Załącznik nr 1 do rozeznania rynku

Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest rozbudowa środowiska sieciowych modułów kryptograficznych HSM (Hardware Security Module) w Ministerstwie Sprawiedliwości.
2. Zamawiający posiada obecnie środowisko w ramach, którego uruchomiony jest 1 moduł kryptograficzny HSM Thales nShield Connect+ 500+ wraz z 7 licencjami klienckimi.
3. Przedmiot zamówienia obejmuje:
   WARIANT 1 – formularz cenowy z załącznika 2a:
   a) Dostawę, montaż, konfigurację instalację, uruchomienie i wdrożenie 1 modułu kryptograficznego HSM Thales nShield Connect+ 500+ wraz z 3 licencjami klienckimi.
   b) Odnowienie wsparcia technicznego dla HSM Thales nShield Connect+ 500+ będącego w posiadaniu Ministerstwa Sprawiedliwości.
   c) Świadczenie usługi weryfikacji i aktualizacji obu urządzeń w celu dostosowania i przygotowania ich do wykorzystywania w procesie tworzenia pieczęci kwalifikowanej zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 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. Aktualizacja urządzeń ma przede wszystkim doprowadzić do podniesienia wersji oprogramowania obu urządzeń do najnowszej wersji zgodnej z listą QSCD (Qualified signature creation device).
   d) Połączenie urządzenia posiadanego przez Zamawiającego oraz dostarczonego urządzenia w klaster o wysokiej dostępności (High Availability) działający w trybie active-passive. Specyfika klastra musi umożliwić wykorzystanie na urządzeniu będącym w trybie aktywnym 10 licencji klienckich, a urządzenie będące w trybie pasywnym musi posiadać możliwość przejęcia zadań wraz z obsługą licencji klienckich na wypadek awarii (failover).
   e) Dostawę, usługę osadzenia oraz konfiguracji certyfikatu pieczęci kwalifikowanej w zbudowanym klastrze HSM. Certyfikat musi być ważny przez okres 24 miesięcy od daty uruchomienia klastra modułów kryptograficznych.
   f) Zapewnienie wsparcia technicznego dla obu urządzeń na okres 12 miesięcy od dnia dostarczenia nowego urządzenia do Ministerstwa Sprawiedliwości. Posiadane przez Ministerstwo Sprawiedliwości urządzenie HSM Thales nShield Connect+ 500+ nie posiada obecnie wsparcia technicznego.

   WARIANT 2 – formularz cenowy z załącznika 2b:
   a) Dostawę, montaż, konfigurację instalację, uruchomienie i wdrożenie 2 modułów kryptograficznych HSM wraz z 10 licencjami klienckimi wraz ze świadczeniem usługi weryfikacji i aktualizacji obu urządzeń w celu dostosowania i przygotowania ich do wykorzystywania w procesie tworzenia pieczęci kwalifikowanej zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady

(UE) 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. Aktualizacja urządzeń ma przede wszystkim doprowadzić do podniesienia wersji oprogramowania obu urządzeń do najnowszej wersji zgodnej z listą QSCD (Qualified signature creation device).

b) Połączenie dostarczonych urządzeń w klaster o wysokiej dostępności (High Availability) działający w trybie active-passive. Specyfika klastra musi umożliwić wykorzystanie na urządzeniu będącym w trybie aktywnym 10 licencji klienckich, a urządzenie będące w trybie pasywnym musi posiadać możliwość przejęcia zadań wraz z obsługą licencji klienckich na wypadek awarii (failover).
c) Migrację na nowostworzony klaster centrów certyfikacji z urządzenia HSM Thales nShield Connect+ 500+ będącego w posiadaniu Ministerstwa Sprawiedliwości wykorzystującego 7 licencji.
d) Dostawę, usługę osadzenia oraz konfiguracji certyfikatu pieczęci kwalifikowanej w zbudowanym klastrze HSM. Certyfikat musi być ważny przez okres 24 miesięcy od daty uruchomienia klastra modułów kryptograficznych.
e) Zapewnienie wsparcia technicznego dla obu urządzeń na okres 12 miesięcy od dnia ich dostarczenia do Ministerstwa Sprawiedliwości.

