Opis przedmiotu zamówienia

1. Nazwa zamówienia

Zakup, wdrożenie i utrzymanie narzędzia do kompleksowej obsługi procesu wnioskowania o dane jednostkowe z systemu Centralnej Ewidencji Pojazdów i Kierowców (CEPiK).

2. Oznaczenie przedmiotu zamówienia wg Kod CPV:

48900000-7 - Różne pakiety oprogramowania i systemy komputerowe.

72263000-6 - Usługi wdrażania oprogramowania.

72611000-6 - Usługi w zakresie wsparcia technicznego.

3. Słownik pojęć

1. **Administrator** – pracownik Zamawiającego posiadający uprawnienia do parametryzacji (konfigurowania) Systemu.
2. **AD/LDAP** - AD (Active Directory) i LDAP (Lightweight Directory Access Protocol) są protokołami służącymi do zarządzania i przeglądania katalogów w sieciach komputerowych. AD jest rozwiązaniem dla systemu Windows i jest integralną częścią tego systemu operacyjnego. LDAP jest ogólnym protokołem, który może być używany przez różne systemy operacyjne i aplikacje**.**
3. **Awaria** - nieprawidłowe działanie Systemu, w szczególności stan, w którym nie jest możliwe korzystanie z Systemu w sposób zgodny z jego przeznaczeniem, Umową lub Dokumentacją. Awaria dzieli się na Awarię Krytyczną i Awarię Niekrytyczną.
4. **Awaria Krytyczna –** Awaria wywołująca nieprawidłowe działanie Systemu, powodujące całkowity brak możliwości korzystania z Systemu albo ograniczenie korzystania z Systemu uniemożliwiające spełnianie jego podstawowych funkcji określonych w ust.18.
5. **Awaria Niekrytyczna –** Awaria inna niż Awaria Krytyczna.
6. **Baza Wiedzy -** repozytorium informacyjne, które ma gromadzić wszystkie informacje o Systemie i stanowić pomoc techniczną dla Użytkowników, w tym informacje o rozwiązywanych problemach, obejściach i inne porady, wskazówki, instrukcje**.**
7. **Błąd -** każda, stwierdzona na etapie częściowych lub końcowych testów akceptacyjnych lub powdrożeniowych, niezgodność działania Systemu, w tym jego elementu, z Umową, OPZ lub Dokumentacją, uniemożliwiająca całkowicie lub w ograniczonym zakresie niezakłócone korzystanie z funkcjonalności Systemu.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

8. **Czas naprawy –** czas na usunięcie Awarii liczony od momentu zgłoszenia Awarii do momentu dostarczenia przez Wykonawcę rozwiązania usuwającego Awarię**.**
9. **Dokumentacja** - wszelka dokumentacja dotycząca Systemu, dostarczona lub wykonana w ramach Umowy, w szczególności lecz nie wyłącznie, Projekt techniczny; analiza, Dokumentacja powykonawcza; Dokumentacja użytkowa, instrukcje obsługi, oraz wszelka inna dokumentacja dotycząca przedmiotu Umowy, w tym materiały szkoleniowe, lub pochodząca od producenta Systemu; a także aktualizacje Dokumentacji dokonywane w okresie obowiązywania Umowy. Dokumentacja jest wersjonowana i dostarczana w formie elektronicznej w języku polskim.
10. **Dokumentacja powykonawcza –** dokumentacja wykonana lub dostarczona przez Wykonawcę opisująca architekturę, konfigurację i parametryzację Systemu.
11. **Dokumentacja użytkowa –** dokumentacja wykonana lub dostarczona przez Wykonawcę zawierająca procedury eksploatacyjne; awaryjne i instrukcje stanowiskowe; umożliwiająca prawidłowe korzystanie z Systemu Użytkownikom oraz Administratorom.
12. **Dzień roboczy** – dni od poniedziałku do piątku; oprócz dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej.
13. **Godziny eksperckie** - usługi świadczone przez Wykonawcę, dotyczące m.in. konsultacji; instruktażu, usuwania wątpliwości lub rozwiązywania bieżących problemów Zamawiającego związanych z obsługą, w tym: instalacją, konfiguracją, administracją, integracją Systemu. Usługi będą realizowane w miejscu zainstalowania Oprogramowania lub zdalnie, w Dni Robocze w godzinach 08.00-17.00, o ile strony nie postanowią inaczej.
14. **Obejście –** tymczasowe rozwiązanie w ramach Systemu umożliwiające korzystanie z Systemu, nieusuwające przyczyny Awarii, zaproponowane przez Wykonawcę i zaakceptowane przez Zamawiającego. Obejście nie stanowi usunięcia Awarii i nie zwalnia Wykonawcy od obowiązku jej usunięcia.
15. **Oprogramowanie –** całość lub dowolny element oprogramowania spełniającego wymagania określone w niniejszym OPZ; dostarczanego lub wykonywanego w ramach realizacji Umowy; niezbędnego do prawidłowego funkcjonowania Systemu; wraz z odpowiednimi licencjami uprawniającymi do korzystania z Oprogramowania. Pojęcie to obejmuje również wszystkie aktualizacje i elementy przewidziane przez producenta Oprogramowania dla prawidłowego korzystania z Oprogramowania. Przez aktualizacje rozumie się uaktualnienia Oprogramowania, w tym nowe wersje Oprogramowania (upgrade), niższe wersje Oprogramowania (downgrade), wydania uzupełniające, poprawki programistyczne (patche), nowe wydania Oprogramowania będące kontynuacją linii produktowej, oraz inne dostosowania zapewniające prawidłowe korzystanie z Oprogramowania.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

16. **Platforma zgłoszeniowa –** serwis www umożliwiający użytkownikom Zamawiającego rejestrowanie Zgłoszeń, Zamówień, w tym w ramach serwisu gwarancyjnego, wsparcia technicznego**.**
17. **Projekt techniczny –** Dokument techniczny opracowany przez Wykonawcę, zawierający specyfikację techniczną, analizę wymagań, opisujący wszystkie istotne dla zakresu prac związanych z Systemem, uwarunkowania oraz zależności, wraz z niezbędnym szczegółowym opisem zakresu prac wykonanych na potrzeby wdrożenia Systemu.
18. **Rozwiązanie** – usunięcie Awarii Systemu, po uzgodnieniu z Zamawiającym dopuszczalne jest uznanie zastosowanego Obejścia jako usunięcie Awarii.
19. **System** – Oprogramowanie do kompleksowej obsługi procesu wnioskowania o dane jednostkowe z systemu Centralnej Ewidencji Pojazdów i Kierowców; którego podstawowymi funkcjami są:

    1) Obsługa procesu wnioskowania o dostęp do API
    2) certyfikacja i nadanie dostępów do API dla wnioskodawców, w tym dla poszczególnych lokalizacji;
    3) integracja z zewnętrznymi podmiotami przez API (wejście-wyjście)
    4) dekretacja i monitoring wniosków w ramach funkcji Koordynatora,
    5) elektroniczna obsługa wniosków przez operatora po stronie Zamawiającego,
    6) funkcja automatyzująca proces weryfikacji (z wykorzystaniem np. funkcji OCR) danych i załączników w ramach wniosków obsługiwanych w procesie obsługowym[1]
    7) integracja i pobranie danych z systemem CEPIK
    8) rejestracja wniosków z innych kanałów przez Operatorów
    9) raportowanie i informacja zarządcza – tworzenie raportów zarządczych i indywidualnych

20. **Środowisko produkcyjne –** oznacza infrastrukturę Zamawiającego wraz z zainstalowanym na niej Oprogramowaniem, określonym przedmiotem zamówienia, zarówno w ośrodku głównym jak i ośrodku zapasowym.
21. **Środowisko testowe** - oznacza infrastrukturę Zamawiającego odwzorowaną ze środowiskiem produkcyjnym, posiadające komponenty potrzebne do wykonania testów.
22. **Umowa** – umowa zawarta między Zamawiającym, a Wykonawcą na realizację przedmiotu zamówienia opisanego w niniejszym OPZ.
23. **Wsparcie techniczne –** usługi zapewniane przez Wykonawcę w oparciu o wsparcie techniczne producenta Oprogramowania, w okresie 12/24/36 miesięcy od daty podpisania protokołu

[1] Funkcjonalność dodatkowa, dodatkowo wyceniana.

odbioru końcowego wdrożenia Systemu, mające na celu zapewnienie poprawnego działania Systemu oraz wsparcie Zamawiającego w korzystaniu z Systemu.

