Zaproszenie do złożenia oferty cenowej w celu oszacowania wartości zamówienia

1. Centrum Informatyki Resortu Finansów zaprasza w ramach rozeznania rynku oraz w celu oszacowania wartości przedmiotu zamówienia pn: **Zakup urządzeń HSM wraz z wdrożeniem sprzętu oraz usługą wsparcia technicznego** do przedstawienia oferty cenowej* na załączonym **formularzu rozeznania rynku.**

2. **Opis przedmiotu zamówienia, zakres i warunki świadczenia:**
   Szczegóły zamówienia opisuje *Załącznik A*.

3. **Termin wykonania przedmiotu zamówienia:**
   a. **Dla części A (Dostawa sprzętu): W terminie 30 dni od dnia zawarcia umowy;**
   b. **Dla części B (Wdrożenie): W terminie do 31.03.2020 r.;**
   c. **Dla części C (Świadczenie usługi wsparcia technicznego): Wykonawca zobowiązuje się do realizacji przedmiotu Umowy od dnia odbioru wdrożenia przez okres 48 miesięcy.**

4. **Zabezpieczenie należytego wykonania przedmiotu zamówienia:**
   10 % wartości przedmiotu zamówienia.

5. Wypełniony formularz należy złożyć drogą elektroniczną w terminie do dnia **5 sierpnia 2019 r.** do godz.19:00 na adres mateusz.pyrka@mf.gov.pl

   Osoba wyznaczona do kontaktu Mateusz Pyrka (tel. 48 367 36 83).

**oferta cenowa nie stanowi oferty w rozumieniu ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny, ani też nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych*

FORMULARZ ROZEZNANIA RYNKU W CELU OSZACOWANIA WARTOŚCI ZAMÓWIENIA

pn: **Zakup urządzeń HSM wraz z wdrożeniem sprzętu oraz usługą wsparcia technicznego**

1. **Dane Wykonawcy**

Nazwa Wykonawcy:	
Adres:	
Adres email/ nr telefonu:	
Osoba do kontaktów roboczych (e-mail, tel.):	
Data sporządzenia:	

2. **Szacunkowa wartość przedmiotu zamówienia zawierająca wszelkie koszty związane z przedmiotem zamówienia:**

Cześć A: Dostawa sprzętu

Wartość w PLN netto	Wartość w PLN brutto

Lista urządzeń (HSM-y oraz urządzenia do zdalnej administracji)

Lp.	Liczba sztuk	Producent	Model

Cześć B: Wdrożenie

Wartość w PLN netto	Wartość w PLN brutto

Cześć C: Usługa wsparcia technicznego

Wartość w PLN netto	Wartość w PLN brutto

……
Podpis Wykonawcy

Załącznik A

1. Przedmiotem zamówienia jest modernizacja środowiska sieciowych modułów kryptograficznych (Hardware Security Module, dalej „HSM") w Centrum Informatyki Resortu Finansów.

2. Zamawiający w środowiskach informatycznym używa aktualnie następujących urządzeń HSM:

Lp.	Model	Ilość	Wersja	Rodzaj środowiska
1	nShield Connect 500 (Thales)	2	Server: 2.59.5; Module: 2.50.16	produkcyjne
2	nShield Connect 500 (Thales)	1	Server: 2.59.5; Module: 2.50.16	testowe
3	nShield Edge (Thales)	1	Server: 2.59.5; Module: 2.50.17	produkcyjne
4	nShield Edge (Thales)	1	Server: 2.59.6; Module: 2.50.17	remote operator
5	nShield Solo 2000 F3 (Thales)	2	Server: 3.21.3; Module: 2.61.2	produkcyjne

Zamawiający wykorzystuje następujące oprogramowanie:
- Comarch HSM Server,
- KryptoSerwis,

przystosowane do współpracy z urządzeniami wymienionymi w Lp. 1-4.
- Enigma SignService,
- Enigma TS

przystosowane do współpracy z urządzeniami wymienionymi w Lp. 5.

