa teleinformatycznego Rozbudowanego Systemu według normy ISO/IEC 27005,

9.2.7. wykaz procesów biznesowych wraz z analizą przepływów pomiędzy systemami, wraz z ich uszczegółowieniem / dostosowaniem / zaprojektowaniem.

9.3. Analiza Przedwdrożeniowa musi zostać przygotowana w sposób przejrzysty z jasnym podziałem na elementy wymagane w przedmiocie zamówienia. W ramach analizy muszą być opisane w szczególności:

9.3.1. Projekt Rozbudowy Systemu zawierający:

a) Opis koncepcji rozbudowy Systemu;

b) Architekturę Rozbudowanego Systemu (architekturę fizyczną, logiczną, z podziałem na moduły funkcjonalne);

c) Opis sposobu integracji z infrastrukturą Zamawiającego;

d) Opis sposobu prezentacji danych/integracji z innymi systemami;

e) Szczegółowy plan wdrożenia rozbudowywanego Systemu;

- plan kolejności wdrożenia poszczególnych komponentów Rozbudowanego Systemu lub Rozbudowanej Części Systemu
- plan migracji
- plan testów
- plan odbiorów
- opis wraz z ilością planowanych do wykonania środowisk testowych
- szczegółowe uzgodnienia Stron Umowy dotyczące:
    - zakresu i sposobu migracji istniejących systemów informatycznych do Rozbudowanego Systemu

- zakresu i sposobu integracji systemów z Rozbudowanym Systemem
- sposobu organizacji i przeprowadzenia testów funkcjonalnych oprogramowania w ramach Rozbudowanego Systemu lub Rozbudowanej Części Systemu;
- szczegółowy zakres i sposób przeprowadzenia testów wydajnościowych na Rozbudowanym Systemie lub Rozbudowanej Części Systemu;

- opis istniejącej infrastruktury
- opis wszystkich istniejących komponentów systemu PUE
- opis istniejących interfejsów komunikacyjnych/integracji systemu PUE
- opis modelu danych systemu PUE
- procesy biznesowe realizowane przez system PUE
- zgodność Dokumentu analizy z wymaganiami dla dokumentacji wskazanymi w rozdziale 7: Wymagania w zakresie sposobu realizacji zamówienia oraz dokumentacji, w szczególności części: Dokumentacja Analityczna

f) Projekt techniczny Rozbudowanego Systemu lub Rozbudowy zawierający:

- Opis koncepcji Rozbudowy Systemu lub Rozbudowy Części Systemu;
- Architekturę Rozbudowanego Systemu lub Rozbudowanej Części Systemu (architekturę fizyczną, logiczną, z podziałem na moduły funkcjonalne);
- Opis sposobu realizacji wszystkich wymagań wynikających z OPZ poprzez umieszczenie szczegółowego opisu sposobu realizacji w stosunku do każdego wymagania (przedstawiony w formie tabelarycznej z uwzględnieniem numeracji wymagań), przy czym powielenie treści wymagania nie może być opisem sposobu jego realizacji
- Opis sposobu wykorzystania infrastruktury udostępnionej przez Zamawiającego celem budowy Rozbudowanego Systemu lub Rozbudowanej Części Systemu wraz z informacjami o planowanej rozbudowie infrastruktury lub braku potrzeby rozbudowy;
- Opis sposobu integracji z publicznymi rejestrami państwowymi np. Węzłem Krajowym, w tym metod zabezpieczających Rozbudowany System przed konsekwencjami zmian w tych rejestrach;
- mapowanie procesów biznesowych na Rozbudowany System lub Rozbudowaną Część Systemu;
- Szczegółowy harmonogram realizacji przedmiotu Umowy z zaznaczeniem kamieni milowych;
- opis ryzyk projektowych wraz z informacją o sposobie monitorowania i rejestrowania ryzyka, rodzajem działań jakie zostaną podjęte w przypadku wystąpienia ryzyka i określeniem budżetu ryzyka

9.3.2. Opis sposobu integracji Systemu z posiadanymi przez Zamawiającego systemami;

9.3.3. Harmonogram Wdrożenia, uszczegółowiający Harmonogram, o którym mowa w Rozdziale 5 z zaznaczeniem: kamieni milowych, listą produktów;

9.3.4. Plan komunikacji w projekcie;

9.3.5. Administracja;

9.3.6. Bezpieczeństwo;

9.3.7. Technologia w zakresie głównych komponentów;

9.3.8. Ryzyka projektowe wraz z informacją o sposobie monitorowania i rejestrowania ryzyka, rodzaju działań jakie zostaną podjęte w przypadku wystąpienia ryzyka i określenie budżetu ryzyka;

9.4. Dokument analizy musi być przygotowany zgodnie z wymaganiami dla dokumentacji, wskazanymi w rozdziale 10.

9.5. Wykonawca w ramach Analizy Przedwdrożeniowej ustali wraz z Zamawiającym w szczególności logiczny podział odpowiedzialności za niżej wymienione zadania wraz z odpowiednimi artefaktami w postaci polityk i procedur wytworzonym przez Wykonawcę w ramach dokumentacji powdrożeniowej:

9.5.1. Instalacja, konfiguracja aplikacji i wszystkich wymaganych usług na serwerach aplikacyjnych,

9.5.2. Administracja użytkownikami serwerów,

9.5.3. Monitorowanie dostępności i funkcjonalności serwerów aplikacyjnych, bazodanowych i infrastruktury,

9.5.4. Realizacja działań mających na celu minimalizację ryzyka oraz zapobieganie występowaniu awarii środowisk,

9.5.5. Realizacja działań mających na celu minimalizację ryzyk związanych z podatnościami bezpieczeństwa,

9.5.6. Analiza logów pod kątem pojawiających się błędów,

9.5.7. Analiza działających na serwerze aplikacji w celu zapewnienia jak najlepszych osiągów w dostępnych środowiskach,

9.5.8. Rozwiązywanie incydentów i problemów dot. serwerów aplikacyjnych w procesach zarządzania incydentami, problemami i usuwaniem awarii oraz wdrożeniami zmian infrastrukturalnych, projektowych i rozwojowych,

9.5.9. Zarządzanie wydajnością oraz pojemnością serwerów, np.: rozwiązaniem pozwalającym na planowanie i zarządzanie pojemnością w oparciu o skonsolidowane dane z systemu monitorowania infrastruktury informatycznej. Monitoring obejmuje zasoby sprzętowe, usługi, aplikacje,

9.5.10. Wykonywanie kopii systemowych, aplikacji i danych wraz z przywracaniem usług po awarii,

9.5.11. Aktualizacja komponentów w ramach zarządzania wydaniem.

9.6. Wykonawca będzie stosował iteracyjne, przyrostowe podejście do dostarczania wyników pracy realizowane poprzez pracę w kolejnych następujących po sobie etapach ustalonych z Zamawiającym. Każdy etap będzie zawierał plan na kolejną iterację z zadaniami, które zostaną zrealizowane jako niezbędne do dostarczania wyników pracy w danym etapie oraz opisami jakościowymi, jakie muszą spełniać dostarczane kolejno produkty (funkcjonalności, Przyrosty, dokumenty itp.) - definicja ukończenia. Każdy cykl będzie przedstawiał kolejne przyrosty produktu.

10. Wymagania w zakresie scenariuszy testowych i testów

10.1. Scenariusze testowe muszą być możliwe do wykorzystania w czasie utrzymania i rozwoju Rozbudowanego Systemu – do przeprowadzania testów regresyjnych (po wgraniu aktualizacji, nowych funkcjonalności i innych zmianach w Rozbudowanym Systemie).

10.2. Scenariusze testowe muszą być aktualizowane niezwłocznie po dokonaniu zmian w Rozbudowanym Systemie w ramach Usług Wsparcia i Usług Rozwoju.

10.2.1.

10.3. Zamawiający może przeprowadzić testy eksploracyjne i inne dodatkowe testy Rozbudowanego Systemu.

10.4. Wymagania szczegółowe do testów Rozbudowanego Systemu.

10.4.1. Testy integracyjne – przeprowadzane przez Wykonawcę

a) Muszą pokrywać wszystkie interfejsy wykorzystywane w komunikacji pomiędzy podsystemami/modułami/komponentami Rozbudowanego Systemu,

b) Muszą pokrywać wszystkie interfejsy wykorzystywane w komunikacji z systemami zewnętrznymi z którymi Rozbudowany System zostanie zintegrowany

c) Muszą być wykonywane dla każdej właściwej wersji oprogramowania przekazywanej przez Wykonawcę,

d) Wykonawca każdorazowo zobowiązany jest do przekazania Zamawiającemu raportu z testów integracyjnych;

e) Przekazany raport z testów modułowych musi potwierdzać zakończenie testów z wynikiem pozytywnym

10.4.2. Testy regresyjne - przeprowadzane przez Wykonawcę

a) Muszą być wykonane po każdej aktualizacji systemu wprowadzającej zmianę w Rozbudowanym Systemie,

b) Wykonawca każdorazowo zobowiązany jest do przekazania Zamawiającemu raportu z testów regresyjnych,

10.4.3. Testy akceptacyjne – przeprowadzane przez Zamawiającego w celu potwierdzenia prawidłowości działania Rozbudowanego Systemu z uwzględnieniem wszystkich wymagań funkcjonalnych i niefunkcjonalnych oraz przypadków użycia.

10.4.4. Testy bezpieczeństwa – przeprowadzane przez Wykonawcę w celu potwierdzenia prawidłowości działania Oprogramowania pod kątem bezpieczeństwa Rozbudowanego Systemu. Po zakończeniu testów bezpieczeństwa przed przekazaniem Rozbudowanego Systemu do odbioru, Wykonawca przekaże Zamawiającemu raport z testów bezpieczeństwa Rozbudowanego Systemu.