24. **Użytkownik –** osoba korzystająca z Systemu o zdefiniowanych w Systemie uprawnieniach w zależności od roli w procesie lub organizacji.
25. **Wada -** każda, stwierdzona na etapie częściowych lub końcowych testów powdrożeniowych, niezgodność działania Systemu, w tym jego elementu, z Umową, OPZ lub Dokumentacją, uniemożliwiająca całkowicie lub w ograniczonym zakresie niezakłócone korzystanie z wszystkich funkcjonalności Systemu.
26. **Zgłoszenie –** dowolny wniosek lub incydent zgłoszony do Wykonawcy zgłoszony kanałem wskazanym w rozdziale 13 ust.e) niniejszego OPZ.
27. **Zlecenie –** zgłoszenie zapotrzebowania na realizację Godzin eksperckich w ramach prawa opcji.
28. **Zmiana -** definicja zgodna z aktualną wersją słownika ITIL.
29. **Czas reakcji** - Czas liczony od momentu przekazania do Wykonawcy przez zamawiającego zgłoszenia do momentu potwierdzenia przez wykonawcę do zamawiającego rozpoczęcia obsługi zgłoszenia.

4. Przedmiot zamówienia

4.1.1. Przedmiotem zamówienia w ramach zamówienia podstawowego jest zakup, wdrożenie i utrzymanie narzędzia do kompleksowej obsługi procesu wnioskowania o dane jednostkowe z systemu Centralnej Ewidencji Pojazdów i Kierowców, z wyłączeniem z wyłączeniem funkcji opisanej w pkt poniżej:

a) funkcja automatyzująca proces weryfikacji (z wykorzystaniem np. funkcji OCR) danych i załączników w ramach wniosków obsługiwanych w procesie obsługowym – opcja dodatkowa[2]

4.1.2. w ramach opcji:

a) godziny eksperckie - świadczenie w ramach opcji Godzin eksperckich zgodnie opisem w OPZ.

5. Termin realizacji zamówienia

1. Realizacji przedmiotu zamówienia: w terminie nie dłuższym niż ….[3] miesięcy od dnia zawarcia umowy.
2. System zostanie objęty gwarancją przez okres 12/24/36 miesięcy od dnia podpisania przez strony bez zastrzeżeń protokołu odbioru końcowego wdrożenia Systemu.
3. Dostarczone licencje na Oprogramowanie zostaną objęte wsparciem technicznym wraz z dostępem do aktualizacji pochodzących z oficjalnego kanału producenta, przez okres

[2] Funkcjonalność dodatkowa, dodatkowo wyceniana.
[3] Prosimy o podanie wartości w formularzu wyceny załączonym do RFI.

12/24/36 [4]miesięcy od dnia podpisania przez strony bez zastrzeżeń protokołu odbioru końcowego wdrożenia Systemu.

4. Licencje dostarczone w ramach opcji zostaną objęte wsparciem technicznym wraz z dostępem do aktualizacji pochodzących z oficjalnego kanału producenta od dnia podpisania protokołu ich odbioru do dnia zakończenia wsparcia technicznego licencji zakupionych w ramach zamówienia podstawowego liczonego zgodnie z opisem w ust. 3 powyżej.

6. Przedmiot zamówienia podstawowego

Przedmiotem zamówienia podstawowego jest zakup, wdrożenie i utrzymanie narzędzia do kompleksowej obsługi procesu wnioskowania o dane jednostkowe z systemu Centralnej Ewidencji Pojazdów i Kierowców, w tym co najmniej:

1) Obsługa procesu wnioskowania o dostęp do API;
2) certyfikacja i nadanie dostępów do API dla wnioskodawców, w tym dla poszczególnych lokalizacji;
3) integracja z zewnętrznymi podmiotami przez API (wejście-wyjście);
4) dekretacja i monitoring wniosków w ramach funkcji Koordynatora;
5) elektroniczna obsługa wniosków przez operatora po stronie Zamawiającego,
6) zapewnienie możliwości przygotowania i eksportu pliku word ze wskazanymi przez Operatora danymi z wniosku i/lub załączników;
7) integracja i pobranie danych z systemem CEPIK;
8) udostępnienie przez API odpowiedzi na wniosek w postaci np. pdf, xml;
9) rejestracja wniosków z innych kanałów przez Operatorów;
10) raportowanie i informacja zarządcza – tworzenie raportów zarządczych i indywidualnych.

7. Organizacja Projektu

1. Przygotowanie projektu technicznego wdrożenia narzędzia do kompleksowej obsługi procesu wnioskowania o dane jednostkowe z systemu Centralnej Ewidencji Pojazdów i Kierowców, tj. dokumentu opracowanego przez Wykonawcę zawierającego:
   1) specyfikację techniczną, w tym architekturę systemu, architekturę integracji, funkcje systemu, opis konfiguracji i parametryzacji Systemu, opis struktur bazy danych, opis modelu

[4] Należy wycenić każdą z opcji

uprawnień, opis koncepcji administrowania systemem, opis zasad bezpieczeństwa i ochrony danych, opis sposobu integracji z systemami Zamawiającego;

2) specyfikację Infrastruktury IT zapewniającej spełnienie wymagań wydajnościowych Systemu
   a. Zamawiający udostępni maszyny wirtualne wskazane przez Wykonawcę. Zostaną one zainstalowane na infrastrukturze VMware lub KVM.
   b. Zastosowane przez Wykonawcę komponenty aplikacji (w szczególności biblioteki lub Oprogramowanie standardowe) nie mogą wymuszać wyboru technologii wskazanej w punkcie 2a (tzw. brak vendor lock-in).
   c. Środowisko produkcyjne Infrastruktury IT musi umożliwiać obsługę następującego obciążenia:
      i. Wpływ około 7 000 wniosków dziennie i około 150 000 wniosków miesięcznie,
      ii. Odbiór danych dla około 7000 wniosków dziennie
3) zalecaną konfigurację oraz prognozę skalowania Infrastruktury w ciągu trzech latach użytkowania Systemu zapewniającej spełnienie wymagań wydajnościowych Systemu w oparciu o doświadczenia Wykonującego u innych Zamawiających w oparciu o specyfikację opisaną
   w pkt.2)
4) Projekt architektury aplikacji zawierającej połączenia sieciowe pomiędzy maszynami wirtualnymi oraz środowiskami znajdującymi się na zewnątrz wydzielonego VPC. Projekt architektury musi uwzględniać elementy w zakresie bezpieczeństwa (np. potrzebę wystawienia load balancerów lub firewalli). Wykonawca przygotuje Projekt architektury dla środowisk produkcyjnych i testowych.
5) opisy wszystkich istotnych dla zakresu prac związanych z Systemem uwarunkowań oraz zależności;
6) opis sposobu prowadzenia projektu, w tym opis zakresu prac niezbędnych do wykonania na potrzeby wdrożenia Systemu;

2. Opracowanie Harmonogramu, który musi określać terminy realizacji przez Wykonawcę poszczególnych etapów realizacji zamówienia, przyjmując jako termin odniesienia datę podpisania Umowy, w tym:
   1) termin wykonania Projektu technicznego,
   2) termin wykonania analizy przedwdrożeniowej oraz sporządzenia jej dokumentacji;
   3) termin dostawy licencji do Oprogramowania;
   4) termin instalacji, wdrożenia oraz konfiguracji systemu w podziale na etapy;

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

5) termin wykonania integracji systemu ze wskazanymi systemami informatycznymi Zamawiającego;
6) termin przeprowadzenia testów akceptacyjnych i powdrożeniowych, sporządzenia i dostarczenie dokumentacji;
7) termin uruchomienia produkcyjnego systemu;
8) termin przeprowadzenia szkoleń, sporządzenia i dostarczenia dokumentacji z przeprowadzonych szkoleń;
9) termin dostawy kompletu Dokumentacji Systemu;
10) termin podpisania protokołu odbioru końcowego,
11) realizacja serwisu gwarancyjnego i wsparcia technicznego w okresie 36 miesięcy od daty podpisania protokołu odbioru.