3. Zamówienie obejmuje:
   a) Dostarczenie (wraz z zamontowaniem, podłączeniem oraz uruchomieniem) wraz z oprogramowaniem, licencjami, dokumentacją 5 identycznych sieciowych urządzeń HSM, spełniających co najmniej wymagania określone w tabeli z pkt 4 w dalszej części *Załącznika A*.
   b) Skonfigurowanie urządzeń do pracy w klastrze o wysokiej dostępności, zgodnie z zakresem opisanym w dalszej części *Załącznika A*.
   c) Skonfigurowanie urządzeń do pracy z oprogramowaniem wymienionym w pkt 2.
   d) Dostarczenie, skonfigurowanie i uruchomienie 2 zestawów urządzeń do zdalnego administrowania HSM z lokalizacji w sieci WAN resortu finansów (administrator) oraz zdalnego zarządzania kluczami kryptograficznymi na HSM (operator) wraz z niezbędnym oprogramowaniem, licencjami oraz dokumentacją.
   e) Skonfigurowanie mechanizmu tworzenia, przechowywania i odtwarzania z kopii zapasowej kluczy kryptograficznych (wraz z dostarczeniem niezbędnych urządzeń i oprogramowania, jeśli konieczne).
   f) Opracowanie i dostarczenie Zamawiającemu szczegółowej instrukcji przeniesienia kluczy kryptograficznych z urządzeń wymienionych w pkt 2, dostarczenie narzędzi (jeśli wymagane) oraz dokonanie, przy udziale Zamawiającego, przeniesienia materiału kryptograficznego (kluczy) na dostarczone urządzenia.
   g) Przystosowanie (jeżeli będzie to wymagane) dostarczonych urządzeń HSM do składania kwalifikowanej pieczęci elektronicznej 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 (QSCD).
   h) Opracowanie i dostarczenie Zamawiającemu szczegółowej dokumentacji zgodnie z zakresem opisanym w dalszej części *Załącznika A*.
   i) Przeszkolenie personelu Zamawiającego w zakresie administrowania i konfigurowania dostarczonych urządzeń i oprogramowania oraz zarządzania materiałem kryptograficznym zgodnie z zakresem opisanym w dalszej części *Załącznika A*.
   j) Świadczenie usługi wsparcia technicznego, zgodnie z zakresem opisanym w dalszej części *Załącznika A*.

4. Wymagania dla urządzeń HSM

Lp.	**Opis wymagania**
1	Obudowa urządzenia przystosowana do montażu w szafie rack 19". Zestaw akcesoriów montażowych dostarczony wraz z urządzeniem.
2	Wbudowane redundantne (min. 2) zasilacze hot-swap przystosowane do zasilania z sieci ~230V.
3	Urządzenie udostępnia usługi za pośrednictwem interfejsu Ethernet - co najmniej 2 złącza Gigabit Ethernet (RJ45).
4	Urządzenie musi umożliwiać obsługę kluczy RSA co najmniej o długościach: 1024, 2048, 4096 bitów.
5	Urządzenie musi zapewniać wsparcie dla algorytmów: RSA, ECDSA, AES, DES, Triple DES.
6	Urządzenie musi obsługiwać funkcje skrótu: SHA-1, SHA-2 (256, 384, 512).
7	Urządzenie musi zapewnić sprzętową akcelerację operacji kryptograficznych.
8	Urządzenie musi posiadać możliwość przechowywania i operowania na wielu kluczach jednocześnie (co najmniej 100).