10.4.5. Zakres testów bezpieczeństwa:

a) Rozbudowany System musi być zgodny z wytycznymi zawartymi w metodyce OWASP Testing Guide w najnowszej stabilnej wersji oraz w dokumencie OWASP ASVS w najnowszej stabilnej wersji (Application Security Verification Standard).

b) Rozbudowany System musi być zgodny z wytycznymi zawartymi w standardzie PTES (Penetration Testing Execution Standard) w zakresie infrastruktury.

c) Rozbudowany System musi posiadać mechanizmy zabezpieczające przed typowymi zagrożeniami(nieaktywne konta, anomalie protokołów, anomalie ruchu, ataki typu: Dos, Ddos, backdoor, ataki związane z ładowaniem plików, Cross-site request forgery, Cross-site scripting, Cross-site tracking, Sql Injection, Php Injection, Session Hijacking, Session Fixation, Path traversal, kradzież cookies)

d) Zbieranie informacji o aplikacji (w trakcie testów muszą być sprawdzane m.in.:),
   i) badanie struktury aplikacji z użyciem narzędzi typu spider/crawler,
   ii) weryfikacja wpisów w pliku robots.txt,
   iii) wyszukiwanie informacji o aplikacji w wyszukiwarkach Internetowych,
   iv) identyfikacja punktów wejściowych do aplikacji,
   v) identyfikacja wersji aplikacji, serwera WWW i innych jej cech,
   vi) identyfikacja kodów błędów

e) Testy konfiguracji (w trakcie testów muszą być sprawdzane m.in.:),
   i) mechanizmy kryptograficzne stosowane w ramach aplikacji i infrastruktury (stosowanie protokołu SSL/TLS),
   ii) ustawienia dostępu do bazy danych,
   iii) obsługa plików o różnych rozszerzeniach,
   iv) istnienie na serwerze poprzednich wersji lub kopii zapasowych aplikacji,
   v) istnienie interfejsów do zarządzania oraz próby dostępu do nich,
   vi) typy obsługiwanych żądań http

f) Testy mechanizmów uwierzytelniających (w trakcie testów muszą być sprawdzane m.in.:),
   i) weryfikacja bezpieczeństwa przekazywania parametrów uwierzytelnienia,
   ii) testy możliwości enumeracji kont użytkowników aplikacji,
   iii) testy pod kątem występowania kont domyślnych,
   iv) próby ominięcia mechanizmów uwierzytelnienia,
   v) testy mechanizmów odzyskiwania hasła,
   vi) testy mechanizmów zapamiętywania hasła,
   vii) testy mechanizmów wylogowania,
   viii) weryfikacja mechanizmów pamięci podręcznej,
   ix) weryfikacja polityki haseł,
   x) weryfikacja podatności typu Direct Object Reference

g) Testy mechanizmów zarządzania sesją (w trakcie testów muszą być sprawdzane m.in.:),
   i) weryfikacja schematu zarządzania sesją,
   ii) obsługa parametrów sesji przez aplikację (pliki Cookies),
   iii) próby podszywania się pod zalogowanego Użytkownika,
   iv) próby wstrzykiwania innych parametrów sesji,
   v) odporność na ataki typu Session Fixation,
   vi) weryfikacja jawności parametrów sesji,
   vii) weryfikacja mechanizmów wygaszania sesji,
   viii) weryfikacja istnienia podatności typu CSRF (Cross Site Request Forgery)

h) Testy mechanizmów autoryzujących (w trakcie testów muszą być sprawdzane m.in.:),
   i) podatność na ataki typu PathTraversal i File Include,
   ii) odporność mechanizmów autoryzacji na próby ich obejścia,
   iii) możliwość eskalacji uprawnień do wyższego poziomu,
   iv) weryfikacja podatności typu Direct Object Reference

i) Testy logiki biznesowej (W trakcie testów muszą być sprawdzane m.in.:),
   i) weryfikację możliwości fałszowania zapytań,
   ii) analizę mechanizmów integralności,
   iii) weryfikację istnienia limitów,
   iv) próby ominięcia zakładanych ścieżek wykonania procesów,
   v) weryfikację obsługi różnych typów plików,
   vi) weryfikację możliwości przesłania do aplikacji złośliwego kodu

j) Testy walidacji danych i możliwości wstrzykiwania kodu (W trakcie testów muszą być sprawdzane m.in.:),
   i) weryfikację istnienia podatności Cross-Site Scripting (Reflected, Stored),
   ii) analizę podatności typu HTTP verb pollution/tampering,
   iii) analizę pod kątem istnienia podatności SQL Injection, w tym blind, time-delay, Boolean, database specific,
   iv) weryfikację pod kątem podatności typy OS command injection,
   v) weryfikację pod kątem podatność klasy serwer side injection,
   vi) analizę pod kątem istnienia podatności LDAP Injection,
   vii) analizę pod kątem istnienia podatności XML/XPATH Injection,
   viii) weryfikację pod kątem istnienia podatności typu local/remote file inclusion,

ix) analizę pod kątem istnienia błędów typu buffer overflow, heap overflow, format string

k) Testy mechanizmów obsługi błędów,

i) W trakcie testów muszą być sprawdzane komunikaty o błędach jakie zostaną wywołane przez wprowadzanie różnych wartości parametrów oraz tzw. stack traces

l) Testy po stronie klienta (przeglądarki),

i) weryfikacja podatności typu DOM based Cross Site Scripting,

ii) weryfikacja podatności typu HTML Injection,

iii) weryfikacja podatności typu Client Side URL Redirect,

iv) weryfikacja podatności typu Client Side Resource Manipulation,

v) analiza zastosowanej polityki Cross Origin Resource Sharing,

vi) weryfikacja podatności typu Clickjacking

m) Testy z wykorzystaniem Fuzzing-u,

n) Weryfikacja mechanizmów kryptograficznych pod kątem możliwości użycia słabych algorytmów,

i) weryfikację możliwości użycia słabych algorytmów kryptograficznych (szyfrów symetrycznych, asymetrycznych, funkcji skrótu),

ii) analizę pod kątem ujawniania poufnych informacji przez aplikację

10.4.6. Testy wydajnościowe – przeprowadzane przez Wykonawcę w celu potwierdzenia spełnienia wymagań wydajnościowych Rozbudowanego Systemu. Po zakończeniu testów wydajności przed przekazaniem Rozbudowanego Systemu do odbioru, Wykonawca przekaże Zamawiającemu raport z testów bezpieczeństwa Rozbudowanego Systemu.

a) Wykonawca wykona testy wydajnościowe Rozbudowanego Systemu dwa razy. Pierwszy test przed przekazaniem Rozbudowanego Systemu do odbioru. Drugi w terminie uzgodnionym z Zamawiającym w okresie pomiędzy Odbiorem Końcowym a końcem okresu Gwarancji.

b) Po zakończeniu testów wydajnościowych Wykonawca przekaże Zamawiającemu raport z testów wydajnościowych,

c) Testy wydajnościowe muszą obejmować co najmniej:

i) Realizacja testów obejmie wykonanie zaproponowanego i odpowiedniego rodzaju testu wydajnościowego przy pomocy dedykowanych skryptów testowych, opisanych w metodyce, odzwierciedlających konkretne scenariusze wykorzystania aplikacji przez Użytkownika lub żądania generowane w ramach integracji pomiędzy systemami.

ii) Skrypty służące do realizacji takiego testu muszą zostać stworzone przy pomocy dedykowanego narzędzia Open Source wspierającego testy wydajnościowe i polegają na nagraniu ruchu generowanego i odbieranego

przez aplikację, a następnie – odpowiednio sparametryzowane – uruchamiane będą wielokrotnie, symulując wykorzystywanie aplikacji przez zdefiniowaną liczbę Użytkowników.

iii) Wykonawca w swojej metodyce musi zaproponować i uzasadnić liczbę cykli wykonywania testu i iteracji, przy czym plan musi uwzględniać różne cele kolejnych cykli/iteracji – np.: weryfikacja wydajności Rozbudowanego Systemu po implementacji poprawek, weryfikacja wydajności Rozbudowanego Systemu po implementacji poszczególnych zmian, badanie wydajności Rozbudowanego Systemu przy zmieniającym się obciążeniu.

iv) Testy wydajnościowe muszą polegać na weryfikacji wydajności Rozbudowanego Systemu po stronie serwera/ów aplikacji i/lub bazy danych, Wykonawca do tych pomiarów musi użyć własnych dodatkowych narzędzi Open Source, które musi dostarczyć i zaimplementować w infrastrukturze Zamawiającego.

v) Wykonawca, poza wygenerowaniem obciążenia, musi na bieżąco przeprowadzać monitoring parametrów środowiska testowanego. Monitoring musi zostać prekonfigurowany wg planu przy pomocy dedykowanego do tego celu narzędzia i umożliwiać wskazanie zależności pomiędzy generowanym obciążeniem i ewentualnym obniżeniem wydajności poszczególnych komponentów środowiska, tak aby możliwe zidentyfikowanie „wąskich gardeł" Rozbudowanego Systemu.

d) Realizacja testów wydajnościowych obejmuje wykonanie następujących kroków:

i) Przygotowanie Planu Testów,

ii) Opracowanie Profilu Ruchu,

iii) Przygotowanie środowiska roboczego dla skryptów wydajnościowych,

iv) Generowanie danych wejściowych, wymaganych do realizacji testów wydajnościowych,

v) Projektowanie i implementacja automatów testowych,

vi) Zestawienie i konfiguracja monitoringu,

vii) Badanie możliwości środowiska (skalowanie Rozbudowanego Systemu),

viii) Wykonanie Testu (pomiary wydajności Rozbudowanego Systemu).

A) Proces testów rozpoczyna się w trakcie trwania procesu implementacji i nie powinien zaczynać się przed zakończeniem procesu projektowania Proces testów uwzględnia etapy dotyczące procesu implementacji, procesu wdrożenia i odbioru.

B) Zakres kolejnych iteracji testów musi być przyrostowy, tzn. w określonej iteracji testowane są wszystkie elementy przetestowane w poprzednich iteracjach oraz nowe, wytworzone w obecnej iteracji. Powtarzanie raz wykonanych testów (scenariuszy lub przypadków testowych) może być uzupełniane o nowe elementy (np. wynikające z rozwoju istniejących funkcjonalności), a więc testy cech systemu z poprzednich iteracji nie muszą być jedynie testami regresyjnymi.

C) Zamawiający wymaga, aby Wykonawca wdrożył praktykę programistyczną polegającą na ciągłej integracji (ang. Continuous Integration). Stworzony kod, który będzie umieszczany w repozytorium Zamawiającego (Atlassian BitBucket zintegrowany z Jira i Confluence), będzie przechodził automatyczne testy zgodności reguł składni danego języka programowania, które zostały opisane w rozdziale 13 Bezpieczeństwo kodu. Po pozytywnej weryfikacji reguł, stworzony kod trafi na serwer ciągłej integracji, np. Jenkins, a tam odbędą się następujące automatyczne czynności:

1. kompilacja kodu,
2. testy jednostkowe,
3. testy integracyjne,
4. budowa pakietu, który będzie gotowy do wgrania na środowisko testowe.

D) Stworzone środowisko testowe będzie okresowo przechodzić testy:

1. testy wydajnościowe w celu wykrycia tzw. wąskich gardeł i ewentualnych wycieków pamięci (np. Jmeter),
2. testy kompatybilności publicznych interfejsów dostępowych (np. SoapUI).

E) Repozytorium kodów źródłowych, serwery ciągłej integracji i serwery obsługujące rejestr stworzonych paczek zapewniają kontrolę uprawnień, zabezpieczenia przed nieuprawnionym dostępem, kontrolę wprowadzonych zmian i pełną rozliczalność.