8. Dostawa Systemu wraz z licencjami

8.1.1.1. Dostawa oprogramowania wraz z niezbędnymi licencjami wieczystymi systemów oraz aplikacji w tym dla poszczególnych ról użytkowników:

1) administratorów (4 licencje);
2) użytkowników z dostępem do funkcjonalności w ramach roli Operator (80 licencji);
3) użytkowników z dostępem do funkcjonalności w ramach roli Koordynator (6 licencji).

9. Instalacja Systemu:

9.1.1.1. Instalacja Systemu nastąpi:

1) na wydzielonej części lokalnej infrastruktury Zamawiającego, obejmującej przygotowane środowisko testowe, a na kolejnym etapie środowisko produkcyjne;
2) w Dni robocze w godzinach 08.00-17.00; chyba że Strony postanowią inaczej,
3) pod nadzorem przedstawicieli Zamawiającego.

10. Wdrożenie, konfiguracja i uruchomienie Systemu

10.1.1.1. Wdrożenie ze strony Wykonawcy przeprowadzą osoby z doświadczeniem i kompetencjami wskazane przez Wykonawcę w wykazie dołączonym do Oferty.

10.1.1.2. Wykonawca zobowiązuje się do stosowania standardów zarządzania projektem z wykorzystaniem jednej ze stosowanych w praktyce rynkowej metodyk zarządzania projektem IT.

10.1.1.3. Za stosowanie tego standardu podczas realizacji Umowy odpowiedzialny będzie Kierownik Projektu wskazany przez Wykonawcę w Dokumentacji projektowej.

10.1.1.4. Wdrożenie nastąpi przy aktywnym współudziale wyznaczonych pracowników Zamawiającego.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

10.1.1.5. Wykonawca zainstaluje komponenty oferowanego Oprogramowania (np. wymagane biblioteki, Oprogramowanie standardowe) na maszynach wirtualnych wskazanych w Projekcie Technicznym. Maszyny wirtualne zostaną wykreowane przez Zamawiającego i będą posiadały zainstalowany system operacyjny wskazany przez Wykonawcę.

10.1.1.6. W ramach Wdrożenia Wykonawca dokona hardeningu komponentów instalowanych w ramach prac wskazanych powyżej.

10.1.1.7. Wdrożenie obejmie budowę i zasilenie bazy danych (hurtowni danych) stanowiącej integralną część Systemu dostarczonego przez Wykonawcę.

10.1.1.8. Wdrożenie modułów obsługujących procesy wyszczególnione w rozdziale 6 zgodnie z wymaganiami funkcjonalnymi określonymi w rozdziale 16 niniejszego OPZ.

10.1.1.9. Integrację ze sobą dostarczonych modułów.

10.1.1.10. Konfigurację, parametryzację i budowę połączeń oraz przepływów (workflow) pomiędzy wszystkimi elementami Systemu.

10.1.1.11. Przygotowanie widoków i raportów w zależności od uprawnień użytkowników Systemu.

10.1.1.12. Zdefiniowanie profili, ról i uprawnień w Systemie.

10.1.1.13. Wykonanie innych, nieprzewidzianych czynności niezbędnych do prawidłowego wdrożenia Systemu.

10.1.1.14. Wdrożenie i odbiór prac będą prowadzone etapowo zgodnie z Harmonogramem.

10.1.1.15. Po każdym zakończonym etapie będzie podpisywany oddzielny protokół odbioru produktów prac zrealizowanych w jego ramach.

10.1.1.16. Zamawiający przewiduje płatność po zakończonym odbiorze końcowym.

11. Testy akceptacyjne i powdrożeniowe

1. Testy akceptacyjne i powdrożeniowe

1.1.1.1. Po zakończeniu przez Wykonawcę realizacji każdego z etapów wdrożenia Systemu, zostaną wykonane testy akceptacyjne oraz powdrożeniowe, potwierdzające zgodność z zamówieniem zarówno pod kątem funkcjonalnym jak i niefunkcjonalnym. Wykonawca koordynuje testy zgodnie z harmonogramem oraz potwierdza gotowość środowisk do testów po stronie zamawiającego.

1.1.1.2. Przeprowadzone przez Wykonawcę testy akceptacyjne i powdrożeniowe odnoszą się do procesów i modułów objętych danym etapem z zastrzeżeniem, że po zakończeniu realizacji ostatniego z etapów wynikających z Harmonogramu wdrożenia Systemu, będą swoim zakresem obejmować całościowo wdrożony System.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1.1.1.3. Testy akceptacyjne i powdrożeniowe zostaną przeprowadzone przez Wykonawcę w oparciu o scenariusze testowe przygotowane przez Wykonawcę w tym celu. Dane testowe na środowisku testowym zostaną przygotowane przez Wykonawcę w celu przeprowadzenia testów akceptacyjnych.

1.1.1.4. Dla każdego etapu, Wykonawca wykona instalację oprogramowania na środowisku testowym, które zweryfikuje przed oddaniem do testów akceptacyjnych lub powdrożeniowych i stan środowiska przekaże w formie raportu.

1.1.1.5. Zamawiający wymaga, aby każdorazowo testy przeprowadzone po zakończeniu przez Wykonawcę realizacji każdego z etapów wdrożenia Systemu obejmowały swoim zakresem:

1) testy w zakresie funkcjonalności określonych w rozdziale 18 niniejszego OPZ;
2) testy zaimplementowanych procesów, o których mowa w rozdziale 6 niniejszego OPZ;
3) testy bezpieczeństwa;
4) testy integracyjne;
5) testy wydajnościowe.

1.1.1.6. Testy akceptacyjne powinny być przeprowadzone w środowisku w pełni odzwierciedlającym zakres funkcjonalny, w tym integracji z innymi systemami, pod kątem wydajności stanowiącym minimum 1:4 środowisko produkcyjne.

1.1.1.7. Testy powdrożeniowe powinny być przeprowadzone w środowisku testowym będącym odzwierciedleniem 1:1 środowiska produkcyjnego.

1.1.1.8. Testy powdrożeniowe będą przeprowadzane każdorazowo w siedzibie Zamawiającego lub online przy udziale przedstawiciela Zamawiającego.

1.1.1.9. Przeprowadzenie testów będzie każdorazowo zakończone sporządzeniem przez Wykonawcę raportu z testów, stanowiącego załącznik do protokołu odbioru.

1.1.1.10. Testy zostaną uznane za wykonane z wynikiem pozytywnym, jeżeli w ich trakcie nie wystąpią żadne błędy.

1.1.1.11 testy zostaną uznane za pozytywne, jeśli:

- nie będzie błędów krytycznych, bądź wysokich, bądź zostaną błędy niższych poziomów i brak ich wpływu na działanie aplikacji zostanie potwierdzony przez Wykonawcę i Zamawiającego
- albo błędy zgłoszone podczas testów zostaną naprawione we wskazanym terminie i powtórnie sprawdzone w kolejnej iteracji testów

12. Zakres szkoleń

1.1.2. Wykonawca musi zaplanować, zorganizować i przeprowadzić szkolenia obsługi Systemu dla Administratorów i Użytkowników Systemu wskazanych przez Zamawiającego.

