Tom III SWZ - OPZ - OPIS PRZEDMIOTU ZAMÓWIENIA

Rozdział I Przedmiot zamówienia.

Przedmiotem zamówienia jest zakup Usługi Wsparcia Technicznego dla oprogramowania podpisu elektronicznego na okres 36 miesięcy w wariancie wsparcia 24/7 w celu kontynuowania poprawnej pracy systemów biznesowych resortu finansów, wymagających funkcjonalności podpisu elektronicznego. Obecnie wykorzystywane jest oprogramowanie Enigma Centaur, które nie posiada już wsparcia producenta. W ramach zamówienia zostanie wykonana aktualizacja oprogramowania podpisu elektronicznego posiadanego przez Zamawiającego w celu zapewnienia krytycznym systemom biznesowym Ministerstwa Finansów w pełni bezpiecznego i funkcjonalnego mechanizmu podpisu elektronicznego.

Rozdział II. Zakres i warunki świadczenia Usługi Wsparcia Technicznego dla Oprogramowania:

1. Wykonawca jest zobowiązany do świadczenia Usługi Wsparcia Technicznego przez okres 36 miesięcy od dnia zawarcia umowy. Usługa Wsparcia Technicznego dla Oprogramowania zapewniona przez Wykonawcę obejmuje:
   1) aktualizację oraz dostęp do aktualizacji Oprogramowania, w szczególności poprzez dostarczanie nowych wersji Oprogramowania, dostarczanie wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych. W przypadku wystąpienia trudności w związku z instalacją aktualizacji, wersji podwyższonych, wydań uzupełniających lub poprawek programistycznych dla Oprogramowania, o których mowa powyżej, Wykonawca zobowiązuje się do wsparcia Zamawiającego w sposób określony w pkt 5 poniżej;
   2) Aktualizacja oprogramowania podpisu elektronicznego nie może wiązać się z koniecznością wprowadzania zmian w kodzie działających systemów, a także konfiguracji (również infrastruktury technicznej Zamawiającego), zakłócającej działanie istniejących systemów biznesowych, korzystających obecnie z oprogramowania Enigma Signservice:
   3) Wykonawca w ramach wynagrodzenia jest zobowiązany w terminie do dwóch miesięcy po podpisaniu umowy do przeprowadzenia przeszkolenia z obsługi dostarczonego oprogramowania podpisu elektronicznego w formie szkolenia online (czas trwania: 2 dni, maksymalna liczba uczestników: 10), co zostanie potwierdzone Protokołem Odbioru Przeprowadzenia Instruktażu
   4) Wykonawca w ramach wynagrodzenia jest zobowiązany do dostarczenia w terminie do dwóch miesięcy po podpisaniu umowy dokumentacji powykonawczej wdrożonego oprogramowania podpisu elektronicznego, co zostanie potwierdzone Protokołem

Odbioru Dokumentacji Powykonawczej. Po podpisaniu umowy Zamawiający przekaże Wykonawcy do uzupełnienia szablon dokumentacji powykonawczej.

5) wsparcie w korzystaniu z Oprogramowania polegającego w szczególności na:
   a) obsłudze Zgłoszeń oraz śledzenia ich statusu, w formie elektronicznej poprzez kanały komunikacyjne dostępne przez 24 godziny, 7 dni w tygodniu w języku polskim lub angielskim,
   b) zapewnieniu dostępu do portalu www umożliwiającego wysyłanie Zgłoszeń i ich monitorowanie, służącego również do kompleksowego zarządzania posiadanymi licencjami (kluczami licencyjnymi) dla Oprogramowania, dostępnego dla Zamawiającego 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku,
   c) zapewnieniu pojedynczego punktu kontaktowego do: eskalacji Zgłoszeń i koordynacji działań Usługi Wsparcia Technicznego; bieżącego doradztwa w zakresie najlepszych praktyk, które pomagają zmniejszyć zarówno liczbę, jak i krytyczność Zgłoszeń wpływających na poziom funkcjonalności Oprogramowania; optymalizacji rozwiązań pod kątem potrzeb Zamawiającego; koordynacji zaleceń technicznych.