F) W procesie testów Zamawiający wyróżnia następujące rodzaje testów, które zostaną zrealizowane przez Wykonawcę:

1. Testy wewnętrzne,
2. Testy jednostkowe,
3. Testy akceptacyjne,
4. Testy wydajnościowe.

G) W procesie testów Zamawiający wyróżnia następujące rodzaje testów, które zostaną zrealizowane przez podmiot zewnętrzny wskazany przez Zamawiającego przy współpracy Wykonawcy:

1. Testy penetracyjne.

H) W ramach prowadzonych testów, Zamawiający wymaga spełnienia następujących warunków:

1. Pozytywny wynik testów wewnętrznych jest warunkiem koniecznym do rozpoczęcia testów akceptacyjnych;
2. Pozytywny wynik testów akceptacyjnych jest warunkiem koniecznym do odbioru oprogramowania i wykonania wdrożenia masowego na środowisku produkcyjnym;
3. Testy akceptacyjne są prowadzone na jednej wersji oprogramowania tzn.:
   a. cała tura testów akceptacyjnych musi być przeprowadzona na jednej wersji oprogramowania;
   b. po rozpoczęciu testów akceptacyjnych dopuszcza się implementację, która polega na usunięciu błędów kosmetycznych.

I) Wykonawca zobowiązany jest do opracowania strategii testowania w postaci odrębnego dokumentu. Celem strategii testowania jest udokumentowanie decyzji dotyczących procesu testowania w danym przedsięwzięciu. Strategia testowania doprecyzowuje metodykę tam, gdzie metodyka nie przesądza konkretnych rozwiązań lub gdzie specyfika przedmiotu zamówienia wymaga odpowiednich ustaleń na etapie realizacji. Dokument musi powstać przed zaplanowaniem i wykonaniem testów, jednak później może podlegać uzgodnionym przez Wykonawcę i Zamawiającego aktualizacjom.

J) Strategia testowania jest pierwszym produktem procesu testowania.

K) Wykonawca zobowiązany jest do opracowania raportu z testów jako produktu wytworzonego w ramach testów i dokumentującego wykonane testy.

L) Raport z testów zawiera co najmniej:

1. Zakres testów odpowiadający zapisom Planu testów;
2. Wyniki testów;
3. Plan działań następczych związany z wynikami testów.

M) Jeżeli w trakcie testów wystąpiły błędy, Wykonawca zobowiązany jest do wprowadzenia poprawek i ponownej weryfikacji oprogramowania. Dodatkowo, wybierane są działania z planu testów, które powinny zostać powtórzone, mimo że wskazały na pozytywną weryfikację oprogramowania. Powtarzanie działań ma na celu zapewnienie, że wprowadzane w wyniku błędów poprawki nie powodują błędów w innych elementach oprogramowania. W przypadku wystąpienia jakiegokolwiek błędu podczas poprawianych testów, musi zostać podjęta udokumentowana decyzja co do dalszego postępowania.

11. Wymagania w zakresie sposobu realizacji zamówienia oraz dokumentacji

11.1. Zamawiający informuje, iż w celach realizacji projektu stosuje metodykę zarządzania projektami PRINCE2 z możliwością zastosowania metodyki AgilePM do wybranych jego elementów.

11.2. Zamawiający informuje, że w przypadku, gdy określił w SWZ wymagania z użyciem znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, to takie określenie należy traktować jako przykładowe. W każdym takim wskazaniu Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych, przy czym wykazanie równoważności jest po stronie Wykonawcy.

11.3. Zamówienie będzie realizowane w siedzibie Wykonawcy lub w miejscu przez niego wybranym oraz w siedzibie Zamawiającego. Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do realizacji poszczególnych elementów Umowy w siedzibie Zamawiającego.

11.4. Wykonawca zobowiązuje się do przestrzegania wewnętrznych procedur oraz regulaminów obowiązujących osoby przebywające w siedzibie Zamawiającego.

11.5. Zamawiający ma prawo do rejestrowania spotkań Zamawiającego z Wykonawcą (w formie nagrania cyfrowego).

11.6. Z każdego spotkania Wykonawca sporządzi notatkę na bieżąco i uzgodni jej treść z uczestnikami spotkania ze strony Zamawiającego przed zakończeniem spotkania. Uzgodnienia zawarte w notatce będą obowiązujące po akceptacji przez Zamawiającego.

11.7. Wykonawca będzie zamieszczał notatki w repozytorium prowadzonym i udostępnionym dla personelu Wykonawcy przez Zamawiającego pod adresem https://confluence.uke.gov.pl

11.8. W odniesieniu do schematu nazewnictwa dokumentów nazwy wszystkich dokumentów przechowywanych w Repozytorium podlegają następującej konwencji:

PUE2-NazwaDokumentu-RRMMDDx

gdzie:

PUE2 to oznaczenie projektu – na wypadek, gdyby plik/dokument miał być użyty także w innym kontekście,

x- oznacza numer kolejnej wersji dokumentu z tego samego dnia.

11.9. Dokumentacja musi być pogrupowana tematycznie i zawierać spis i charakterystykę wszystkich składników dokumentacji oraz musi być dostarczona:

11.9.1. w postaci papierowej, w formie spiętych, zszytych lub bindowanych egzemplarzy,

11.9.2. w postaci elektronicznej – w formie plików PDF, plików pakietu MS Office oraz w odpowiednich notacjach – UML 2.1 lub BPMN 2.0.

11.10. W przypadku odniesień do zewnętrznej dokumentacji, zewnętrzna dokumentacja musi zostać dołączona lub zostać precyzyjnie wskazana, a odwołanie musi wskazać na konkretną stronę/fragment dokumentacji zewnętrznej.

11.11. Dokumentacja wytworzona w ramach przedmiotu zamówienia musi zostać opatrzona, co najmniej w stopce lub nagłówku pierwszej strony (jeżeli podsiada załączniki również na pierwszych stronach załączników):

11.11.1. obowiązującymi logotypami Programu Operacyjnego Polska Cyfrowa, Unii Europejskiej wraz z wyrażeniem UNIA EUROPEJSKA Europejski Fundusz Rozwoju Regionalnego oraz logotypem Urzędu Komunikacji Elektronicznej,

11.11.2. informacją o współfinansowaniu produktu przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu państwa w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020.

11.12. Wzór przykładowej dokumentacji projektu, opatrzonej wymaganymi logotypami znajduje się w Załączniku nr 4 do OPZ.

11.13. W przypadku dokonania zmian w Rozbudowanym Systemie Dokumentacja Użytkownika zostanie zaktualizowana przez Wykonawcę w zakresie opisu dokonanych zmian.

11.14. Zaktualizowana Dokumentacja musi być przekazywana do odbioru wraz z modyfikacją wprowadzaną w Rozbudowanym Systemie (wynikającą z prac wykonanych w ramach Gwarancji, Usług Wsparcia oraz Usług Rozwoju).

11.15. Po każdej aktualizacji Rozbudowanego Systemu nowa wersja Dokumentacji musi być wgrana do repozytorium administrowanego przez Zamawiającego.

Wymagania ogólne do dokumentacji:

11.16. Każdy dokument musi być sporządzony w języku polskim,

11.17. Każdy dokument musi zawierać metrykę informującą o:

11.17.1. Osobie odpowiedzialnej za przygotowanie dokumentu ze strony Wykonawcy,

11.17.2. Autorach dokumentu,

11.17.3. Numerze wersji dokumentu,

11.17.4. Wersji podsystemu/modułu/komponentu Rozbudowanego Systemu,

11.17.5. Dacie wytworzenia wersji dokumentu,

11.17.6. Historii zmian. Opis każdej zmiany dokumentu musi uwzględniać:

a) Opis zmiany wraz ze wskazaniem części dokumentu, których dotyczy zmiana,

b) Datę zmiany,

c) Autora zmiany,

11.18. Każdy dokument musi zawierać słownik pojęć i skrótów użytych w dokumencie. Pojęcia i skróty muszą być posortowane w kolejności alfabetycznej.

11.19. Każdy dokument musi posiadać strukturę i być podzielony na ponumerowane rozdziały, podrozdziały.

11.20. Struktura dokumentu musi zostać zaprezentowana w spisie treści dokumentu.

11.21. Każdy dokument musi być logicznie spójny z pozostałymi dokumentami wytwarzanymi przez Wykonawcę w ramach projektu.

11.22. Wszystkie dokumenty wytwarzane przez Wykonawcę w ramach zamówienia muszą zostać przekazane Zamawiającemu w formatach:

11.22.1. Plik Microsoft Word 2013 lub wyższej, w wersji edytowalnej oraz plik PDF,

11.22.2. Na żądanie Zamawiającego Wykonawca dostarczy dokument w postaci drukowanej (wydruk kolorowy).

11.23. Wykonawca zobowiązany jest do prowadzenia, aktualizacji i zarządzania repozytorium dokumentacji. Repozytorium zostanie zrealizowane w oparciu o narzędzie JIRA Confluence pod adresem https://confluence.uke.gov.pl eksploatowane przez Zamawiającego lub inne uzgodnione z Zamawiającym.

11.24. Wszystkie artefakty będą modelowane w odpowiednich notacjach – UML 2.1 lub BPMN 2.0.

W ramach przedmiotu Umowy Wykonawca wytworzy następującą dokumentację:

Dokumentacja Użytkownika

11.25. Dokumentacja Użytkownika musi zawierać szczegółowy opis wszelkich funkcjonalności i właściwości dostarczonego Rozbudowanego Systemu, pozwalający na poprawną konfigurację i eksploatację Rozbudowanego Systemu, zgodnie z jego przeznaczeniem.

11.26. Dokumentacja Użytkownika musi składać się z wymienionych poniżej elementów i uwzględniać przypisane do nich wymagania:

11.26.1. Pomoc kontekstowa – Rozbudowany System musi zostać wyposażony w system pomocy kontekstowej.

a) Wykonawca opracuje i przedstawi projekt pomocy kontekstowej dla komponentów Rozbudowanego Systemu

b) Projekt pomocy kontekstowej musi uwzględniać wszystkie ekrany, na których pomoc kontekstowa ma być dostępna;

11.26.2. Instrukcja Użytkownika musi uwzględniać poniższe wymagania:

a) Wykonawca powinien przedstawić opis wykonania wszystkich czynności dostępnych dla Użytkownika (Zewnętrznego i Wewnętrznego) wynikających z realizacji przypadków użycia, który musi składać się co najmniej z określenia:

i) Sposobu konfiguracji aplikacji,

ii) Celu czynności wykonywanych przez Użytkownika,

iii) Możliwych scenariuszy realizacji,

iv) Poszczególnych kroków,

v) Zestawienia komunikatów o błędach,

b) Instrukcja Użytkownika - Wykonawca musi opracować instrukcję Użytkownika, która szczegółowo opisze kolejne kroki wymagane do pełnej realizacji obowiązku sprawozdawczego w Rozbudowanym Systemie.

i) Instrukcja użytkownika musi zawierać ilustracje w postaci zrzutów ekranu i sekwencji wideo.

ii) Instrukcja użytkownika musi zostać opracowana dla wszystkich dostępnych w Rozbudowanym Systemie ścieżek wprowadzania danych: poprzez uzupełnianie i edycję danych w profilu Użytkownika/Podmiotu, poprzez uzupełnianie i wysyłanie wniosków, poprzez tworzenie formularzy i nowych usług, poprzez zarządzanie profilem podmiotu oraz umów operatorskich.