1.1.3. Szkolenia z obsługi i funkcjonalności Systemu zostaną podzielane na bloki tematyczne dotyczące ogólnych właściwości Systemu, specyficznych właściwości poszczególnych modułów zaimplementowanych w narzędziu oraz ich działania i obsługi.

1.1.4. Oddzielne szkolenie zostanie przeprowadzenie dla Administratorów Systemu z zakresu budowy infrastruktury, działania i obsługi Systemu.

1.1.5. Wykonawca przeszkoli co najmniej 4 wskazane przez Zamawiającego osoby do roli pełnienia funkcji Administratorów.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1.1.6. Wykonawca przeszkoli co najmniej 6 wskazane przez Zamawiającego osoby do roli pełnienia funkcji Koordynatorów.

1.1.7. Wykonawca przeszkoli do 40 osób wskazanych przez Zamawiającego jako i użytkownicy Systemu, z uwzględnieniem możliwości przeszkolenia przez nie pozostałych osób w organizacji.

1.1.8. Szkolenia dla Użytkowników odbędą się w formie zdalnej za pośrednictwem MS Teams w grupach nieprzekraczających 10 osób.

1.1.9. Szkolenia odbędą się w oddzielnych terminach dla każdej z grup Użytkowników.

1.1.10. Szkolenia zostaną przeprowadzone po produkcyjnym uruchomieniu Systemu w terminach określonych w Harmonogramie.

1.1.11. Szkolenia muszą się odbywać w Dniach roboczych w godzinach od 7:00 do 15:00.

1.1.12. Wykonawca przed przeprowadzeniem szkoleń dla Użytkowników i Administratorów przedstawi ich szczegółowy program i harmonogram obejmujące: zakres tematyczny (w tym zakres tematyczny bloków, o których mowa w ust 2 powyżej, terminy, koncepcję ich przeprowadzenia) do akceptacji Zamawiającego.

1.1.13. Wykonawca przed przeprowadzeniem szkoleń przedstawi Zamawiającemu propozycję materiałów szkoleniowych.

1.1.14. Szkolenia i materiały szkoleniowe zostaną przygotowane w języku polskim,

1.1.15. Wykonawca musi dostarczyć zaakceptowane przez Zamawiającego materiały szkoleniowe uczestnikom poszczególnych szkoleń w formie elektronicznej na co najmniej 5 Dni roboczych przed rozpoczęciem szkoleń.

1.1.16. Szkolenia powinny mieć formę warsztatów prowadzonych w konwencji merytorycznego wykładu z praktycznymi ćwiczeniami polegającymi na samodzielnym wykorzystaniu funkcjonalności Systemu.

1.1.17. Osoby wyznaczone przez Wykonawcę do przeprowadzenia szkoleń muszą mieć odpowiednie kwalifikacje; tj. znać na poziomie co najmniej bardzo dobrym architekturę i działanie Systemu oraz posiadać doświadczenie w prowadzeniu szkoleń dla różnych grup Użytkowników.

1.1.18. W okresie do 5 Dni roboczych od zakończenia szkoleń Wykonawca złoży Zamawiającemu sprawozdanie z przeprowadzonych szkoleń, które musi zawierać co najmniej następujące informacje: nazwę szkolenia, datę szkolenia, nazwiska prowadzących, listę uczestników szkolenia, informację o przekazaniu materiałów szkoleniowych, informację, że szkolenie zostało zrealizowane zgodnie z przedstawionym i zaakceptowanym przez Zamawiającego programem.

1.1.19. Wykonawca wyraża zgodę na nagranie szkoleń.

13. Wymagania w zakresie Gwarancji i serwisu

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

a) Wykonawca zobowiązany jest zapewnić Zamawiającemu gwarancję dla Systemu na okres 36 miesięcy liczonych od dnia podpisania protokołu odbioru końcowego przez Zamawiającego. Wykonawca zobowiązuje się do wykonywania swoich zobowiązań z tytułu gwarancji w oparciu o gwarancję producenta Systemu lub autoryzowanego partnera producenta Systemu.

b) Serwis gwarancyjny będzie realizowany zdalnie lub w siedzibie Zamawiającego przez osoby posiadające odpowiednie uprawnienia i kwalifikacje, potwierdzone certyfikatami wystawionymi przez producenta Systemu.

c) Wszelkie czynności związane z realizowaniem praw wynikających z gwarancji, Zamawiający będzie mógł realizować w języku polskim.

d) W razie Awarii Zamawiający będzie uprawniony do dokonywania zgłoszeń za pośrednictwem następujących kanałów zgłoszeniowych:
   1) poczty elektronicznej;
   2) platformy zgłoszeniowej (serwisu, aplikacji do obsługi zgłoszeń);
   3) telefonicznie.

e) Zamawiający jest uprawniony do dokonywania zgłoszeń w trybie 24/7/365 za pośrednictwem poczty elektronicznej lub platformy zgłoszeniowej oraz telefonicznie w godzinach 7.00-18.00 w Dni Robocze.

f) Za chwilę dokonania zgłoszenia Awarii uważa się datę i godzinę jego zgłoszenia przez

g) Zamawiającego przez jeden z kanałów zgłoszeniowych, o których mowa powyżej. W przypadku zgłoszenia Awarii przez więcej niż jeden kanał zgłoszeniowy, chwilą dokonania zgłoszenia będzie data i godzina zgłoszenia wcześniejszego.

h) Wykonawca zobowiązany jest do potwierdzenia Czasu Reakcji odpowiednim automatycznym wpisem w systemie ITSM (dotyczy to również zgłoszeń składanych na adres email lub telefonicznie), nie później niż w ciągu 60 minut od czasu dokonania zgłoszenia przez Zamawiającego.

i) Dla zgłoszeń dokonanych poza zdefiniowanymi godzinami zgłoszeń (Dni robocze w godz. 7:00-18:00), czas potwierdzenia zgłoszenia rozpocznie swój bieg od godziny 7.00 następnego Dnia roboczego, następującego po dniu w którym dokonano Zgłoszenia, chyba że strony postanowią inaczej.

j) W przypadku Zgłoszeń kierowanych innym kanałem niż platforma zgłoszeniowa (e-mail, telefonicznie), wszystkie Zgłoszenia muszą być zarejestrowane przez Wykonawcę również w Aplikacji do Obsługi Zgłoszeń w sposób pozwalający na archiwizację danych o czasie i treści zgłoszenia.

k) Wykonawca zobowiązany będzie zapewnić wykonywanie zobowiązań z tytułu gwarancji zgodnie z następującymi zasadami:

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1) Awarie będą usuwane w ramach gwarancji w Dni robocze w godz. 7:00-18:00 lub w godzinach ustalonych przez Strony;
2) Wykonawca zobowiązuje się do usuwania Awarii:
   a) Awarii Krytycznych – nie później niż do 8 godzin od zgłoszenia Awarii Krytycznej;
   b) Awarii Niekrytycznych - nie później niż do 72 godzin od chwili zgłoszenia Awarii Niekrytycznej.

l) Dla zgłoszeń dokonanych poza zdefiniowanymi godzinami serwisu gwarancyjnego (Dni Robocze w godz. 7:00-18:00), Czas Naprawy Awarii rozpocznie swój bieg od godziny 7.00 następnego Dnia roboczego, następującego po dniu w którym dokonano Zgłoszenia, chyba że Strony postanowią inaczej.

m) W przypadku Awarii Krytycznej, o ile będzie dostępne zastosowanie Obejścia, Zamawiający dopuści takie Obejście do czasu jej usunięcia z jednoczesną zmianą priorytetu – z Awarii Krytycznej na Awarię Niekrytyczną - od chwili zastosowania Obejścia.

n) W przypadku Awarii Niekrytycznej o ile będzie dostępne zastosowanie Obejścia, Zamawiający dopuści takie Obejście do czasu jej usunięcia z jednoczesnym wydłużeniem Czasu Naprawy do 108 godzin.

o) Usunięcie Awarii polega na przywróceniu zgodności działania Oprogramowania z jego przeznaczeniem, Umową lub Dokumentacją.

p) Wykonawca dokona naprawy/usunięcia każdej Awarii, która nastąpi w okresie Gwarancji bez dodatkowego wynagrodzenia.

q) Umowa będzie stanowiła dokument gwarancyjny bez konieczności składania dodatkowego dokumentu na okoliczność udzielenia Gwarancji.