2. Wymagany przez Zamawiającego Czas Reakcji na Zgłoszenie gwarantowany przez Wykonawcę wynosi:
   1) dla Zgłoszeń o krytycznym priorytecie - w czasie wskazanym w ofercie Wykonawcy, nie dłuższym jednak niż 1 godzina; czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 4 godzin;
   2) do 8 godzin dla Zgłoszeń o wysokim priorytecie; czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 1 dnia roboczego
   3) do 1 dnia roboczego dla Zgłoszeń o średnim priorytecie; czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 2 dni roboczych
   4) do 2 dni roboczych dla Zgłoszeń o niskim priorytecie; czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 4 dni roboczych

   Zamawiający wymaga obsługi nieograniczonej ilości Zgłoszeń dla każdego priorytetu przez cały okres obowiązywania Umowy.
3. Zamawiający zastrzega sobie prawo do zmiany priorytetu Zgłoszenia w każdym czasie. Wówczas Czas Reakcji dla Zgłoszenia o zmienionym priorytecie liczony będzie od czasu zgłoszenia zmiany priorytetu. Priorytet Zgłoszeń o krytycznym priorytecie nie może być zmieniony na niższy.
4. W Czasie Reakcji przewidzianym dla poszczególnych priorytetów Zgłoszeń, Wykonawca potwierdzi za pomocą kanałów komunikacyjnych przyjęcie Zgłoszenia i rozpocznie prace w celu zdiagnozowania Incydentu. Wykonawca zobowiązany jest do niezwłocznego podjęcia wszelkich niezbędnych działań zmierzających do rozwiązania Zgłoszenia i przywrócenia w pełni prawidłowego działania Oprogramowania.

5. Wykonawca jest zobowiązany udostępnić na stronie internetowej, której adres został wskazany w Umowie, dostępnej dla Zamawiającego, odpowiednie pliki do pobrania, zawierające poprawki programistyczne/aktualizacje, wersje podwyższone, wydania uzupełniające i nowe wersje Oprogramowania będącego w posiadaniu Zamawiającego, niezwłocznie po ich udostępnieniu na stronie dedykowanej dla Oprogramowania.
6. W przypadku braku możliwości pobrania plików ze wskazanej przez Wykonawcę strony internetowej, Wykonawca jest zobowiązany na każde żądanie Zamawiającego do dostarczenia poprawek programistycznych/aktualizacji/wersji podwyższonych, wydań uzupełniających i nowych wersji Oprogramowania na elektronicznych nośnikach informacji w terminie do 5 Dni Roboczych od dnia zgłoszenia takiego żądania, co zostanie potwierdzone Protokołem Przekazania (którego wzór stanowi **Załącznik nr 2** do Umowy). Żądanie Zamawiający składa w formie elektronicznej na adres e-mail wskazany w Umowie lub telefonicznie pod numerem wskazanym w Umowie.
7. Wykonawca jest zobowiązany do zawiadamiania Przedstawiciela Zamawiającego z minimum 48 godzinnym wyprzedzeniem o planowanych przerwach technologicznych serwisu internetowego, poprzez umieszczaną w nim informację lub za pomocą poczty elektronicznej. W trakcie planowanej niedostępności serwisu internetowego Wykonawca zobowiązuje się do przyjmowania Zgłoszeń i udzielania informacji o ich statusie przez telefon lub za pomocą poczty elektronicznej. W czasie braku dostępu serwisu internetowego Wykonawca jest zobowiązany do obsługi Zgłoszeń. Brak dostępu serwisu internetowego nie będzie podstawą do naliczania kary umownej, pod warunkiem, że przerwa ta nie będzie trwała dłużej niż 4 godziny w Okresie Rozliczeniowym.
8. Zamawiający wymaga świadczenia Usługi 24 godziny na dobę, 7 Dni w tygodniu, 365 dni w roku.