Dokumentacja Techniczna

11.27. W Dokumentacji Technicznej muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną, z punktu widzenia technicznego, eksploatację Rozbudowanego Systemu.

11.28. Dokumentacja Techniczna musi uwzględniać:

11.28.1. Projekty infrastruktury wymaganej do uruchomienia wszystkich podsystemów, modułów, komponentów Rozbudowanego Systemu,

11.28.2. Projekty infrastruktury wymaganej do uruchomienia podsystemów wspierających usługi związane z jej wdrożeniem i eksploatacją,

11.28.3. Relacje pomiędzy elementami Architektury oraz wymaganiami architektonicznymi wraz z usługami związanymi z jej eksploatacją,

11.28.4. Specyfikację oprogramowania standardowego, które zostanie wykorzystane do implementacji i eksploatacji Rozbudowanego Systemu,

11.28.5. Wykaz bibliotek standardowych z określeniem ich wersji potrzebnych do uruchomienia Rozbudowanego Systemu

11.28.6. Opis narzędzi do monitorowania operacyjnego platformy techniczno-systemowej Rozbudowanego Systemu,

11.28.7. Opis narzędzi do monitorowania dostępności i wydajności Rozbudowanego Systemu,

11.28.8. Opis narzędzi do kolekcjonowania danych o zdarzeniach generowanych przez infrastrukturę i podsystemy Rozbudowanego Systemu,

11.28.9. Opis narzędzi do tworzenia i odtwarzania kopii zapasowych,

11.28.10. Przygotowaną przez Wykonawcę politykę tworzenia i odtwarzania kopii zapasowych,

11.28.11. Specyfikację zasobów infrastruktury (sprzęt i licencje) wymaganych do implementacji Rozbudowanego Systemu w podziale na Środowiska z uwzględnieniem konfiguracji:

a) Warstwy wirtualizacji i systemów operacyjnych,

b) Pamięci masowej,

c) Sieci LAN,

11.28.12. Specyfikację warstw Rozbudowanego Systemu z uwzględnieniem:

a) Warstwy bazodanowej

i) Opis konfiguracji zastosowanego w rozwiązaniu silnika baz danych

ii) Opis konfiguracji klastra baz danych

iii) Zestawienia parametrów konfiguracyjnych

b) Warstwy Front-end

i) Opis konfiguracji zastosowanych w rozwiązaniu serwerów Web

ii) Opis konfiguracji klastra serwerów Web

iii) Zestawienia parametrów konfiguracyjnych warstwy Front-end

c) Warstwy Back-end

i) Opis konfiguracji zastosowanego w rozwiązaniu serwerów aplikacji

ii) Opis konfiguracji klastra serwerów aplikacji

iii) Zestawienia parametrów konfiguracyjnych warstwy Back-end

W projekcie Wykonawca uwzględni projekty innych podsystemów/komponentów, które zostaną użyte w rozwiązaniu.

Dokumentacja Administratora Rozbudowanego Systemu

11.29. Dokumentacja Administratora Rozbudowanego Systemu musi zawierać zestaw dokumentacji szczegółowo opisujących zastosowane rozwiązania zapewniające spełnienie wymagań ogólnych (zgodnie z wymaganiami prawa) oraz specyficznych zamawiającego dotyczących bezpiecznej eksploatacji. Dokumentacja, w szczególności, musi zawierać:

11.29.1. Opis zastosowanych mechanizmów logowania zdarzeń, śladu audytowego oraz kontroli i monitorowania działań w aplikacji/systemie w tym wszelkich prób naruszenia zasad bezpieczeństwa;

11.29.2. Opis funkcjonalności, interfejs oraz zasady zarządzania kontami (Użytkownikami) oraz uprawnieniami poszczególnych ról, profili, Użytkowników itp.;

11.29.3. Opis sposobu realizacji wymagań wynikających z obowiązujących przepisów o ochronie danych osobowych;

11.29.4. Opis zabezpieczeń interfejsów oraz opis metod zapewnienia poufności i kontrolowalności tych kanałów przepływu informacji, jeśli aplikacja wykorzystuje jakiekolwiek mechanizmy wymiany informacji z innymi systemami;

11.29.5. Opisy instalacji, konfiguracji i parametryzacji oprogramowania zastosowanego przy budowie Rozbudowanego Systemu (stos technologiczny) z uwzględnieniem:

a) Zestawienia wersji zastosowanego oprogramowania, w tym oprogramowania systemowego, narzędziowego i aplikacyjnego,

b) Zestawienia parametrów systemu operacyjnego i oprogramowania narzędziowego, które są modyfikowane pod względem wartości domyślnych;

11.29.6. Opisy instalacji, konfiguracji i parametryzacji oprogramowania aplikacyjnego Rozbudowanego Systemu (stos technologiczny) z uwzględnieniem:

a) Zestawienia parametrów oprogramowania aplikacyjnego z podaniem:

i) Definicji i opisu parametru i jego znaczenia,

ii) Wartości parametru (w tym minimalnej i maksymalnej wartości parametru),

iii) Zestawienia i opisu plików konfiguracyjnych zawierających standardową konfigurację po uruchomieniu;

b) Dokumentacja musi zawierać opis działań, które muszą zostać zrealizowane przy wystąpieniu komunikatu;

11.29.7. Dokumentacja Administratora Rozbudowanego Systemu musi zawierać komplet procedur administracyjnych uwzględniających:

a) Pełną instalację Rozbudowanego Systemu,

b) Uruchomienie i zatrzymanie komponentów Rozbudowanego Systemu,

c) Opis metod zmian parametrów komponentów Rozbudowanego Systemu,

d) Kontrolę poprawności działania Rozbudowanego Systemu względem przyjętych parametrów wydajnościowych i jakościowych,

e) Zarządzanie uprawnieniami,

f) Wykonanie i odtworzenie kopii zapasowej,

g) Analizę działań Użytkowników w Rozbudowanym Systemie,

h) Postępowanie i naprawę Rozbudowanego Systemu w przypadku awarii;

11.29.8. Każda z procedur w Dokumentacji Administratora Rozbudowanego Systemu musi zawierać co najmniej następujące informacje:

a) Identyfikator procedury,

b) Nazwa procedury,

c) Wersja procedury,

d) Data początku obowiązywania procedury,

e) Cel realizacji procedury,

f) Warunki uruchomienia procedury,

g) Warunki zakończenia realizacji procedury – opis efektu końcowego realizacji procedury,

h) Odpowiedzialność - określenie osób/ról ponoszących odpowiedzialność za stosowanie procedury,

i) Wykaz dokumentów związanych - wykaz dokumentów związanych, w tym dokumentów opisujących procedury zależne,

j) Wykaz aplikacji wspomagających wykonywanie procedur (np. system monitorowania),

k) Tryb postępowania - opis kolejnych kroków procedury.

Dokumentacja Testowa

11.30. Wykonawca musi opracować i przedstawić do akceptacji Zamawiającego:

11.30.1. Plany testów dla każdego z typów realizowanych testów:

a) Testy integracyjne,

b) Testy regresji,

c) Testy akceptacyjne,

d) Testy bezpieczeństwa,

e) Testy wydajności,

11.30.2. Scenariusze testowe dla wszystkich typów testów,

11.30.3. Zestawienie przypadków testowych,

11.30.4. Dane testowe dla poszczególnych przypadków;

11.31. Plan Testów przygotowany przez Wykonawcę musi zawierać co najmniej następujące informacje:

11.31.1. Słownik pojęć,

11.31.2. Wprowadzenie i cel testów,

11.31.3. Przedmiot i zakres testów,

11.31.4. Zestawienie scenariuszy testowych wraz z pokryciem wymagań przez poszczególne scenariusze,

11.31.5. Zestawienie przypadków testowych dla poszczególnych scenariuszy wraz z opisem pól,

11.31.6. Kryteria rozpoczęcia testów,

11.31.7. Kryteria zakończenia testów,

11.31.8. Zasady raportowania i cykl życia scenariuszy testowych,

11.31.9. Lista narzędzi testowych,

11.31.10. Zdefiniowanie ograniczeń (np. dostępność zasobów wymaganych do przeprowadzenia testów, ograniczenia wynikające z harmonogramu),

11.31.11. Kategorie incydentów,

11.31.12. Harmonogram testów,

11.31.13. Opis środowiska testowego,

11.31.14. Opis struktury Zespołu testowego,

11.31.15. Opis zakresu danych testowych, dostarczanych przez Wykonawcę dla poszczególnych scenariuszy testowych;

11.32. Scenariusze testowe muszą zawierać co najmniej następujące informacje:

11.32.1. Konstrukcja scenariuszy testowych musi zapewniać możliwość ich wykonania przez osoby wskazane przez Zamawiającego (osoby niebędące członkami Zespołu Wykonawcy), posiadające kwalifikacje w zakresie testowania aplikacji.

11.32.2. Konstrukcja scenariuszy testowych musi zapewniać możliwość zweryfikowania pokrycia wymagań i przypadków użycia. W szczególności musi być możliwe zidentyfikowanie:

a) Wymagań (funkcjonalnych i niefunkcjonalnych) weryfikowanych przez scenariusz testowy,

b) Przypadków użycia weryfikowanych przez scenariusz testowy;

11.32.3. Dokument scenariusza testowego musi uwzględniać:

a) Identyfikator scenariusza,

b) Warunki wejściowe – lista warunków, jakie muszą być spełnione, aby można było rozpocząć wykonanie scenariusza testowego,

c) Określenie zakresu danych testowych,

d) Listę przypadków testowych wchodzących w skład scenariusza testowego;

11.32.4. Dokument przypadku testowego musi uwzględniać:

a) Uporządkowany i jednoznaczny zestaw kroków wykonywanych przez testera,

b) Opis oczekiwanego wyniku po wykonaniu poszczególnych kroków,

c) Dodatkowe weryfikacje, które muszą zostać wykonane po zrealizowaniu danego scenariusza (np. czy dokonał się właściwy zapis w logu aplikacji);

Dokumentacja Analityczna

11.33. Wykonawca musi przedstawić dokumentację analityczną będącą elementem Analizy Przedwdrożeniowej i przedstawić ją do Odbioru wraz z Analizą Przedwdrożeniową.

11.34. Dokumentacja analityczna obejmuje wszystkie wymagania i przypadki użycia.

11.35. Wykonawca musi utrzymywać i aktualizować repozytorium wymagań i przypadków użycia.

11.35.1. Repozytorium musi być prowadzone w narzędziu zaproponowanym przez Wykonawcę i uzgodnionym z Zamawiającym. Zamawiający ma prawo wskazać Wykonawcy narzędzie do prowadzenia repozytorium.