14. Wymagania w zakresie wsparcia technicznego oraz w zakresie dokumentacji

Wymagania dotyczące architektury rozwiązania:

1. System powinien został zbudowany w architekturze trójwarstwowej w oparciu o mikroserwisy, umożliwiając skalowanie poziome (HPA) i pionowe.
2. Preferowane uruchomienie na platformie konteneryzacji Kubernetes.
3. Zapewniony mechanizm redundancji dla bazy danych oraz zapewnienie wysokiej dostępności (HA), preferowane w modelu Active-Active.
4. Po stronie CEPiK, konieczne zbudowanie nowego API, limitującego ilość udostępnianych danych oraz będące odseparowanym interface dla nowego systemu (prace realizowane po stronie COI).

Wymagania techniczne dotyczące bezpieczeństwa:

1. API dla Integratorów:

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1.1. Dostęp do interfejsów API udostępnianych integratorom zewnętrznym musi być realizowany wyłącznie z wykorzystaniem szyfrowanych połączeń HTTPS.
1.2. System musi wymagać wzajemnego uwierzytelniania TLS (mutual TLS – mTLS) pomiędzy systemem integratora a systemem Zamawiającego.
1.3. Połączenia bez poprawnie zweryfikowanego certyfikatu klienta nie mogą być dopuszczone do komunikacji z API.
1.4. W ramach mechanizmu mTLS zarówno serwer API jak i system integratora muszą przedstawiać certyfikaty cyfrowe podczas ustanawiania połączenia TLS.
1.5. System musi umożliwiać powiązanie certyfikatu klienta z konkretnym integratorem (np. z identyfikatorem client_id)
1.6. System musi umożliwiać obsługę wielu certyfikatów przypisanych do jednego Integratora.
1.7. Certyfikaty wykorzystywane w mechanizmie mTLS muszą być zgodne ze standardem X.509.
1.8. System musi umożliwiać weryfikację certyfikatów klientów w oparciu o:
  1.8.1. listę zaufanych urzędów certyfikacji (CA),
  1.8.2. listę dopuszczonych certyfikatów klienta.
1.9. System musi umożliwiać:
  1.9.1. rejestrację certyfikatu integratora,
  1.9.2. aktualizację certyfikatu,
  1.9.3. unieważnienie certyfikatu.
1.10. System musi wspierać mechanizmy sprawdzania ważności certyfikatu, w szczególności:
  1.10.1. sprawdzanie daty ważności,
  1.10.2. obsługę list CRL lub protokołu OCSP.
1.11. Po ustanowieniu połączenia mTLS Integrator musi uzyskać token dostępu OAuth 2.0.
1.12. System musi wspierać mechanizm OAuth 2.0 Client Credentials Flow z wykorzystaniem mTLS jako metody uwierzytelniania klienta.
1.13. System musi implementować mechanizm uwierzytelniania oraz autoryzacji z wykorzystaniem tokenów JWT (JSON Web Token) zgodnych ze specyfikacją RFC 7519. Mechanizm uwierzytelniania musi wspierać architekturę stateless, w której informacje o sesji użytkownika są przechowywane w tokenie.
1.14. Tokeny JWT muszą być podpisywane kryptograficznie (rekomendowane RS256),
1.15. System musi obsługiwać mechanizm refresh tokenów umożliwiających odnowienie tokenu dostępowego.
1.16. System musi umożliwiać powiązanie tokenu JWT z certyfikatem klienta wykorzystywanym w połączeniu mTLS.
1.17. Token JWT powinien zawierać identyfikator klienta (client_id) odpowiadający certyfikatowi użytemu w połączeniu TLS.
1.18. System musi uniemożliwiać użycie tokenu przez innego klienta niż ten, który uzyskał go przy użyciu danego certyfikatu.
1.19. System musi implementować mechanizm kontroli dostępu oparty o role (RBAC – Role Based Access Control) w celu zarządzania uprawnieniami Integratorów korzystających z API.
1.20. Dostęp do zasobów API musi być kontrolowany na podstawie:
  1.20.1. tożsamości klienta (client_id),
  1.20.2. przypisanych ról,
  1.20.3. zakresów uprawnień (scope) zawartych w tokenie JWT.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1.21. Każdy Integrator korzystający z API musi posiadać przypisaną co najmniej jedną rolę określającą zakres dostępnych operacji.
1.22. System musi zapewniać:
  1.22.1. stosowanie protokołu TLS w wersji 1.2 lub wyższej,
  1.22.2. stosowanie silnych zestawów szyfrów kryptograficznych,
  1.22.3. weryfikację certyfikatów klientów podczas zestawiania połączenia TLS,
  1.22.4. odrzucanie połączeń z nieznanych lub unieważnionych certyfikatów.
1.23. System musi rejestrować w logach audytowych wszystkie zdarzenia związane z uwierzytelnianiem, autoryzacją oraz dostępem do API udostępnianego Integratorom.
1.24. System musi umożliwiać integrację z narzędziami monitorowania bezpieczeństwa (SIEM) w celu wykrywania:
  1.24.1. wielokrotnych nieudanych prób uwierzytelnienia,
  1.24.2. prób użycia nieważnych lub zmodyfikowanych tokenów,
  1.24.3. prób dostępu z nieautoryzowanych adresów IP,
  1.24.4. nietypowej liczby wywołań API przez Integratora.
  1.24.5. Logi powinny być zapisywane w formacie umożliwiającym ich automatyczną analizę, np.: JSON, CEF, syslog.
1.25. System musi zapewniać:
  1.25.1. ochronę logów przed modyfikacją i usunięciem przez użytkowników aplikacyjnych,
  1.25.2. możliwość wykrycia prób manipulacji logami,
  1.25.3. synchronizację czasu systemowego (np. NTP), aby zapewnić spójność znaczników czasu.
1.26. System musi zapewniać walidację wszystkich danych wejściowych przekazywanych do API, w tym:
  1.26.1. parametrów zapytań (query parameters),
  1.26.2. nagłówków HTTP,
  1.26.3. danych przesyłanych w treści żądania (payload),
  1.26.4. załączników przesyłanych przez Integratorów.
1.27. Walidacja musi obejmować w szczególności:
  1.27.1. sprawdzenie typu danych,
  1.27.2. weryfikację długości danych,
  1.27.3. weryfikację formatów danych (np. identyfikatory, daty),
  1.27.4. weryfikację formatu załączanego pliku,
  1.27.5. skanowanie antywirusowe dodawanych załączników,
  1.27.6. odrzucenie nieoczekiwanych parametrów,
  1.27.7. odrzucenie danych zawierających niedozwolone znaki lub struktury.
1.28. W przypadku niepoprawnych danych API musi zwrócić odpowiedni kod błędu HTTP (np. 400 Bad Request).
1.29. API musi umożliwiać przesyłanie załączników przez Integratorów w sposób bezpieczny. W szczególności system musi zapewniać:
  1.29.1. weryfikację typu pliku (MIME type),
  1.29.2. weryfikację rozszerzenia pliku,
  1.29.3. weryfikację maksymalnego rozmiaru pliku,
  1.29.4. weryfikację zgodności typu pliku z deklarowanym formatem,
  1.29.5. skanowanie AV importowanych załączników,

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1.29.6. odrzucenie plików niespełniających wymagań bezpieczeństwa.

1.30. System musi umożliwiać konfigurację dopuszczalnych formatów plików, np.:
1.30.1. PDF,
1.30.2. XML,
1.30.3. JSON,
1.30.4. CSV,
1.30.5. JPG/PNG.