Rozdział III Czynności odbioru Usługi Wsparcia Technicznego dla Oprogramowania:

1. Najpóźniej w 2 Dni Robocze od zawarcia Umowy Wykonawca dostarczy Przedstawicielowi Zamawiającego pisemnie na adres Zamawiającego oraz w formie elektronicznej potwierdzenie, iż posiadane Oprogramowanie jest objęte usługą Wsparcia Technicznego na okres 48 miesięcy od daty zawarcia Umowy. Wykonawca zapewnia i gwarantuje, że Potwierdzenie będzie dostępne dla Zamawiającego przez cały okres trwania Umowy.
2. Najpóźniej w dniu zawarcia Umowy Zamawiający zweryfikuje Potwierdzenie objęcia Oprogramowania Usługą Wsparcia Technicznego w zakresie kompletności tej Usługi, co zostanie potwierdzone Protokołem Odbioru Potwierdzenia, którego wzór stanowi ***Załącznik nr 2a*** do Umowy. W przypadku zastrzeżeń do realizacji przedmiotu Umowy Zamawiający zgłosi je do Protokołu Odbioru Potwierdzenia. Wykonawca zobowiązany jest w terminie do 3 Dni Roboczych do uwzględnienia zgłoszonych zastrzeżeń i ponownego

przedstawienia Zamawiającemu do akceptacji Protokołu Odbioru Potwierdzenia.

3. Do ponownej weryfikacji Protokołu Odbioru Potwierdzenia przez Zamawiającego ma zastosowanie procedura opisana w ust. 2.
4. Niezależnie od powyższej procedury odbioru, Wykonawca zobowiązany jest do dochowania terminów określonych w Umowie, w szczególności w zakresie świadczenia usługi Wsparcia Technicznego dla Oprogramowania.
5. Każdy protokół, dla swej ważności musi zostać podpisany przez obie Strony.
6. Wykonawca zobowiązuje się do przesłania Przedstawicielowi Zamawiającego pisemnie na adres Zamawiającego oraz dostarczania w formie elektronicznej w terminie 5 Dni Roboczych od daty zakończenia każdego Okresu Rozliczeniowego, podpisany przez Wykonawcę Protokół Odbioru Usługi Wsparcia Technicznego (którego wzór stanowi Załącznik nr 3 do Umowy), zawierający zestawienie wszystkich Zgłoszeń w danym Okresie Rozliczeniowym oraz czynności wykonanych przez dedykowanego inżyniera w ramach świadczonej usługi. Zamawiający w ciągu 5 Dni Roboczych od otrzymania od Wykonawcy Protokołu Odbioru Usługi Wsparcia Technicznego powiadomi w formie elektronicznej na adres e-mail Przedstawiciela Wykonawcy o akceptacji Protokołu Odbioru Usługi Wsparcia Technicznego lub o jego nieprawidłowościach.
7. W przypadku stwierdzenia nieprawidłowości, Zamawiający zwraca Protokół Odbioru Usługi Wsparcia Technicznego Przedstawicielowi Wykonawcy w celu uzupełnienia lub poprawienia. Wykonawca usunie nieprawidłowości w terminie do 3 Dni Roboczych i przedstawi Protokół Odbioru Usługi Wsparcia Technicznego do ponownej weryfikacji Przedstawicielowi Zamawiającego.
8. Do ponownej weryfikacji Protokołu Odbioru usługi Wsparcia Technicznego przez Zamawiającego ma zastosowanie procedura opisana w ust. 6 i 7 powyżej, z tym jednak zastrzeżeniem, że Zamawiający dokona ponownej weryfikacji w terminie do 3 Dni Roboczych.

Rozdział IV. Opis środowiska Zamawiającego:

Opis obecnie działającego środowiska oprogramowania podpisu elektronicznego

1. Obecnie w środowisku podpisu elektronicznego Zamawiającego wykorzystywane jest oprogramowanie podpisu elektronicznego Enigma Centaur.
2. Poniżej znajduje się opis konfiguracji poszczególnych środowisk:

    - Na środowisku produkcyjnym oprogramowanie podpisu elektronicznego wykorzystuje rozwiązanie ze sprzętowym generowaniem podpisu elektronicznego w postaci **dwóch** urządzeń typu network HSM nCipher nShield Connect 500+ CC.

Serwery na których jest zainstalowane oprogramowanie Enigma Centaur to maszyny wirtualne z system operacyjnym: Red Hat Enterprise Linux Server 7.X,

- Na środowisku testów zewnętrznych oprogramowanie podpisu elektronicznego wykorzystuje rozwiązanie ze sprzętowym generowaniem podpisu elektronicznego w postaci **jednego** urządzenia typu network HSM nCipher nShield Connect 500+ CC. Serwer na którym jest zainstalowane oprogramowanie Enigma Centaur to maszyna wirtualna z system operacyjnym: Red Hat Enterprise Linux Server 7.X,
- Środowisko testowe wewnętrzne i deweloperskie: to dwie maszyny wirtualne (brak sprzętowego generowania podpisu elektronicznego) z system operacyjnym: Red Hat Enterprise Linux Server 7.x.