11.35.2. Wszystkie artefakty muszą być modelowane w odpowiednich notacjach – UML 2.1, BPMN 2.0.

11.35.3. Wykonawca musi zapewnić Zamawiającemu dostęp do repozytorium przez cały okres trwania Umowy.

11.35.4. W repozytorium muszą być utrzymywane co najmniej następujące typy wymagań:

a) Szczegółowe wymagania funkcjonalne,

b) Szczegółowe wymagania niefunkcjonalne,

c) Szczegółowe wymagania bezpieczeństwa,

d) Szczegółowe wymagania wydajnościowe.

11.35.5. Wykonawca musi zapewnić, że wymagania i przypadki użycia są niesprzeczne i spójne logicznie.

11.35.6. W przypadku prowadzenia repozytorium analitycznego we własnym narzędziu Wykonawca po zakończeniu projektu musi przekazać repozytorium Zamawiającemu. Repozytorium musi być aktualne na moment zakończenia projektu.

11.36. Dokumentacja przypadków użycia:

11.36.1. Dokument przypadku musi zawierać co najmniej:

a) Identyfikator przypadku użycia, jednoznacznie identyfikujący wymaganie (identyfikator nie może być zmieniony),

b) Nazwa przypadku użycia,

c) Opis przypadku użycia – kompletny opis definiujący cel przypadku użycia,

d) Wersja – numer kolejnej wersji przypadku użycia,

e) Autor przypadku użycia,

f) Data utworzenia przypadku użycia,

g) Scenariusze przypadku użycia,

h) Warunki wejściowe,

i) Warunki wyjściowe,

j) Status przypadku użycia – minimalny zestaw statusów:

i) Zgłoszony – przypadek użycia, który został zgłoszony i jest w trakcie analizy,

ii) Zatwierdzony – przypadek użycia, dla którego zakończono analizę i został zatwierdzony do realizacji,

iii) Odrzucony – przypadek użycia, który został odrzucony po etapie analizy,

k) Źródło – źródło pochodzenia przypadku użycia (np. dokładne określenie terminu spotkania, na którym zgłoszono przypadek użycia)

11.36.2. Wszystkie przypadki użycia muszą zostać opisane przy użyciu scenariusza podstawowego (scenariusz oczekiwany) oraz co najmniej jednego scenariusza alternatywnego. Liczba scenariuszy alternatywnych uzależniona jest od ilości możliwych przebiegów danego przypadku użycia,

11.36.3. Wszystkie scenariusze przypadków użycia muszą:

a) Posiadać ponumerowane kroki,

b) Zawierać opisy interakcji aktora z Rozbudowanym Systemem, która odbywa się wyłącznie w ramach jednego, opisywanego przypadku użycia oraz składać się z na przemian występujących po sobie działań realizowanych przez aktora i Rozbudowany System,

c) Być przyporządkowane do odpowiedniego warunku wyjścia określonego dla tego przypadku użycia,

11.36.4. Nie jest dopuszczalne by scenariusze alternatywne posiadały takie same treści jak scenariusz podstawowy. Scenariusz alternatywny musi wskazywać na kroki, które w danym scenariuszu realizowane są inaczej niż w scenariuszu podstawowym. Dla scenariuszy, które posiadają więcej niż 10 kroków zostanie przygotowany diagram aktywności,

11.36.5. Wszystkie przypadki użycia muszą zostać:

a) Powiązane z właściwymi wymaganiami, które realizują (pokrycie wymagań przez przypadki użycia),

b) Pogrupowane i skorelowane z obszarami funkcjonalnymi, których dotyczą,

c) Przekazane Zamawiającemu po wcześniejszym zweryfikowaniu przez Wykonawcę pod względem niesprzeczności oraz poprawności logicznej,

d) Przedstawione w formie diagramu:

i) Diagram musi być zaprezentowany graficznie (diagram przypadków użycia),

ii) Diagram musi uwzględniać co najmniej jednego aktora,

iii) Diagram musi prezentować wszystkie elementy powiązane, punkty rozszerzeń,

11.36.6. Wykonawca musi zapewnić, że zdefiniowany zbiór przypadków użycia będzie kompletny i będzie opisywał cały Rozbudowany System.

11.36.7. Zarządzanie zmianą przypadków użycia - każda zmiana wymagania musi obejmować:

a) Zmianę numeru wersji przypadku użycia,

b) Datę zgłoszenia i zatwierdzenia zmiany przypadku użycia,

c) Opis zmiany,

d) Autora zmiany.

Kody źródłowe

11.37. Wykonawca musi wgrywać do prywatnego repozytorium, które będzie w posiadaniu Zamawiającego, całą dokumentację łącznie z kodami źródłowymi komponentów Rozbudowanego Systemu każdorazowo przed instalacją w dowolnym środowisku (produkcyjnym/testowym/innym) nowej wersji Rozbudowanego Systemu, jego hot-fix'a lub rozszerzenia. Repozytorium musi zawierać kody źródłowe wszystkich komponentów programowych Rozbudowanego Systemu, w tym: procedury, pliki konfiguracyjne, skrypty itd., wszystkie aktualizacje i poprawki, a także wdrożenia w ramach rozwoju wprowadzane w toku trwania umowy muszą mieć odzwierciedlenie we wspomnianym repozytorium, muszą być udokumentowane i muszą posiadać odpowiednie komentarze. Repozytorium będzie stanowiło źródło programów, skryptów, kodów, etc. niezbędnych w procesach instalacji lub modyfikacji/rozszerzenia Rozbudowanego Systemu, które będą wykorzystywane przez narzędzia automatyzujące te procesy.

11.38. Wykonawca musi przekazać Zamawiającemu:

11.38.1. W zakresie kodu aplikacji:

a) aktualny kod aplikacji i jego skompilowane wersje w podziale na poszczególne komponenty Rozbudowanego Systemu, który umożliwiał będzie jego kompilację, o ile kod będzie kompilowany,

b) aktualną dokumentację dla kodu źródłowego zawierającej minimum:

i) listę wszystkich klas i funkcji wraz z opisem parametrów wejściowych i wyjściowych (w tym pełne API),

ii) listę bibliotek i kontrolek, wraz z ich wersjami, gdzie pod pojęciem kontrolek Zamawiający rozumie zestaw kodu w językach HTML, JavaScript i CSS odpowiedzialny za wygląd i funkcjonalność graficznego elementu sterowania (np. pole formularza, przycisk), możliwy do wielokrotnego zastosowania w różnych częściach Rozbudowanego Systemu,

iii) przepływ danych pomiędzy poszczególnymi komponentami Rozbudowanego Systemu (w postaci diagramów) w tym szczegółowy wykaz operacji komunikacji z bazami danych,

iv) instrukcje kompilowania kodów źródłowych (o ile będą kompilowane) oraz instrukcje instalacje wytworzonych komponentów w środowisku oprogramowania standardowego,

v) opis parametrów konfiguracyjnych komponentów Rozbudowanego Systemu.

11.38.2. W zakresie baz danych:

a) aktualne skrypty umożliwiające utworzenie baz danych, tabel, widoków, synonimów, procedur składowanych i funkcji,

b) aktualną dokumentację do baz danych, tabel, widoków, synonimów, procedur składowanych i funkcji,

c) dokumentacja musi zawierać minimum takie informacje jak: nazwy danych, typy, wartości domyślne, opis kluczy głównych i kluczy zewnętrznych, indexy, w przypadku procedur i funkcji wartości wejściowe i wyjściowe,

11.39. Zamawiający wymaga by kod źródłowy Rozbudowanego Systemu spełniał wyspecyfikowane niżej minimalne kryteria. Definicje poszczególnych metryk zostały zdefiniowane i są dostępne pod adresem: https://docs.sonarqube.org/latest/user-guide/metric-definitions/

11.39.1. Reliability – A

11.39.2. Security – A

11.39.3. Maintainability – A

11.39.4. Duplications - 1%

11.39.5. Weryfikacja spełnienia wymagania zostanie zrealizowana w oparciu o ostatnią dostępną wersję (na dzień przekazania do Odbioru Rozbudowy Systemu) oprogramowania SonarQube dostępnego pod adresem: https://www.sonarsource.com/products/sonarqube/downloads/

11.40. Kod źródłowy Rozbudowanego Systemu musi posiadać zdefiniowaną konwencję (ang. style guide) określającą:

11.40.1. Sposób formatowania kodu, zasady nazewnictwa zmiennych, klas, metod,

11.40.2. Zasady komentowania kodu. Zamawiający wymaga, aby komentarze zawierały krótkie opisy działania poszczególnych klas i metod, definicje użytych zmiennych,

11.40.3. Zasady i konwencje opisu zdarzeń generowanych w Rozbudowanym Systemie (w szczególności opisy błędów),

11.40.4. Wykonawca przygotuje dokument opisujący konwencję dla języków programowania wykorzystywanych w Rozbudowanym Systemie i przedstawi ją do akceptacji Zamawiającemu,

11.40.5. Kod źródłowy Rozbudowanego Systemu musi zostać napisany w języku programowania w takiej wersji, dla której w dającej się przewidzieć przyszłości będzie zapewnione wsparcie i poprawki bezpieczeństwa,

11.40.6. W razie konieczności przepisania kodu Istniejącego systemu Wykonawca zrealizuje prace związane z przepisaniem kodu Istniejącego systemu w ramach wynagrodzenia za realizację umowy.

11.40.7. Wykonawca musi przygotować zbiór gotowych elementów HTML/CSS, skryptów JS, które umożliwią utworzenie responsywnej strony internetowej, zgodny z BOOTSTRAP w wersji co najmniej 5.3. Wykonawca opracuje i wdroży repozytorium utworzonych klas służących wizualizacji interfejsów użytkownika (HTML, CSS, JS, Sass). Zamawiający pod pojęciem repozytorium elementów HTML/CSS rozumie serwer CDN - Content Delivery Network.

11.41. Zamawiający wymaga, by kod źródłowy Rozbudowanego Systemu był zarządzany zgodnie z wzorcem ciągłej integracji (continuous integration). Dlatego Wykonawca musi skonfigurować i utrzymywać w czasie trwania Umowy środowiska ciągłej integracji (continuous integration) z wykorzystaniem posiadanego przez Zamawiającego oprogramowania Jenkins i Bitbucket, które będzie uwzględniało następujący zestaw narzędzi:

11.41.1. Repozytorium kodu,

11.41.2. Automatyczne budowanie oprogramowania Rozbudowanego Systemu,

11.41.3. Testy statyczne kodu źródłowego oraz weryfikację zgodności formatowania kodu względem przyjętej konwencji formatowania kodu,

11.41.4. Testy automatyczne,

11.41.5. Repozytorium oprogramowania na potrzeby składowania binariów poszczególnych wersji Rozbudowanego Systemu oraz wykorzystywanych bibliotek.