1.31. System musi umożliwiać konfigurowanie maksymalnego dopuszczalnego rozmiar pliku załącznika.

1.32. API dla Integratora musi być zaprojektowane i zaimplementowane zgodnie z dobrymi praktykami bezpieczeństwa aplikacji, w szczególności z uwzględnieniem zaleceń OWASP Top 10.

1.33. System musi implementować mechanizm rate limiting, który ogranicza liczbę zapytań API wykonywanych przez Integratora w określonym czasie. Mechanizm ten powinien umożliwiać:
1.33.1. ograniczenie liczby zapytań na klienta (client_id),
1.33.2. ograniczenie liczby zapytań z jednego adresu IP,
1.33.3. konfigurację progów zapytań w jednostce czasu (np. na minutę).
1.33.4. W przypadku przekroczenia limitu API musi zwrócić kod odpowiedz HTTPi 429 Too Many Requests,

1.34. System musi rejestrować zdarzenia bezpieczeństwa związane z jego użyciem, w szczególności:
1.34.1. przesyłanie załączników,
1.34.2. odrzucenie pliku z powodu zagrożenia,
1.34.3. przekroczenie limitów zapytań,
1.34.4. próby ataków (np. blokada konta po kilku nieudanych próbach logowania).

1.35. Logi te muszą być przekazywane do systemu centralnego logowania oraz systemu monitorowania bezpieczeństwa wskazanego przez Zamawiającego.

2. GUI dla Pracowników (administracyjne)
   a. Interfejs administracyjny systemu (GUI dla Pracownika) musi być przeznaczony wyłącznie dla uprawnionych administratorów systemu.
   b. Dostęp do GUI musi być ograniczony wyłącznie do użytkowników znajdujących się w sieci wewnętrznej. W szczególności dostęp musi być możliwy z sieci wewnętrznej organizacji lub z sieci zewnętrznej wyłącznie poprzez bezpieczne połączenie VPN.
   c. GUI administracyjne nie może być bezpośrednio dostępne z publicznej sieci Internet.
   d. System musi zapewniać silne uwierzytelnianie użytkowników,
   e. Uwierzytelnianie musi obejmować co najmniej dwa składniki (2FA – Two-Factor Authentication).
   f. Dopuszczalne metody drugiego składnika uwierzytelniania obejmują w szczególności:
      i. aplikacje generujące jednorazowe kody (TOTP),
      ii. sprzętowe tokeny uwierzytelniające,
      iii. karty kryptograficzne z certyfikatem użytkownika,
      iv. inne mechanizmy zgodne z polityką bezpieczeństwa Zamawiającego.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

g. System powinien umożliwiać integrację z infrastrukturą klucza publicznego (PKI) w celu wykorzystania certyfikatów użytkowników.
h. System musi wymuszać stosowanie polityki haseł zgodnej z dobrymi praktykami bezpieczeństwa.
i. Hasła użytkowników muszą być przechowywane w systemie wyłącznie w postaci bezpiecznych skrótów kryptograficznych.
j. System musi zostać zaprojektowany oraz zaimplementowany zgodnie z uznanymi standardami bezpieczeństwa aplikacji. W szczególności wymagane jest stosowanie dobrych praktyk bezpieczeństwa opisanych w standardach: OWASP Top 10 czy też OWASP Application Security Verification Standard.
k. System powinien spełniać wymagania co najmniej poziomu 2 (L2) standardu OWASP ASVS, który jest przeznaczony dla aplikacji przetwarzających dane o podwyższonym poziomie wrażliwości.
l. System musi implementować mechanizmy ochrony przed próbami nieautoryzowanego logowania. W szczególności system musi zapewniać:
    i. ograniczenie liczby nieudanych prób logowania,
    ii. automatyczną blokadę konta po określonej liczbie błędnych prób logowania,
    iii. możliwość odblokowania konta przez administratora lub po określonym czasie.
    iv. Każda próba logowania, zarówno udana jak i nieudana, musi być rejestrowana w logach audytowych.
m. System musi odkładać logi audytowe obejmujące zdarzenia związane z korzystaniem z GUI administracyjnego. W szczególności logowane muszą być:
    i. próby logowania (udane i nieudane),
    ii. zmiany konfiguracji systemu,
    iii. operacje administracyjne na danych,
    iv. zmiany uprawnień użytkowników,
    v. blokady i odblokowania kont.
n. Logi audytowe muszą być chronione przed modyfikacją oraz dostępne wyłącznie dla uprawnionych administratorów.

o. System musi stosować mechanizm kontroli dostępu oparty na rolach (RBAC).
    i. Uprawnienia użytkowników muszą być nadawane na podstawie przypisanych ról.
    ii. System musi umożliwiać ograniczenie dostępu do:
        1. poszczególnych funkcji administracyjnych,
        2. określonych modułów systemu,
        3. określonych operacji (np. odczyt, modyfikacja, usuwanie danych).
        4. System musi stosować zasadę minimalnych uprawnień (least privilege).
p. System musi zapewniać walidację wszystkich danych wprowadzanych przez użytkowników w GUI administracyjnym. Walidacja musi obejmować w szczególności:
    i. weryfikację typu danych,
    ii. kontrolę długości danych,
    iii. weryfikację poprawności formatów,
    iv. odrzucenie niedozwolonych znaków lub struktur danych.
q. Mechanizmy walidacji muszą chronić system przed typowymi podatnościami aplikacyjnymi,

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

r. Komunikacja pomiędzy przeglądarką użytkownika a systemem musi być realizowana wyłącznie z wykorzystaniem bezpiecznego protokołu HTTPS. System musi stosować aktualne i bezpieczne konfiguracje protokołu TLS.
s. System musi implementować mechanizm uwierzytelniania oraz autoryzacji z wykorzystaniem tokenów JWT (JSON Web Token) zgodnych ze specyfikacją RFC 7519. W szczególności wymagane jest:
   i. stosowanie tokenów sesyjnych posiadających ograniczony czas ważności,
   ii. automatyczne wygaśnięcie sesji po określonym czasie bezczynności użytkownika,
   iii. możliwość natychmiastowego unieważnienia sesji po wylogowaniu użytkownika,
   iv. wymuszenie ponownego uwierzytelnienia użytkownika po wygaśnięciu sesji.
t. Tokeny sesyjne muszą być przekazywane wyłącznie szyfrowanym kanałem HTTPS oraz przechowywane po stronie klienta w sposób ograniczający ryzyko ich przechwycenia lub nieautoryzowanego użycia.

3. System powinien umożliwiać integrację z systemami bezpieczeństwa, np.:
   a. WAF,
   b. API Gateway,
   c. Systemami monitorowania bezpieczeństwa (SIEM).
4. API musi być zaprojektowane i zaimplementowane zgodnie z dobrymi praktykami bezpieczeństwa aplikacji, w szczególności z uwzględnieniem zaleceń **OWASP Top 10**.
5. System musi zostać zaprojektowany w architekturze mikroserwisowej, zapewniającej logiczną separację komponentów odpowiedzialnych za różne obszary funkcjonalne oraz różne typy integracji systemowych. Architektura systemu powinna umożliwiać niezależny rozwój, skalowanie oraz wdrażanie poszczególnych komponentów systemu.W szczególności wymagane jest wydzielenie odrębnych mikroserwisów odpowiedzialnych za obsługę różnych kategorii interfejsów komunikacyjnych.
6. System musi zapewniać logiczną oraz architektoniczną separację interfejsów API przeznaczonych dla użytkowników wewnętrznych (GUI dla Pracowników) oraz dla systemów zewnętrznych (Integratorów). W szczególności wymagane jest zastosowanie odrębnych mikroserwisów udostępniających API dla tych dwóch kategorii odbiorców:

   a. mikroserwisu API dla Integratorów, przeznaczonego do komunikacji z systemami zewnętrznymi,
   b. mikroserwisu API dla GUI, wykorzystywanego przez aplikację administracyjną systemu.