9	Urządzenie musi umożliwiać odtworzenie materiału kryptograficznego (kluczy) z kopii zapasowej przechowywanej poza urządzeniem.
10	Urządzenie musi umożliwiać wydzielenie co najmniej 10 partycji, zestawów kart do zarządzania grupami kluczy.
11	Urządzenie musi zapewnić ochronę dostępu do kluczy za pomocą kart kryptograficznych z podziałem sekretu (z możliwością konfigurowania liczby wymaganych kart "n" spośród wszystkich "m").
12	Urządzenie musi zapewnić obsługę wielu serwerów (klientów HSM) korzystających z kluczy w HSM. Umożliwia obsługę wielu (co najmniej 10) jednoczesnych połączeń od różnych hostów.
13	Urządzenie musi posiadać możliwość pracy w trybie redundantnym (dwa lub więcej urządzeń w trybie active-active).
14	Urządzenie musi udostępnić programowe i (opcjonalnie) sprzętowe urządzenia klienckie do bezpiecznej komunikacji z HSM.
15	Urządzenie musi udostępniać interfejsy aplikacyjne: PKCS#11, Microsoft CryptoAPI/CNG, Java (JCE), OpenSSL.
16	Urządzenie musi posiadać możliwość lokalnego oraz zdalnego (poprzez sieć LAN/WAN) zarządzania konfiguracją.
17	Urządzenie musi posiadać możliwość lokalnego i zdalnego (poprzez sieć LAN/WAN) zarządzania operacjami na kluczach kryptograficznych.
18	Urządzenie musi posiadać wydajność co najmniej 150 podpisów na sekundę kluczem RSA o długości 2048 bitów.
19	Urządzenie musi być zgodne z FIPS 140-2 Level 2 oraz FIPS 140-2 Level 3 – potwierdzone certyfikatem.
20	Urządzenie musi być zgodne z IPv4 oraz IPv6.
21	Urządzenie musi posiadać znak zgodności CE.
22	Urządzenie musi być zgodne z QSCD oraz znajdować się na aktualnej liście *"Compilation of : Member States' notifications on: Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2) and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014"*.
23	Urządzenie musi zapewnić wsparcie dla Microsoft Windows Server 2012, 2016, Windows 10.
24	Urządzenie musi zapewnić wsparcie dla Red Hat Enterprise Linux 6, 7; Suse Enterprise Linux 11, 12.
25	Oprogramowanie oraz dokumentacja urządzeń musi być w wersji językowej polskiej lub angielskiej. Dokumentacja powinna być dostępna w wersji elektronicznej oraz aktualna na dzień dostawy urządzeń.

5. Cześć A - Dostawa sprzętu:

Wymagania w zakresie dostawy, montażu i uruchomienia:

a) Wykonawca w ramach dostawy sprzętu jest zobowiązany do dostarczenia sprzętu do serwerowni w Radomiu i Warszawie.
b) Dostawa i wszelkie czynności z nią związane realizowane będą przez Wykonawcę w Dni Robocze w godzinach 7:00-19:00
c) Urządzenia będą wykorzystywane w dwóch odseparowanych środowiskach: produkcyjnym oraz testowym.
d) W środowisku testowym zastosowane zostanie jedno urządzenie zlokalizowane w ośrodku przetwarzania (OP) w Radomiu.
e) W środowisku produkcyjnym zastosowane zostaną cztery urządzenia, zlokalizowane po dwa w OP w Radomiu oraz Warszawie, połączone w klaster wysokiej dostępności. Zamawiający zapewni pomiędzy obu ośrodkami połączenie sieciowe odpowiadające logicznie sieci LAN oraz przydzieli adresację urządzeń. Wykonawca dostarczy i zamontuje urządzenia w miejscach wskazanych przez Zamawiającego. Zamawiający zapewni doprowadzenie do miejsc montażu przyłączy zasilania oraz sieci LAN.
f) Infrastruktura aplikacyjna korzystająca z urządzeń HSM jest ulokowana na zwirtualizowanej platformie sprzętowo-programowej w jednym OP z możliwością uruchomienia zamiennie w drugim OP (ośrodek zapasowy). Zamawiający pod kierunkiem Wykonawcy zainstaluje i skonfiguruje oprogramowanie klienckie niezbędne do współpracy środowisk aplikacyjnych Zamawiającego z HSM. Wykonawca opracuje i dostarczy instrukcję instalacji i konfiguracji wraz z dostawą sprzętu i oprogramowania.
g) Zdalne operacje administratorskie i operatorskie będą realizowane poprzez sieć WAN resortu finansów z lokalizacji w Białymstoku oraz Radomiu. Zamawiający dysponuje na ten cel stanowiskami wyposażonymi w komputery z systemem operacyjnym Windows 10.
h) Jeżeli w celu zintegrowania środowiska HSM z oprogramowaniem Zamawiającego (wymienionym w pkt 2) konieczne będzie wytworzenie dodatkowego oprogramowania, Wykonawca przekaże Zamawiającemu kod źródłowy tego oprogramowania oraz przeniesie na Zamawiającego autorskie prawa majątkowe.