3. Oprogramowanie Enigma Centaur realizuje m.in. następujące usługi kryptograficzne, wykorzystywane przez systemy biznesowe Zamawiającego:

Interfejs	**Nazwa usługi**	**Opis**
SOAP Lokalizacja: *adres_serwera_HSM:port /sopelService/services/ signService?wsdl*	signUPO	Wywołanie usługi podpis XAdES-BES, zwraca podpis typu enveloping
	getTime	Wywołanie usługi zwrócenie stempla czasu
	signDocument	Metoda podpisuje przesłany dokument zgodnie z przesłanymi parametrami podpisu
SOAP Lokalizacja: *adres_serwera_HSM:port /sopelService/services/ sopelService?wsdl*	signUPO	Wywołanie usługi podpis XAdES-BES, zwraca podpis typu enveloping
	getTime	Wywołanie usługi zwrócenie stempla czasu
REST Lokalizacja: *adres_serwera_HSM:port /sopelService/services/ sopelServiceREST*	/signUPO	Wywołanie usługi podpis XAdES-BES, zwraca podpis typu enveloping
	/getTime	Wywołanie usługi zwrócenie stempla czasu
	/signDocument	Wywołanie zwraca podpisany dokument zgodnie z

		przekazanymi parametrami podpisu
TSA Lokalizacja: *adres_serwera_HSM:port /TSA2/tsa2*	Wywołanie usługi znakowania czasem	
Wartości dla elementów *adres_serwera* i port zależą od konfiguracji wybranego serwera HSM		

4. Komunikacja pomiędzy aplikacjami biznesowymi a oprogramowaniem podpisu elektronicznego jest szyfrowana i dwustronnie uwierzytelniana, z autoryzacją zarówno serwera, jak i klienta.

Opis minimalnych wymagań, jakie po wykonaniu aktualizacji

Oprogramowanie musi posiadać

1. Oprogramowanie podpisu elektronicznego musi współpracować z urządzaniami typu network HSM nCipher nShield Connect 500+ CC, a także wspierać inne urządzenia fizyczne typu HSM dostępne na rynku. Zamawiający zastrzega sobie możliwość zmiany urządzeń po zakończeniu wsparcia na obecnie używane urządzenia
2. Oprogramowanie podpisu elektronicznego musi współpracować z Red Hat Enterprise Linux Server 7.X oraz wersje wyższe, a także wspierać inne systemy operacyjne Linux dostępne na rynku. Zamawiający zastrzega sobie możliwość zmiany urządzeń po zakończeniu wsparcia na obecnie używany system
3. Oprogramowanie podpisu elektronicznego musi samodzielnie udostępniać usługi kryptograficzne na maszynach wirtualnych bez konieczności wykorzystania urządzeń fizycznych typu Hardware Security Modules (HSM).
4. Oprogramowanie podpisu elektronicznego musi zapewnić obsługę:

   a) Podpisu elektronicznego w formatach:
      - XAdES
      - CAdES
      - PAdES
      - ASiC

   b) Algorytmów / funkcji skrótu:
      - SHA-2 (SHA-256 oraz SHA-512)

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

<ds:SignatureMethod Algorithm=" http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>

<ds:DigestMethod Algorithm=" http://www.w3.org/2001/04/xmlenc#sha512"/>

<ds:Transform Algorithm=" http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

- Obsługa wymienionych algorytmów / funkcji skrótu powinna być w prosty sposób konfigurowalna. Oprogramowanie powinno mieć możliwość włączenia / wyłączenia danego algorytmu.
- Oprogramowanie musi posiadać możliwość implementacji algorytmu SHA-3.
    - SHA-3 (SHA3-256)

<ds:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha3-256"/>

<ds:DigestMethod Algorithm="http://www.w3.org/2007/05/xmlenc#sha3-256"/>

<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

c) Wymagana długość kluczy RSA - 1024, 2048 oraz 4096.
d) Wydajność – realizacja min. 50 podpisów na sekundę z kluczem o największej możliwej i dopuszczalnej długości, wykonanych na pliku o wielkości nie mniejszej niż 4 KB, lub ograniczona przez wydajność urządzenia fizycznego typu Hardware Security Modules (HSM).
e) Możliwość znakowania czasem (RFC 1361) oraz zwracania stempla czasu urzędowego.