7. API dla Integratorów musi być odseparowane od API wykorzystywanego przez GUI zarówno na poziomie logicznym, jak i infrastrukturalnym.
8. Architektura systemu musi zapewniać:
   a. brak bezpośredniego dostępu Integratorów do API przeznaczonego dla frontendów administracyjnych,
   b. brak możliwości korzystania przez GUI dla Pracowników z API przeznaczonego dla Integratorów,
   c. niezależne skalowanie oraz rozwój obu interfejsów API.
9. System musi posiadać dedykowany mikroserwis integracyjny przeznaczony do komunikacji z systemami Zamawiającego. Mikroserwis ten powinien pełnić rolę warstwy integracyjnej umożliwiającej:

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

a. wymianę danych z systemami Zamawiającego,
b. realizację procesów integracyjnych,
c. transformację i mapowanie danych pomiędzy systemami.

10. Systemy wewnętrzne Zamawiającego komunikują się z systemem Obsługi wniosków wyłącznie poprzez dedykowany mikroserwis integracyjny.
11. Mikroserwis integracyjny musi być odseparowany od pozostałych interfejsów systemu (API udostępnianego Integratorom zewnętrznym, API wykorzystywanego przez GUI administracyjne). Separacja ta musi być realizowana zarówno na poziomie architektury aplikacyjnej, jak i infrastruktury sieciowej.
12. Mikroserwis integracyjny musi być dostępny wyłącznie w sieci wewnętrznej,
13. Mikroserwis integracyjny nie może być eksponowany do sieci publicznej ani poprzez publiczne API Gateway.
14. Komunikacja pomiędzy budowanym systemem a systemami wewnętrznymi Zamawiającego musi wykorzystywać wymagane przez Zamawiającego mechanizmy uwierzytelniania i autoryzacji, w szczególności mechanizmy oparte na silnym uwierzytelnianiu usług (np. certyfikaty, tokeny dostępu, podpisy kryptograficzne lub inne wskazane przez Zamawiającego standardy).
15. Architektura rozwiązania musi umożliwiać dostosowanie sposobu uwierzytelniania i autoryzacji do wymagań systemu Zamawiającego bez konieczności ingerencji w pozostałe komponenty systemu.
16. System musi zapewniać szyfrowanie danych przechowywanych w bazie danych (data at rest), stosować uznane i bezpieczne algorytmy kryptograficzne oraz separację kluczy kryptograficznych od przechowywanych danych.
17. System musi zapewniać bezpieczne zarządzanie kluczami kryptograficznymi (przechowywanie kluczy HSM/KMS, kontrolę dostępu do kluczy, możliwość rotacji kluczy kryptograficznych),
18. Dane osobowe zwracane w odpowiedzi na wniosek Integratora muszą być dodatkowo przechowywane w bazie danych w postaci zaszyfrowanej przy użyciu kryptografii asymetrycznej PGP z wykorzystaniem kluczy publicznych Integratorów. Szyfrowanie musi być realizowane z wykorzystaniem standardu PGP lub kompatybilnego standardu OpenPGP. Zaszyfrowane dane powinny być możliwe do odszyfrowania wyłącznie przez Integratora posiadającego właściwy klucz prywatny.
19. System musi umożliwiać zarządzanie kluczami publicznymi Integratorów (klucze PGP) wykorzystywanymi do szyfrowania danych. Wymagania funkcjonalne do zarządzania kluczami PGP:
    a. rejestrowanie klucza publicznego Integratora w systemie,
    b. weryfikacja poprawności klucza publicznego,
    c. możliwość aktualizacji (rotacji) klucza publicznego,
    d. możliwość unieważnienia klucza publicznego.
20. Klucze publiczne Integratorów muszą być przechowywane w sposób zapewniający ich integralność i ochronę przed nieautoryzowaną modyfikacją.
21. IODO powinien wskazać dodatkowe wymagania w modelu SaaS.

Pozostałe wymagania techniczne

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1. kod aplikacji zaprojektowany przy stosowaniu mechanizmów SOLID oraz CleanCode
2. zastosowanie oprogramowania co najmniej w wersjach:
   Java 21LTS (preferowana 25LTS),
   Springboot 3.2,
   Spring Framework 6.1,
   Angular 19
   PostrgreSQL 17

15. Przedmiot zamówienia w ramach opcji – warunki świadczenia godzin eksperckich:

a. Zamawiający jest uprawniony do zlecenia Wykonawcy w ramach opcji świadczenia Godzin eksperckich przez certyfikowanego przez producenta inżyniera w Dni robocze, w zakresie konsultacji, rozwiania wątpliwości lub rozwiązania bieżących problemów Zamawiającego z obsługi przedmiotu zamówienia, w liczbie do 100[5] roboczogodzin w ramach podpisanej umowy.
   2. W zakresie przedmiotu opcji, rozliczenie wynagrodzenia Wykonawcy będzie następować w oparciu na stawce godzinowej pracy konsultanta, w ramach puli 100 roboczogodzin, z możliwością wykorzystania do końca okresu obowiązywania umowy
b. Osoby realizujące usługi w ramach Godzin eksperckich muszą legitymować się certyfikatem producenta lub akredytowanego przedstawiciela producenta oferowanego rozwiązania potwierdzającym wiedzę techniczną w zakresie przedmiotu Zamówienia na poziomie eksperckim oraz muszą posiadać dostęp do bazy wiedzy tego producenta.
c. W ramach usług realizowanych jako Godziny eksperckie będą świadczone na Zlecenie Zamawiającego m.in.:
   - Konsultacje i wsparcie w zakresie rozbudowy, tuningu i konfiguracji przedmiotu zamówienia;
   - Szkolenia i warsztaty w zakresie przedmiotu Zamówienia
d. Opracowanie i dostarczenie dokumentów, procedur i instrukcji, dot. m.in.:
   - instalacji, konfiguracji oraz parametryzacji przedmiotu zamówienia,
   - aktualizacji i wdrażania poprawek do przedmiotu zamówienia.
e. Wsparcie Zamawiającego w użytkowaniu przedmiotu zamówienia – zarówno techniczne, jak i merytoryczne oraz implementacja nowych funkcjonalności lub modyfikacja już skonfigurowanych.
f. Wsparcie Zamawiającego w użytkowaniu przedmiotu zamówienia – zarówno techniczne, jak i merytoryczne oraz implementacja nowych funkcjonalności lub modyfikacja już skonfigurowanych.
g. Wsparcie Zamawiającego w użytkowaniu przedmiotu zamówienia oraz wsparcie w planowanych pracach serwisowych, a w szczególności:
   - przeprowadzenie standardowych prac serwisowych,
   - przeprowadzanie aktualizacji,
   - weryfikacja poprawności konfiguracji.
h. Skorzystanie z opcji jest uprawnieniem Zamawiającego. Zamawiający nie zobowiązuje się w żaden sposób do skorzystania z opcji. Nieskorzystanie przez Zamawiającego z

[5] Ilość w celu wyłącznie wyceny

opcji nie rodzi po stronie Wykonawcy jakichkolwiek roszczeń w stosunku do Zamawiającego.