Licencje i zarządzanie kluczami / urządzeniami:

i) Wykonawca dostarczy wraz z urządzeniami dla środowiska produkcyjnego licencje uprawniające do: podłączenia do klastra co najmniej 5 serwerów klienckich, wydzielenia co najmniej 8 grup kluczy kryptograficznych (partycji, cardset-ów), zdalnego administrowania HSM-ami oraz zdalnego zarządzania kluczami kryptograficznymi.
j) Wykonawca dostarczy wraz z urządzeniem dla środowiska testowego licencje uprawniające do: podłączenia co najmniej 5 serwerów klienckich, wydzielenia co najmniej 8 grup kluczy kryptograficznych (partycji, cardset-ów), zdalnego administrowania HSM-em oraz zdalnego zarządzania kluczami kryptograficznymi.
k) Wykonawca dostarczy co najmniej 100 kart kryptograficznych do ochrony i zarządzania kluczami kryptograficznymi.
l) Wykonawca dostarczy co najmniej 15 kart kryptograficznych do administrowania HSM-ami.
m) Jeśli do zarządzania konfiguracją przewidziane są inne funkcje chronione odrębnymi kartami (tokenami) kryptograficznymi (oprócz zarządzania kluczami kryptograficznymi i administrowania urządzeniami, np. zarządzanie partycjami), Wykonawca dostarczy karty (tokeny) dla co najmniej 10 administratorów w środowisku produkcyjnym oraz co najmniej 5 administratorów w środowisku testowym.
n) Wykonawca zapewni (skonfiguruje i uruchomi) możliwość zdalnego administrowania urządzeniami oraz kluczami kryptograficznymi z lokalizacji w Białymstoku i Radomiu.

Cześć B – Wdrożenie:

Przeniesienie kluczy kryptograficznych:

a) Zamawiający wymaga dostarczenia instrukcji opisującej szczegółowo proces kopiowania kluczy kryptograficznych z urządzeń wymienionych w pkt 2 na dostarczone urządzenia HSM.
b) Asysta Wykonawcy w ramach dostawy obejmować będzie przeniesienie wybranych przez Zamawiającego kluczy. Pozostałe klucze Zamawiający będzie przenosił samodzielnie korzystając z instrukcji (i narzędzi) dostarczonych przez Wykonawcę. Jeśli Zamawiający nie będzie w stanie przenieść samodzielnie kolejnych kluczy, Wykonawca zobowiązany będzie do zapewnienia bezpośredniej asysty w ramach wdrożenia.
c) Klucze nie będą usuwane z urządzeń obecnie eksploatowanych w momencie przenoszenia. W instrukcji należy opisać sposób usuwania kluczy z urządzeń wymienionych w pkt 2.
d) Podczas przenoszenia kluczy wszystkie urządzenia muszą pozostać w siedzibie Zamawiającego.
e) Wykonawca dostarczy wszelkie niezbędne narzędzia (jeśli będą konieczne) do przenoszenia i usuwania kluczy.
f) Wykonawca będzie na bieżąco usuwał wszelkie błędy i braki stwierdzone w trakcie stosowania instrukcji.