11.42. Na podstawie Dokumentacji Technicznej Wykonawca musi przygotować i wdrożyć procedury do:

11.42.1. Automatycznego budowania poszczególnych wersji Rozbudowanego Systemu,

11.42.2. Automatycznego uruchamiania testów jednostkowych i funkcjonalnych.

11.43. W celu przeprowadzenia procedury odbioru kodów źródłowych Wykonawca przy współudziale Zamawiającego musi dokonać kompilacji, jeśli kod lub jego elementy wymagają kompilacji, przekazanego kodu źródłowego zgodnie z przekazaną Zamawiającemu instrukcją, a następnie dokonać instalacji wytworzonych komponentów w środowisku testowym Rozbudowanego Systemu również zgodnie z przekazaną instrukcją.

11.44. Kod źródłowy użytych komponentów Open Source nie może podlegać zmianom. Modyfikacji mogą podlegać jedynie:

11.44.1. błędnie działające fragmenty kodu, przy czym błąd musi zostać zgłoszony autorom komponentu wraz z poprawionym przez Wykonawcę fragmentem kodu. Potwierdzenie zgłoszenia błędu w oprogramowaniu Open Source musi także zostać przekazane Zamawiającemu.

11.44.2. inne fragmenty, kodu w przypadku uzasadnionej potrzeby i za zgodą Zamawiającego.

11.45. Wszelkie zmiany w funkcjonalności komponentów Open Source muszą być realizowane w formie modułów, rozszerzeń lub wtyczek.

12. Infrastruktura sprzętowa i oprogramowanie udostępniane przez Zamawiającego

12.1. Zamawiający udostępni na potrzeby realizacji umowy następujące nowe zasoby:

12.1.1. Wymaganą przestrzeń dyskową (10TB na potrzeby środowiska produkcyjnego i testowego) udostępnioną z zasobów macierzy NetApp AFF-A400

12.1.2. Obecne zasoby przydzielone do systemu PUE zostaną wykorzystywane w ramach Rozbudowanego Systemu (Procesory wirtualne – 84 rdzenie, Pamięć RAM 288 GB)

12.2. Zamawiający będzie udostępniał Wykonawcy zasoby stopniowo, na podstawie zgłoszonego zapotrzebowania i postępów w realizacji Umowy.

12.3. Wykonawca w porozumieniu z Zamawiającym musi przygotować maszyny wirtualne z zainstalowanym systemem operacyjnym Linux Debian w wersji uzgodnionej z Zamawiającym. Wersja systemu operacyjnego musi mieć status stabilnej i jednocześnie mieć zapewnioną dostępność aktualizacji bezpieczeństwa przez czas trwania Umowy.

12.4. Wykonawca w porozumieniu z Zamawiającym musi przygotować maszyny wirtualne z zainstalowanym systemem operacyjnym min. Windows Server 2019 Datacenter.

12.5. Zamawiający nie dopuszcza stosowania dodatkowych warstw wirtualizacji.

12.6. W ramach projektu zostaną uruchomione następujące środowiska:

12.6.1. Środowisko developerskie (DEV) - środowisko przeznaczone do wytworzenia oprogramowania dedykowanego Rozbudowanego Systemu,

a) Zapewnienie środowisk developerskich leży po stronie Wykonawcy. Wykonawca musi uruchomić środowiska developerskie na własnej infrastrukturze.

12.6.2. Środowisko testowe (TEST) - środowisko przeznaczone do testów akceptacyjnych, eksploracyjnych, bezpieczeństwa i wydajnościowych,

a) Środowisko testowe musi być zbudowane na infrastrukturze Zamawiającego przez Wykonawcę,

b) Instalacja i konfiguracja komponentów środowiska oraz oprogramowania standardowego i dedykowanego leży po stronie Wykonawcy przy wsparciu Zamawiającego,

12.6.3. Środowisko produkcyjne (PROD) - środowisko przeznaczone do produkcyjnego uruchomienia Rozbudowanego Systemu

a) Środowisko produkcyjne musi być zbudowane na infrastrukturze Zamawiającego w oparciu o projekt techniczny przygotowany przez Wykonawcę,

b) Instalacja i konfiguracja komponentów środowiska oraz oprogramowania standardowego i dedykowanego leży po stronie Wykonawcy przy wsparciu Zamawiającego.

12.7. Wymagania w zakresie integracji, instalacji i konfiguracji.

12.7.1. Wykonawca musi wykonać instalację oprogramowania systemowego w porozumieniu z Zamawiającym w następującym zakresie:

a) instalacja i konfiguracja oprogramowania bazodanowego oraz wymaganych do prawidłowego działania Rozbudowanego Systemu baz danych na testowym i produkcyjnym klastrze bazodanowym będącym w posiadaniu Zamawiającego opartym co najmniejna PostgreSQL w wersji 10,

b) konfiguracja skryptów do backupu,

c) instalacja i konfiguracja pozostałego oprogramowania niezbędnego do prawidłowego i bezpiecznego działania Rozbudowanego Systemu w środowisku testowym i produkcyjnym,

d) konfiguracja konektorów systemu monitoringu na poszczególnych elementach infrastruktury.

13. Wymagania w zakresie technologii

13.1. Wymaga się, aby zastosowane przez Wykonawcę do realizacji Rozbudowanego Systemu oprogramowanie, użyte w szczególności do implementacji wymagań, było oprogramowaniem o otwartej licencji (Open Source), która pozwala na legalne oraz nieodpłatne kopiowanie, a także zapewnia swoim użytkownikom prawo do samodzielnego modyfikowania, analizowania i rozbudowy jego kodu, w tym spełnia poniższe warunki:

13.1.1. kod źródłowy musi być powszechnie dostępny do pobrania;

13.1.2. musi być dozwolona redystrybucja modyfikacji;

13.1.3. prawa związane z oprogramowaniem muszą się odnosić do wszystkich odbiorców programu, bez konieczności uzyskiwania dodatkowych licencji;

13.1.4. program nie może być licencjonowany tylko jako część szerszej dystrybucji;

13.1.5. licencja musi być technicznie neutralna tzn. że nie może pociągać za sobą zastrzeżeń dotyczących konkretnego rozwiązania technologicznego, stylu lub interfejsu;

13.1.6. oprogramowanie jest okresowo aktualizowane przez producenta.

13.2. Wszystkie powyższe warunki muszą być realizowanie łącznie przez okres co najmniej 6 miesięcy poprzedzających termin składania Ofert.

13.3. Wymaga się, aby dostęp do funkcjonalności Rozbudowanego Systemu dostępnych dla Użytkowników zewnętrznych zrealizowany był jako dostęp do e-usługi udostępnianej przez Portal Usług Elektronicznych Urzędu Komunikacji Elektronicznej. Modyfikacje w zakresie zmian niezbędnych w Portalu Usług Elektronicznych należą do Wykonawcy.

13.4. Wymaga się, aby istniała możliwość dostępu do Rozbudowanego Systemu, poprzez przeglądarkę, dla Użytkowników zewnętrznych, niezależnie od dostępu przez Portal Usług Elektronicznych.

13.5. Wymaga się, aby Rozbudowany System umożliwiał pracę na wszystkich platformach sprzętowo programowych, na których możliwe jest uruchamianie przeglądarek w aktualnych wersjach stabilnych: Microsoft Edge, Mozilla Firefox, Google Chrome oraz Safari.

13.6. Wymaga się, aby Rozbudowany System był zgodny z wytycznymi WCAG 2.1 na poziomie co najmniej AA.

13.7. Rozbudowany System musi zostać zmodyfikowany lub zbudowany pod względem UX/UI z uwzględnieniem opisu zawartego w załączniku nr 2 do OPZ - Opis stanu docelowego (wymagania funkcjonalne).

13.8. Rozbudowany System musi zapewnić (utrzymać istniejące) posiadane integracje z innymi systemami, o których mowa w dokumentacji systemu PUE. Dokonanie zmian we wszystkich zintegrowanych systemach w celu realizacji wymagania leży po stronie Wykonawcy.

13.9. Rozbudowany System musi posiadać formularz umożliwiający rejestrację zgłoszeń użytkowników w funkcjonującym u Zamawiającego systemie JIRA z zachowaniem informacji o użytkowniku, który dokonuje zgłoszenia.

13.10. Rozbudowany System musi być utworzony przy wykorzystaniu architektury opartej o mikroserwisy/ mikrousługi.

14. Wymagania w zakresie instruktażu dla Użytkowników wewnętrznych UKE

14.1. Wykonawca przygotuje i przeprowadzi, w terminie określonym w Harmonogramie i Harmonogramie Wdrożenia, instruktaże dotyczące obsługi Systemu dla pracowników Zamawiającego. Forma i zakres tematyczny instruktaży muszą zostać zaakceptowane przez Zamawiającego.

14.2. Zamawiający dopuszcza za jego zgodą przeprowadzenie instruktaży w formie zdalnej.

14.3. Instruktaże będą przeprowadzone na minimum trzech poziomach: poziom użytkownika, poziom administratora biznesowego oraz poziom administratora technicznego.

14.4. Maksymalna liczba uczestników:

14.4.1. 6 administratorów technicznych,

14.4.2. 30 użytkowników (z centrali i delegatur UKE).

14.5. Czas instruktażu: minimum 16h (2 dni) – dla każdego z trzech poziomów, przy czym poszczególne poziomy będą realizowane w odrębnych instruktażach i niepokrywających się terminach.

14.6. Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji harmonogram instruktaży, obejmujący terminy realizacji wszystkich instruktaży oraz zakresy tematyczne.

15. Bezpieczeństwo danych osobowych

15.1. Tworzone systemy muszą spełniać wymagania zawarte w RODO, Zasoby uczestniczące w przetwarzaniu danych osobowych będą monitorowane oraz zostanie zaplanowany i przeprowadzony audyt bezpieczeństwa (w oparciu o polską normę PN-ISO/IEC 27001 - Systemy zarządzania bezpieczeństwem informacji).

15.2. Obowiązkiem Wykonawcy jest zapewnienie i udokumentowanie przestrzegania podstawowych zasad przetwarzania danych osobowych zgodnie z treścią RODO, w szczególności:

15.2.1. Zasada zgodności z prawem, rzetelności przejrzystości – dane osobowe muszą być przetwarzane zgodnie z prawem, tj. musi istnieć podstawa prawna przetwarzania tych danych, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą, tzn. informacje dotyczące zbierania, wykorzystywania lub wszelkich innych sposobów przetwarzania danych oraz zakresu, w jakim te dane są lub będą przetwarzane przez administratora PUE muszą być znane i zrozumiałe dla tych osób.