16. Wymagania w zakresie funkcjonalności Systemu

I.	Ogólne wymagania Systemu	
1.	**Wymagania funkcjonalne**	Stanowi załącznik do OPZ – „wymagania funkcjonalne”
2.	**Wymagania w zakresie bezpieczeństwa**	Zgodnie z ustaleniami – dodatkowe uwagi do OPZ ze strony DCB: 1. Sesja do COI uwierzytelniona na więcej niż jednym składniku 2. Sesja do COI powinna wykorzystywać certyfikat kliencki 3. Wymiana plików z instytucjami zewnętrznymi, powinna zakładać obowiązek dostarczenia do COI klucza publicznego instytucji – klucz ten będzie używany do zaszyfrowania pliku wystawianego do instytucji na nowo budowanym systemie 4. Założenie jest takie, że dane oczekujące na pobranie przez instytucję (przygotowane w cepik), są zawsze zaszyfrowane kluczem adresata. 5. Po pobraniu, pliki te powinny zostać usunięte z tego nowego systemu. 6. System ten, musi dostarczyć mechanizm zgodnego z RODO systemu umożliwiającego rozliczenie faktycznego udostępnienia danych osobowych (do potwierdzenia z IODO warunki) 7. Zakładamy, że nowy mechanizm jest docelowy i po okresie przejściowym (integracja zainteresowanych) należy odejść od starego, całkowicie ręcznego systemu przetwarzania. 8. Nowy system nie powinien dopuszczać załączania niezależnych dokumentów PDF (zresztą jakichkolwiek zew. Dokumentów) 9. Dostęp tylko i wyłącznie przez protokoły szyfrowane. Logi audytowe muszą spełniać wszystkie kryteria konsystencji i rozliczalności
3.	**Wymagania dla dodatkowej funkcji automatyzującej proces weryfikacji (z wykorzystaniem np. funkcji OCR) danych i załączników w ramach wniosków**	Celem usługi jest wsparcie urzędnika w ocenie i analizie poprawności złożonej dokumentacji poprzez automatyczną analizę oraz weryfikację danych przesłanych przez wnioskodawcę. Analiza obejmuje porównywanie i weryfikację danych w jednostkowej sprawie, co umożliwi wykrywanie niezgodności, błędów a tym samym ocenę poprawności złożonego wniosku. System powinien umożliwiać automatyczne rozpoznawanie tekstu ze zdjęć oraz skanów dokumentów, automatyczne wykrywanie obszarów tekstowych, rozpoznawanie tekstu w języku polskim

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

	obsługiwanych w procesie obsługowym	oraz obsługę formatów m.in. JPG, PDF, dane w systemie. Wymagana jest automatyczna analiza i porównywanie danych z różnych źródeł, w tym wykrywanie niezgodności i różnic oraz generowanie statusów: np. „zgodne", „niezgodne" oraz „wymaga sprawdzenia". Wymagana dokładność rozpoznawania tekstu (OCR) powinna wynosić co najmniej 90%. System musi umożliwiać jednoczesne przetwarzanie wielu dokumentów, a maksymalny czas analizy pojedynczego dokumentu powinien wynosić do kilku sekund. System musi spełniać wymogi RODO, kontrolę dostępu użytkowników oraz odpowiednie mechanizmy bezpieczeństwa. Powinien zawierać panel administracyjny (może być połączony z panelem głównym Systemu) umożliwiający zarządzanie użytkownikami, konfigurację reguł, przegląd wyników OCR, raportowanie błędów oraz analizę statystyk. System powinien umożliwiać generowanie raportów dotyczących liczby przetworzonych dokumentów, liczby wykrytych błędów, liczby spraw wymagających ręcznej weryfikacji oraz skuteczności automatycznej weryfikacji. Dodatkowo system musi być skalowalny wraz ze wzrostem liczby przetwarzanych dokumentów.

17. Wymagania dotyczące odbioru

1. Wykonawca dostarczy Zamawiającemu Dokumentację, w języku polskim, w wersji elektronicznej.
2. Ponadto Wykonawca dostarczy Zamawiającemu:
   1) nośniki z wersją instalacyjną Oprogramowania o ile nie są dostępne w formie elektronicznej,
   2) wszystkie wymagane klucze licencyjne i aktywacyjne;
   3) umowę licencyjną (w wersji papierowej lub elektronicznej), zawierająca warunki licencjonowania danego Oprogramowania określone przez producenta;
   4) aktualne zestawienie w formacie xls wszystkich dostarczonych pozycji w zakresie Oprogramowania zawierającego informacje m.in. oznaczenie producenta (tzw. part numer), pełna nazwa produktu, metryka licencyjna, wersja i edycja oprogramowania, rodzaj Licencji, okres obowiązywania Licencji, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto, zgodnie z zapisami zawartymi w Ofercie.
3. Wdrożenie Systemu stanowiącego przedmiot zamówienia będzie realizowane i odbierane etapowo. Potwierdzeniem odbioru przedmiotu zamówienia będą podpisane przez Strony bez zastrzeżeń protokoły odbioru etapów, w tym produktów prac poszczególnych etapów wskazanych w Harmonogramie, których wzór określono w Załączniku do Umowy.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

4. Odbiór produktów prac poszczególnych etapów realizacji przedmiotu zamówienia nastąpi każdorazowo w Dniach roboczych w sposób ustalony i zaakceptowany uprzednio przez Strony
5. W ramach procedury odbioru Zamawiający dokona weryfikacji, czy przedmiot odbioru spełnia wymagania określone w Umowie oraz w OPZ.
6. Protokół odbioru produktów prac danego etapu zostanie podpisany przez Zamawiającego bez zastrzeżeń pod warunkiem pozytywnego zakończenia weryfikacji ich zgodności z wymaganiami wskazanymi w Umowie oraz OPZ.
7. Weryfikacja w zakresie wdrożenia zostanie przeprowadzona w drodze testów akceptacyjnych i przeprowadzonych przez Zamawiającego w oparciu o scenariusze testowe dostarczone przez Wykonawcę.
8. Wykonawca zgłosi każdorazowo Zamawiającemu gotowość do przeprowadzenia odbioru w drodze przeprowadzenia testów akceptacyjnych, poprzedzonych pozytywnie zakończonymi testami akceptacyjnymi i powdrożeniowymi przeprowadzonymi przez Wykonawcę (potwierdzonymi w przekazanym Zamawiającemu raporcie) w terminie wynikającym z Harmonogramu w oparciu o scenariusz, o których mowa w rozdziale 12.
9. W przypadku zgłoszenia przez Zamawiającego Wad w produktach wykonanych w ramach poszczególnych etapów lub innej niezgodności tych Produktów z wymaganiami wskazanymi w Umowie i OPZ, odbiór nastąpi po stwierdzeniu przez Zamawiającego usunięcia wszystkich Wad lub przyczyn niezgodności produktów z wymaganiami wskazanymi w Umowie oraz OPZ. W takim przypadku procedurę odbioru powtarza się, aż do czasu dokonania przez Zamawiającego odbioru produktów prac danego etapu bez zastrzeżeń.
10. W przypadku nieuwzględnienia przez Wykonawcę uwag lub zastrzeżeń, zgłoszonych przez Zamawiającego, w wyznaczonym terminie lub uwzględnienia ich niezgodnie z tym, co zgłosił Zamawiający, Zamawiający ma prawo do odstąpienia od Umowy w całości lub w części z przyczyn leżących po stronie Wykonawcy.
11. Terminem wykonania etapu będzie termin wskazany w podpisanym bez zastrzeżeń przez Zamawiającego Protokole odbioru danego etapu.
12. Po zakończeniu i odbiorze produktów prac wszystkich etapów w ramach procedury odbioru Zamawiający dokona końcowej weryfikacji zgodności całości produktu podstawowego przedmiotu zamówienia z wymaganiami opisanymi w Umowie oraz OPZ.
13. Protokół końcowy odbioru systemu stanowiącego przedmiot zamówienia podstawowego zostanie podpisany bez zastrzeżeń przez Zamawiającego pod warunkiem pozytywnego zakończenia weryfikacji jego zgodności z wymaganiami wskazanymi w Umowie i OPZ.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

14. Dokonanie odbioru przez Zamawiającego nie zwalnia Wykonawcy od odpowiedzialności za Wady lub niezgodności produktów danego Etapu lub całości przedmiotu zamówienia w stosunku do Umowy i OPZ, jeżeli były one ukryte.
15. Zamawiający zastrzega sobie prawo do dopuszczenia do udziału w czynnościach odbiorowych osób trzecich jako ekspertów, specjalistów lub biegłych.
16. Wykonawca nie jest uprawniony do wystawienia jednostronnego protokołu odbioru.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl