Załącznik nr 2. Szczegółowy opis zapytania o informację

Informacje ogólne

Wychodząc naprzeciw oczekiwaniom rynkowym chcemy w najbliższej przyszłości umożliwić naszym oraz potencjalnym klientom zawieranie umów w formie w pełni elektronicznej wykluczając przesyłanie umów w formie papierowej. Dodatkowo planowana jest budowa platformy, dzięki której do zalogowania się do wszystkich aplikacji Enei służył będzie jeden login i hasło. Aby móc te procesy w pełni zastosować koniecznym jest uzyskanie potwierdzenia tożsamości w podmiocie zewnętrznym, aby mieć pewność, że osoba rejestrująca konto lub zawierająca umowę jest tą osobą za kogo się podaje.

Podstawowe wymagania

Przedmiotem zamówienia jest zakup usługi potwierdzania tożsamości **mojeID,** które pozwala na bezpieczną weryfikację danych klienta za pomocą bankowości internetowej.
Usługa musi mieć możliwość potwierdzenia, że osoba składająca wniosek/podpisująca umowę jest tą, za którą się podaje lub przekazania informacji, że dane wnioskującego są niezgodne z tymi, które są na umowie lub których dotyczy rejestracja konta. Zamawiający zakłada, że elementami weryfikującymi dane danej osoby mają być co najmniej jej imiona, nazwisko oraz PESEL. Weryfikacja musi odbywać się zgodnie z obowiązującymi przepisami prawnymi, w tym szczególności tymi związanymi z przetwarzaniem danych oraz za zgodą dokonującego weryfikacji. Weryfikacja pozytywna lub negatywna powinna wystąpić niezwłocznie po przekazaniu danych przez Użytkownika. Informację o statusie weryfikacji otrzymać ma zarówno Użytkownik jak i Zamawiający.

Szacowana roczna liczba potwierdzeń tożsamości za pośrednictwem narzędzia to 22 tysiące.

Usługa weryfikacji musi odbywać się poprzez wykorzystanie środka identyfikacji elektronicznej zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, zwane eIDAS.

Wymagania techniczne

W ramach realizacji potwierdzania tożsamości zakładamy, że usługa weryfikacji ma możliwość zintegrowania z systemami Zamawiającego na podstawie wystawienia protokołu REST API. Serwer, który udostępnia funkcjonalności do potwierdzania tożsamości jest zaufanym pośrednikiem pomiędzy systemem Zamawiającego, a stacją roboczą lub smartfonem Użytkownika i zapewnia bezpieczne przekazanie danych do systemu Zamawiającego. Zamawiający wymaga aby system do potwierdzania tożsamości komunikował się z systemem informatycznym Zamawiającego oraz z aplikacją wykonywaną na smartfonie użytkownika przy użyciu protokołu HTTPS.
Komponenty systemu informatycznego wykorzystywanego do potwierdzania tożsamości powinny być zabezpieczane przez następujące moduły:

- WAF (ang. Web Application Firewall) – moduł ochrony aplikacji webowych, który analizuje ruch przychodzący do serwerów i w razie wykrycia treści/zachowań niebezpiecznych lub podejrzanych za niebezpieczne blokuje je i przekazuje do SIEM

- AV (ang. AntiVirus) – moduł ochrony antywirusowej, który oprócz monitorowania przetwarzanych treści (plików) na serwerze realizuje również funkcje:
  - ✓ IDS, HIDS (ang. Intrusion Detection System, Host-based Intrusion Detection System) – moduł wykrywania włamań, moduł wykrywania intruzów,
  - ✓ IPS (ang. Intrusion Prevention System) – moduł zapobiegania włamaniom,
  - ✓ o Log inspection – moduł nadzorowania logów.
- SIEM (ang. Security Information and Event Management) – moduł zarządzania informacjami dot. bezpieczeństwa oraz zdarzeń. Pozwala na zbieranie informacji, zdarzeń, logów z różnych źródeł, a następnie po przetworzeniu, prezentowanie ich oraz raportowanie.

Zamawiający zakłada, że umowa z potencjalnym Wykonawcą zostanie zawarta na 5 lat.

Serwis i utrzymanie

Kategoria	Parametry
Dostępność Usług	97% dostępności w skali miesiąca (liczonej w trybie 24h/7))
Czas na podjęcie błędu krytycznego	1h przez 7 dni w tygodniu
Czas na naprawę błędu krytycznego	4h przez 7 dni w tygodniu
Czas na podjęcie błędu normalnego	8h w dni robocze
Czas na naprawę błędu normalnego	24h w dni robocze

Dostawca zobowiązuje się naprawiać błędy krytyczne i normalne Systemu zgodnie z tabelą powyżej.

Błąd krytyczny to błąd uniemożliwiający korzystanie z Systemu przez wszystkich Użytkowników lub uniemożliwiający całkowicie korzystanie z nich przez Zamawiającego, np. serwer nie odpowiada.

Błąd normalny to błąd utrudniający korzystanie z Systemu przez wszystkich użytkowników lub utrudniający korzystanie z nich przez Zamawiającego np. System działa zbyt wolno.

Spodziewana zwartość odpowiedzi na zapytanie

1. Przedstawienie kosztów niezbędnych do realizacji:
   - całego zadnia (kosztów przygotowania i wdrożenia)

- opłat stałych (ponoszonych cyklicznie za utrzymanie sytemu)
- opłat zmiennych (związanych z potwierdzeniem tożsamości jedną z możliwych metod)

2. Przedstawienie szczegółowego opisu koncepcji technicznej rozwiązania
3. Przedstawienie harmonogramu prac (w tygodniach) z uwzględnieniem:
   - przygotowania dokumentacji/koncepcji rozwiązania
   - prac konfiguracyjnych i instalacyjnych na potrzeby testów
   - przeprowadzenia testów w tym naprawa błędów wynikających z testów bezpieczeństwa
   - przeprowadzenia warsztatów i szkoleń
   - prac konfiguracyjnych i instalacyjnych na potrzeby uruchomienia produkcyjnego
   - przygotowania dokumentacji powykonawczej
   - utrzymania usługi na czas obowiązywania