5. Oprogramowanie musi udostępniać poniższe interfejsy wykorzystywane przez obecnie działające systemy biznesowe Zmawiającego:

<table>
<tr><th>Interfejs</th><th>Nazwa usługi</th><th>Opis</th></tr>
<tr><td rowspan="3">SOAP
Lokalizacja:
adres_serwera_HSM:port
/sopelService/services/
signService?wsdl</td><td>signUPO</td><td>Wywołanie usługi podpis XAdES-BES, zwraca podpis typu enveloping</td></tr>
<tr><td>getTime</td><td>Wywołanie usługi zwrócenie stempla czasu</td></tr>
<tr><td>signDocument</td><td>Metoda podpisuje przesłany dokument zgodnie z przesłanymi parametrami podpisu</td></tr>
<tr><td rowspan="2">SOAP
Lokalizacja:
adres_serwera_HSM:port
/sopelService/services/
sopelService?wsdl</td><td>signUPO</td><td>Wywołanie usługi podpis XAdES-BES, zwraca podpis typu enveloping</td></tr>
<tr><td>getTime</td><td>Wywołanie usługi zwrócenie stempla czasu</td></tr>
<tr><td rowspan="3">REST
Lokalizacja:
adres_serwera_HSM:port
/sopelService/services/
sopelServiceREST</td><td>/signUPO</td><td>Wywołanie usługi podpis XAdES-BES, zwraca podpis typu enveloping</td></tr>
<tr><td>/getTime</td><td>Wywołanie usługi zwrócenie stempla czasu</td></tr>
<tr><td>/signDocument</td><td>Wywołanie zwraca podpisany dokument zgodnie z przekazanymi parametrami podpisu</td></tr>
<tr><td>TSA
Lokalizacja:
adres_serwera_HSM:port
/TSA2/tsa2</td><td colspan="2">Wywołanie usługi znakowania czasem</td></tr>
<tr><td colspan="3">Wartości dla elementów adres_serwera i port zależą od konfiguracji wybranego serwera HSM</td></tr>
</table>

6. Aktualizacja oprogramowania podpisu elektronicznego nie może wiązać się z koniecznością wprowadzania zmian w kodzie działających systemów, a także konfiguracji (również

infrastruktury technicznej Zamawiającego), zakłócającej działanie istniejących systemów biznesowych, korzystających obecnie z oprogramowania Enigma Centaur – opis obecnie działającego środowiska oprogramowania podpisu elektronicznego zawiera Rozdział IV.

7. Oprogramowanie podpisu elektronicznego powinno realizować zadanie równoważenia obciążenia dla żądań wysyłanych do urządzeń typu Hardware Security Modules (HSM) w celu optymalizacji wydajności.
8. Ruch pomiędzy aplikacjami biznesowymi a oprogramowaniem podpisu elektronicznego musi być szyfrowany z użyciem protokołu TLS i dwustronnego uwierzytelniania, z autoryzacją zarówno serwera, jak i klienta (parametry kryptograficzne muszą być konfigurowalne). Oprogramowanie musi umożliwiać włączenie i wyłączenie danego protokołu szyfrowania (SSL3.0 {wycofane} / TLS1.0 {wycofywane/wspierane} / TLS.1.1 {wycofywane/wspierane} / TLS1.2 {wspierane} / TLS1.3 {wspierane} /nowsze wersje TLS {wspierane}) oraz umożliwić implementację nowych protokołów.
9. Oprogramowanie podpisu elektronicznego musi obsługiwać klucze / certyfikaty wystawiane zarówno z infrastruktury Public Key Infrastructure (PKI) Zamawiającego, jak również zakupione u zewnętrznych podmiotów.
10. Oprogramowanie powinno uwzględniać rozwój silniejszych / nowych algorytmów kryptograficznych oraz umożliwić ich implementację.
11. Wykonawca musi dostarczyć na życzenie Zamawiającego bibliotekę, implementującą obecnie stosowane interfejsy do komunikacji z HSM po stronie klienta usługi.