2. Wsparcie techniczne polegać ma przede wszystkim na:
   a) udostępnianiu Zamawiającemu aktualizacji oprogramowania do wersji najnowszej,
   b) udostępnieniu Zamawiającemu nowego oprogramowania (dystrybuowanego także pod inną nazwą handlową), w przypadku, gdyby stanowiło one kontynuację przedmiotowego oprogramowania, a przedmiotowe oprogramowanie nie byłoby dłużej rozwijane oraz wspierane,
   c) naprawie lub wymianie urządzeń w przypadku stwierdzenia ich wadliwości,
   d) świadczeniu wsparcia technicznego w trybie 24/7/365.
   e) zapewnieniu Zamawiającemu dostępu do pełnej i aktualnej dokumentacji i specyfikacji technicznej urządzeń.
3. Dostarczone urządzenia muszą:
   a) posiadać wszystkie niezbędne elementy (szyny, uchwyty, śruby, itp.) do zamontowania urządzenia w szafie typu Rack.
   b) zapewniać ochronę przed nieuprawnionym dostępem i znajdować się w bezpiecznej obudowie odpornej na nieuprawnioną ingerencję zewnętrzną.
   c) zapewniać wsparcie dla różnego rodzaju API, pozwalającego zintegrować urządzenie z każdym środowiskiem przez PKCS#11, Microsoft CryptoAPI, Java oraz OpenSSL.
   d) umożliwiać zarządzanie urządzeniem poprzez interfejs graficzny lub komendy wiersza poleceń.
   e) wspierać przynajmniej następujące algorytmy RSA, DSA, KCDSA, ECDSA, ECDH, AES, Camellia, CAST, DES, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512,Triple DES.
   f) posiadać dwa interfejsy Ethernet o szybkości co najmniej 1 Gb/s.

4. Wykonawca w ciągu 30 dni od podpisania umowy dostarczy nowy/nowe moduły kryptograficzne, a następnie w ciągu 30 dni wykona pozostałe elementy zamówienia.
5. Realizacja zamówienia odbędzie się w siedzibie Zamawiającego przy ul. Czerniakowskiej 100 w Warszawie.
6. Wykonawca otrzyma od Zamawiającego uprawnienia i dostęp fizyczny do środowisk w celu skutecznej realizacji przedmiotu zamówienia.
7. W trakcie realizacji przedmiotu zamówienia Wykonawca wykona dokumentację składającą się z następujących zagadnień:
    a) Analiza istniejącego środowiska Zamawiającego:
        - cele i zadania modułu,
        - struktura nadzoru nad modułem,
        - plan komunikacji ze szczegółowym schematem rozwiązania;
    b) Dokumentacja projektowa:
        - architektura rozwiązania i systemów wspomagających,
        - skalowalność klastra,
        - szczegółowy schemat rozwiązania całego systemu z systemami zależnymi,
        - metody zabezpieczenia klastra,
        - delegacja uprawnień dostępowych do klastra,
    c) Dokumentacja powdrożeniowa:
        - finalna szczegółowa konfiguracja klastra,
        - logiczna struktura systemu,
        - fizyczna struktura systemu,
    d) Procedury utrzymaniowe
        - zasady bieżącego monitorowania i konserwacji klastra,
        - wgrywanie nowych wersji oprogramowania,
        - zasady tworzenia kopii zapasowych sytemu oraz baz danych zawierające harmonogram tworzenia kopii zapasowych, zakres systemu podlegający tworzeniu kopii zapasowej, zasady utrzymania kopii zapasowych, procedury okresowego odzyskiwania systemu z kopii zapasowych;
8. Wsparcie techniczne dla modułów kryptograficznych rozpocznie się od dnia dostarczenia nowego urządzenia lub urządzeń do Ministerstwa Sprawiedliwości. Wykonawca potwierdzi uprawnienia Zamawiającego do wsparcia technicznego odpowiednim dokumentem.
9. Wynagrodzenie za przedmiot umowy zostanie zrealizowane po podpisaniu przez obie Strony protokołu odbioru przedmiotu umowy, który potwierdzi prawidłową realizację zamówienia i uprawnienia Zamawiającego do wsparcia technicznego. Podpisanie protokołu stanowić będzie podstawę do wystawienia przez Wykonawcę faktury, którą Zamawiający opłaci przelewem na rachunek bankowy Wykonawcy wskazany w fakturze w terminie 21 dni od otrzymania
10. Przekroczenie terminów realizacji zamówienia wskazanych w pkt 4 skutkować będzie nałożeniem przez Zamawiającego na Wykonawcę kary umownej w wysokości 0,4% wartości całego Zamówienia za każdy dzień zwłoki w jego realizacji. Do terminów wskazanych w pkt 4 nie wlicza się zwłoki wynikającej z zawinienia Zamawiającego,

niezawinionej awarii infrastruktury lub warstwy aplikacyjno-systemowej po stronie Zamawiającego bądź zdarzenia losowego niezależnego od Wykonawcy.

11. Wraz z propozycją cenową należy załączyć istotne postanowienia umowy.