15.2.2. Zasada ograniczonego celu – dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

15.2.3. Zasada minimalizacji danych – dane mogą być przetwarzane w zakresie adekwatnym, stosownym i ograniczonym do celu, w którym zostały zebrane.

15.2.4. Zasada prawidłowości – dane muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe były prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

15.2.5. Zasada ograniczonego przechowywania – dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez czas ograniczony do ścisłego minimum, nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (retencja danych).

15.2.6. Zasada integralności i poufności – przetwarzanie danych musi odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez stosowanie odpowiednich środków technicznych lub organizacyjnych.

15.2.7. Zasada rozliczalności – administrator danych musi być w stanie wykazać przestrzeganie wszystkich powyższych zasad (prowadzenie odpowiedniej dokumentacji oraz zapewnienie dowodów stosowania powyższych zasad).

15.3. Przestrzeganie zasad przytoczonych w punkcie 15.2. zobowiązuje w szczególności Wykonawcę do zastosowania odpowiednich środków technicznych i organizacyjnych związanych ze spełnieniem wymagań poprzez:

15.3.1. regularne kontrolowanie jakości działania systemów zgodnie z określonym harmonogramem, sposobem i procedurą,

15.3.2. audyt stosowanych algorytmów,

15.3.3. stosowanie zasady minimalizacji danych w procesie zbierania danych oraz odpowiedniej konstrukcji usług formularzowych,

15.3.4. korzystanie z anonimizacji lub pseudonimizacji danych, dla których ustał cel przetwarzania zgodnie z Art. 17 RODO, dla których wsparciem będzie zdefiniowanie i zastosowanie w Systemie rozwiązań odnośnie kopii zapasowych (tworzenie, przechowywanie i odtwarzanie), ochrony kryptograficznej, ochrony przed złośliwym oprogramowaniem,

15.3.5. opracowanie zestawu polityk, procedur i instrukcji dla grupy danych osobowych,

15.3.6. wykorzystanie środków technicznych i organizacyjnych pozwalających spełnić wymagania art. 33 i 34 RODO dotyczących monitorowania, wykrywania, rejestrowania i raportowania naruszeń danych osobowych między innymi poprzez wykorzystanie:

a) systemów klasy SIEM do monitorowania i analizy wszelkich incydentów bezpieczeństwa.

b) systemów klasy DLP (ang. Data Leak/Leakage/Loss Protection/Prevention) integrowanych z systemem klasy SIEM i umożliwiającym dodatkowo monitorowanie wycieku danych, raportowanie o zdarzeniach a także systemową analizę podatności z tytułu naruszeń danych osobowych.

c) zapory firewall (Web Application Firewall; Database Firewall).

15.4. Wykonawca w procesie wytwórczym zapewni, że Rozbudowany Systemu jest zgodnie z RODO zobowiązany do stosowania zasady Privacy By Design polegającej na projektowaniu rozwiązania z poszanowaniem prawa do prywatności jego użytkowników/odbiorców co znajduje wymiar w następujących zasadach:

15.4.1. podejściu proaktywnym, nie reaktywnym, zaradczym, nie naprawczym;

15.4.2. prywatności jako ustawienia domyślnego w fazie projektowej (tzw. Privacy by Default);

15.4.3. prywatności włączonej w projekt (tzw. Privacy Embedded Into Design);

15.4.4. pełnej funkcjonalności (suma dodatnia, nie suma zerowa);

15.4.5. ochrony od początku do końca cyklu życia informacji;

15.4.6. widoczności i przejrzystości;

15.4.7. poszanowania dla prywatności użytkowników.

16. Bezpieczeństwo kodu

16.1. W ramach zapewnienia bezpieczeństwa kodu źródłowego, Wykonawca jest zobowiązany przedstawić metodykę i narzędzia używane do zapewnienia bezpieczeństwa kodu.

16.2. W ramach realizacji przedmiotu zamówienia, Wykonawca jest zobowiązany do realizacji analizy bezpieczeństwa kodu (ang. SAST – Static Application Security Testing) na etapie wytwarzania i weryfikacji kodu w zakresie:

16.2.1. Przeglądów manualnych kodu realizowanych przez zespoły programistyczne mających na celu zidentyfikowanie błędów związanych ze strukturą kodu, przyjętymi dobrymi praktykami, wewnętrznymi regulacjami, jak również zaimplementowanymi regułami biznesowymi i logiką aplikacji. Wykonywane są przez członków zespołu deweloperskiego, posiadających niezbędną wiedzę do przeprowadzenia takiej weryfikacji. Przeglądy muszą być przeprowadzane kilkukrotnie, muszą być też elementem planowania prac zgodnie z przyjętą metodyką projektowania Swoim zakresem mogą objąć cały wytwarzany kod.

16.2.2. Automatycznej analizy statycznej kodu mającej na celu zidentyfikowanie błędów związanych z konstrukcją kodu, definiowaniem zmiennych, wywołaniami metod, użyciem poszczególnych funkcji. Analiza statyczna może weryfikować kod w zakresie wystąpień wzorców wskazujących na prawdopodobieństwo wystąpienia błędu programistycznego jako Common Weakness Enumeration (CWE/SANS TOP 25– Weaknesses - most dangerous software errors) i OWASP Top 10. Analiza musi być przeprowadzana kilkukrotnie na etapie wytwarzania oprogramowania, jak również na etapie testów bezpieczeństwa, będących etapem weryfikacji wytworzonego oprogramowania (testy penetracyjne). Swoim zakresem obejmuje cały wytwarzany kod. W związku z tym, że analiza przeprowadzana jest przy wykorzystaniu dedykowanych narzędzi, niezbędne jest opracowanie reguł i szablonów określających sposób weryfikacji dla zastosowanych języków programowania.

16.2.3. Przeglądów manualnych kodu realizowanych przez zespół bezpieczeństwa mających na celu przeprowadzenie dodatkowej weryfikacji obszarów, w których zidentyfikowano istotne błędy w ramach automatycznej analizy statycznej i testów penetracyjnych. Ma to na celu potwierdzenie potencjalnych błędów (poprzez eliminację „false positives") mogących mieć wpływ na bezpieczeństwo funkcjonowania systemu lub też na obniżenie skuteczności zastosowanych mechanizmów bezpieczeństwa.

16.3. Zakres przeglądów manualnych kodu realizowanych przez zespoły programistyczne będzie indywidualnie planowany w ramach przyjętej metodyki projektowania. Zebrane wyniki będą wykorzystywane na bieżąco przez zespoły programistyczne. Nie będą tworzone dodatkowe artefakty w postaci raportów z przeglądów.

16.4. Analiza statyczna kodu będzie realizowana jako element „continuous integration", przy wsparciu zespołu bezpieczeństwa oraz na zakończenie prac programistycznych, stanowiąc element testów bezpieczeństwa. Na tej podstawie Wykonawca opracuje raport zawierający między innymi listę zidentyfikowanych błędów lub podatności, poziom ich krytyczności oraz rekomendacje związane ze sposobem ich usunięcia.

16.5. Przegląd manualny kodu realizowany przez zespół projektowy będzie stanowił uzupełnienie automatycznej analizy statycznej kodu. Uzyskane informacje o potwierdzonych błędach i podatnościach zostaną dołączone do ww. raportu z analizy statycznej kodu. Powyższa analiza musi uwzględniać rozwiązania eliminujące lub znacząco zmniejszające podatność projektowanego systemu na ataki i być oparta na dobrych praktykach w zakresie bezpiecznego kodowania takimi jak CVE, CERT, MITRE CWE i ująć aktualne trendy w wektorach ataku.

17. Wymagania w zakresie prowadzenia testów w projekcie

Testy penetracyjne

17.1. Testy penetracyjne nie wchodzą w zakres niniejszego zamówienia. Zamawiający podaje założenia dla testów penetracyjnych, które zostaną zrealizowane przez podmiot wskazany przez Zamawiającego.

17.2. Testy zostaną przeprowadzone zgodnie ze standardami testowania bezpieczeństwa, dla przykładu:

17.2.1. Open Web Application Security Project (OWASP) Web Security Testing Guide, Application Security Verification Standard,

17.2.2. Open Source Security Testing Methodology Manual (OSSTMM),

17.2.3. Penetration Testing Execution Standard (PTES).

17.3. Skany podatności zostaną realizowane automatycznie lub w sposób dalece zautomatyzowany (przy użyciu specjalistycznego oprogramowania), uzupełnione testami penetracyjnymi uwzględniającymi wyniki skanowania.

17.4. Zamawiający przewiduje objęcie testami penetracyjnymi elementów Systemu PUE w podziale na dwie grupy:

17.4.1. testy aplikacji – przeprowadzane w środowisku zbieżnym z produkcyjnym, mające zidentyfikować podatności możliwe do wykorzystania w trakcie użytkowania aplikacji. W ramach testów wykorzystywane będą narzędzia wspierające proces testowania (testy półautomatyczne). W ramach tych działań przewidywane są dwa podejścia, pierwsze „Gray Box" (na podstawie dostarczonej dokumentacji projektowej i przekazanej wiedzy od zespołu projektowego) prowadzone z wewnątrz, drugie „Black Box" prowadzone z zewnątrz.

17.4.2. testy infrastruktury – przeprowadzane w środowisku produkcyjnym, mające na celu zweryfikowanie poprawności instalacji i konfiguracji mechanizmów bezpieczeństwa infrastruktury sprzętowo-programowej, w tym:

a. urządzeń sieciowych, serwerów oraz macierzy, systemów operacyjnych;

b. usług sieciowych, aplikacji serwerowych;

c. baz danych;

d. zewnętrznych komponentów bezpieczeństwa;

e. serwerów firewall, urządzeń HSM.

17.5. Testowanie obejmie ryzyka występujące w obszarach, takich jak:

17.5.1. uwierzytelnianie;

17.5.2. zarządzanie sesją;

17.5.3. kontrola dostępu;

17.5.4. walidacja wejścia;

17.5.5. kryptografia;

17.5.6. obsługa błędów i logowanie;

17.5.7. ochrona danych;

17.5.8. bezpieczeństwo komunikacji;

17.5.9. wyszukiwanie złośliwego kodu;

17.5.10. logika biznesowa;

17.5.11. weryfikacja zasobów i plików.

17.6. Proces testowania musi zapewnić, że każdorazowe badanie z uwzględnieniem metodyki zawartej w normach branżowych będzie składało się z następujących, wyróżnionych etapów:

17.6.1. przeprowadzenie badań i testów;

17.6.2. opracowanie oceny eksperckiej;

17.6.3. przedstawienie wiążącego stanowiska;

17.6.4. przedstawienie rekomendacji zmian.

17.7. W wyniku testów penetracyjnych zostanie opracowany raport zawierający między innymi listę zidentyfikowanych błędów i podatności, ich poziom krytyczności (istotności) oraz rekomendacje związane ze sposobem ich usunięcia.

17.8. Wykonawca jest zobowiązany do usunięcia wykrytych w ramach testów penetracyjnych błędów i podatności.

17.9. Zespół testowy będzie musiał spełniać wymóg odpowiedniego doświadczenia popartego rozpoznawalnymi certyfikatami z zakresu cyberbezpieczeństwa, np.:

17.9.1. Offensive Security Proffessional (OSCP)

17.9.2. Certified Ethical Hacker (CEH)

17.9.3. CompTIA Pentest+ (Pentest+)

17.9.4. Certified Information Systems Auditor (CISA)

17.9.5. GIAC Penetration Tester (GPEN)

17.9.6. Certified Information Systems Security Professional (CISSP)

17.10. Rozbudowany system będzie poddawany testom bezpieczeństwa przed wdrożeniem jak i podczas użytkowania - co najmniej jeden raz w roku.

18. Wymagania dotyczące poziomu świadczenia usług

18.1. Poziom dostępności Rozbudowanego Systemu:

18.1.1. Zakres usług dostępu do Rozbudowanego Systemu rozumiany jest jako realizacja przez Rozbudowany System wszystkich funkcjonalności zgodnie z zatwierdzoną Dokumentacją oraz obowiązującym prawem.

18.1.2. Usługi dostępu do Rozbudowanego Systemu będą świadczone w trybie 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, 366 dni w roku przestępnym.

18.1.3. Dla zapewnienia wysokiej dostępności Rozbudowanego Systemu Wykonawca musi zastosować model architektury, który zapewni niezawodność całego rozwiązania. W tym wypadku Zamawiający wymaga zastosowania redundancji komponentów Rozbudowanego Systemu we wszystkich jego warstwach.

18.1.4. Krytyczne komponenty Rozbudowanego Systemu w środowisku produkcyjnym muszą być uruchomione jako klastry serwerów działających w trybie wysokiej dostępności (HA).

18.1.5. W Rozbudowanym Systemie musi zostać zagwarantowana dostępność na poziomie nie mniejszym niż 98% w skali miesiąca.

18.1.6. Dostępność Rozbudowanego Systemu będzie monitorowana z wykorzystaniem narzędzi posiadanych przez Zamawiającego.

18.1.7. Wykonawca musi przygotować skrypty monitorujące dostępność. Skrypty muszą być możliwe do uruchomienia przy użyciu narzędzi posiadanych przez Zamawiającego.

18.2. Poziom wydajności Rozbudowanego Systemu

18.2.1. Rozbudowany System musi zapewnić skalowalność (na poziomie warstw front-end, back-end i warstwie bazodanowej) w zakresie wydajności i pojemności oraz dołączania dodatkowych Użytkowników oraz elementów infrastruktury sprzętowej.

18.2.2. Rozbudowany System musi zapewniać równoległą obsługę Użytkowników. Wydajność Rozbudowanego Systemu musi zostać zapewniona przy korzystaniu z Rozbudowanego Systemu dziennie przez:

a) 100 użytkowników wewnętrznych (pracownicy UKE),

b) 1000– użytkowników zewnętrznych (Przedsiębiorcy telekomunikacyjni, jednostki samorządu terytorialnego, przedsiębiorstwa użyteczności publicznej)

c) 1000 – użytkowników Zewnętrznych (Pozostali, niezalogowani użytkownicy)

18.2.3. Wydajność Rozbudowanego Systemu będzie weryfikowana w czasie testów wydajnościowych, które zostaną przeprowadzone przez Wykonawcę oraz Zamawiającego oraz przy zastosowaniu rozwiązania do monitorowania wydajności.

18.2.4. Czasy odpowiedzi Rozbudowanego Systemu weryfikowane:

a) Czasy odpowiedzi usług Rozbudowanego Systemu, wykorzystywanych przez Użytkowników Wewnętrznych dla co najmniej 98% wszystkich żądań (próbek) muszą być krótsze niż 2 sekundy, przy maksymalnej liczbie jednocześnie pracujących Użytkowników Wewnętrznych,

i) Weryfikacji będą podlegały czasy odpowiedzi dla operacji opisanych przez główne przypadki użycia, jednak nie może to być mniej niż 20% wszystkich zidentyfikowanych przypadków użycia dla Użytkowników Wewnętrznych,

ii) Czasy odpowiedzi usług Systemu wykorzystywanych przez użytkowników zewnętrznych dla co najmniej 98% wszystkich żądań (próbek) muszą być krótsze niż 2 sekundy przy maksymalnej liczbie jednocześnie pracujących użytkowników zewnętrznych. Weryfikacji będą podlegały czasy odpowiedzi dla operacji opisanych przez główne przypadki użycia, jednak nie może to być mniej niż 20% wszystkich zidentyfikowanych przypadków użycia dla użytkowników zewnętrznych.

18.3. Monitorowanie wydajności Rozbudowanego Systemu;

18.3.1. Wykonawca jest zobowiązany do opracowania konfiguracji środowiska Zabbix Zamawiającego w zakresie umożliwiającym prowadzenie testów wydajnościowych oraz monitorowania wydajności i dostępności Systemu.

18.3.2. Na potrzeby monitorowania wydajności Wykonawca musi przygotować rozwiązanie pozwalające na:

a) Rejestrowanie zdarzeń o realizacji operacji (w tym przypadku przez operację należy rozumieć realizację przypadku użycia), z uwzględnieniem:

i) Unikalnego identyfikatora operacji,

ii) Czasów rozpoczęcia operacji i zakończenia operacji,

b) Korelację zdarzeń,

c) Prezentację wyników pomiarów i czasów odpowiedzi Rozbudowanego Systemu w graficznym interfejsie Użytkownika, w które zostanie wyposażone rozwiązanie.

19. Wymagania w zakresie Gwarancji i Usług Wsparcia

19.1. Zasady wykonywania Gwarancji oraz Usług Wsparcia a także ich zakres określa Załącznik nr 10 do SWZ – wzór Umowy.

19.2. Minimalny wymagany przez Zamawiającego okres gwarancji wynosi 3 miesiące od dnia podpisania Protokołu Odbioru Końcowego.

19.3. Wykonawca udzieli Gwarancji oraz będzie świadczył Usługi Wsparcia Systemu. Zgłoszenia w zakresie Gwarancji będą dokonywane za pośrednictwem funkcjonalności Help-Desk, a w przypadku braku takiej możliwości za pośrednictwem poczty elektronicznej na dedykowany adres mailowy Wykonawcy. W przypadku błędów zgłoszenie będzie zawierało co najmniej następujące informacje:

19.3.1. kategoria ujawnionego Błędu w działaniu Systemu,

19.3.2. opis nieprawidłowości w działaniu Systemu,

19.3.3. opis błędu raportowany przez System, o ile będzie dostępny;

19.4. Wykonawca odpowiada za prawidłowe działanie całości Systemu i każdego jego elementu z osobna, zgodnie z wymaganiami określonymi w Umowie, w tym w szczególności w OPZ oraz w Analizie Przedwdrożeniowej.

19.5. Wykonawca odpowiada za zachowanie integralności i ciągłości pracy Systemu, także w przypadku obsługi Błędów, instalacji Aktualizacji, jakichkolwiek poprawek lub innych zmian w Systemie, dokonywanych przez Wykonawcę w celu wdrożenia Rozbudowanego Systemu lub usunięcia Błędów. W ramach obsługi Błędów Systemu Wykonawca nie może usuwać jakichkolwiek danych aktualnych i archiwalnych, z wyjątkiem sytuacji uzgodnionych przez Wykonawcę i Zamawiającego w formie pisemnej pod rygorem nieważności.

19.6. W ramach Gwarancji na System Wykonawca zapewni:

19.6.1. obsługę Błędów w Systemie, w terminach niżej określonych (Gwarantowany Czas Naprawy):

a) Awaria – Błąd powodujący nieprawidłowości w funkcjonowaniu systemu PUE niezgodnie z dokumentacją lub specyfikacją wymagań, powodujące niemożność lub utrudnienia w eksploatacji Systemu,

b) Błąd poziomu 1 – Błąd powodujący brak działania całości systemu lub funkcjonowania mechanizmów bezpieczeństwa,

c) Błąd poziomu 2 – Błąd powodujący brak działania części funkcjonalności lub niekompletność mechanizmów bezpieczeństwa,

d) Błąd poziomu 3 – Błąd dotyczący ergonomii kluczowych funkcjonalności systemu PUE,

e) Błąd poziomu 4 - Błąd dotyczący ergonomii mniej istotnych funkcjonalności, błędy literowe w tekstach pojawiających się na ekranie i wydrukach, uwagi do wyglądu interfejsu użytkowników nie wpływające bezpośrednio na ergonomię.

19.6.2. Gwarantowany czas naprawy powyższych błędów obowiązujący w dni robocze w godzinach 8:00-16:00:

a) Awaria - Wykonawca zobowiązuje się określić przyczynę Awarii i uruchomić system PUE w terminie 4 godzin od zgłoszenia;

b) Błąd poziomu 1 - Wykonawca zobowiązuje się określić przyczynę Awarii i uruchomić system PUE w terminie 12 godzin od zgłoszenia;

c) Błąd poziomu 2 - Wykonawca zobowiązuje się określić przyczynę Awarii i uruchomić system PUE w terminie 44 godzin od zgłoszenia;

d) Błąd poziomu 3 - Wykonawca zobowiązuje się określić przyczynę Awarii i uruchomić system PUE w terminie 5 dni kalendarzowych od zgłoszenia;

e) Błąd poziomu 4 - Wykonawca zobowiązuje się określić przyczynę Awarii i uruchomić system PUE w terminie 10 dni kalendarzowych od zgłoszenia;

19.6.3. usuwanie Błędu Regresji – Wykonawca zobowiązuje się określić przyczynę Błędu Regresji usunąć go i uruchomić System w terminie 7 dni roboczych,

19.7. Dokonując zgłoszenia w ramach Gwarancji, Zamawiający określa kategorię Błędu zgodnie z definicjami zawartymi w OPZ. Kategorię Błędu określa Zamawiający i jest to wiążące dla Wykonawcy.

19.8. Uszkodzone nośniki danych (dyski) pozostają u Zamawiającego.

20. Wymagania w zakresie Usług Rozwoju Rozbudowanego Systemu

20.1. Od dnia podpisania Protokołu Odbioru Wykonawca będzie świadczył Usługi Rozwoju Rozbudowanego Systemu w wymiarze nie mniejszym niż 1 500 roboczogodzin (zegarowych).

20.2. Zasady świadczenia Usług Rozwoju określa Załącznik nr 10 do SWZ – wzór Umowy.

21. Załączniki do OPZ

Załącznik 1 do OPZ – Opis stanu obecnego

Załącznik 2 do OPZ – Opis stanu docelowego (wymagania funkcjonalne)

Załącznik nr 3 do OPZ – Wzór przykładowej dokumentacji projektu, opatrzonej wymaganymi logotypami