Wymagana dokumentacja:

g) Instrukcje montażu, konfiguracji i zarządzania urządzeniami oraz oprogramowaniem.
h) Schemat komunikacji sieciowej dla HSM z wykazem przepływów do serwerów klienckich i stacji administratorskich.
i) Instrukcja przeniesienia kluczy.
j) Instrukcje aktualizacji oprogramowania serwerowego oraz klienckiego.
k) Dokumentacja infrastruktury teleinformatycznej wg szablonu przekazanego przez Zamawiającego, w zakresie wymaganym do zapewnienia miejsc montażu, podłączenia do sieci teleinformatycznych i zasilania.
l) Deklaracje zgodności FIPS, CE, QSCD.

Szkolenie:

m) Wykonawca zobowiązuje przeszkolić do 20 osób spośród personelu Zamawiającego w zakresie konfigurowania i zarządzania urządzeniami, kluczami kryptograficznymi oraz stosowania oprogramowania klienckiego do zadań związanych z utrzymywaniem, eksploatacją, zarządzaniem i diagnozowaniem.
n) Wykonawca zapewni odpowiednie miejsce na przeprowadzenie szkolenia oraz wykładowcę posiadającego kwalifikacje i odpowiednią wiedzę do przeprowadzenia szkolenia.
o) Wykonawca zapewni każdemu z uczestników szkolenia gorący posiłek, kawę i herbatę.
p) Szkolenie będzie przeprowadzone w Warszawie i będzie realizowane w języku polskim.
q) Każdy uczestnik szkolenia musi otrzymać materiały w języku polskim lub angielskim w formie elektronicznej z zakresu, który był omawiany podczas szkolenia. Materiały powinny zawierać w szczególności opis narzędzi programowych i komend wraz z parametrami, niezbędnych do wykonywania zadań wymienionych w pkt m).
r) Szkolenie będzie także obejmowało zagadnienia aktualizowania oprogramowania urządzeń oraz oprogramowania klienckiego, z uwzględnieniem problematyki wstecznej kompatybilności.

s) Szkolenie zostanie przeprowadzone co najmniej w dwóch grupach, w terminach uzgodnionych z Zamawiającym.
t) Szkolenie będzie obejmowało co najmniej 18 godzin zegarowych wykładów i ćwiczeń, rozłożonych po maksymalnie 6 godzin dziennie.
u) Wykonawca zapewni materiały i środowiska szkoleniowe. Każdy z uczestników powinien mieć zapewnione oddzielne stanowisko ćwiczeniowe.
v) Wykonawca dostarczy w terminie do 15 Dni Roboczych przed planowanym szkoleniem harmonogram zawierający:
   - termin,
   - agendę.

Cześć C - Usługa wsparcia technicznego:

Wymagania w zakresie wsparcia technicznego:

1. Wykonawca w ramach usługi wsparcia technicznego jest zobowiązany do dostarczania i wdrażania aktualizacji oprogramowania firmware urządzeń HSM w terminie wskazanym przez Zamawiającego oraz dostarczania aktualizacji oprogramowania klienckiego. Wykonanie aktualizacji obejmuje:
   a) analizę kompatybilności z eksploatowanym oprogramowaniem klienckim;
   b) wdrożenie zaktualizowanego oprogramowania firmware;
   c) wykonanie instruktażu z obsługi wdrożonej aktualizacji oprogramowania firmware, jeśli oprogramowanie wprowadziło istotne dla obsługi bądź eksploatacji zmiany;
2. Wykonawca w ramach wynagrodzenia jest zobowiązany do świadczenia usługi przez okres 48 miesięcy w wariancie wsparcia 365/24/7 na rzecz Zamawiającego w odniesieniu do urządzeń HSM w zakresie:
   1) aktualizacji oprogramowania, w szczególności dostarczania nowych wersji oprogramowania, dostarczania wersji podwyższonych, wydań uzupełniających bez dodatkowych opłat licencyjnych,
   2) wsparcia w korzystaniu z urządzeń HSM, w szczególności:
      a) świadczenia pomocy w zakresie obsługi Zgłoszeń pocztą elektroniczną lub telefonicznie lub z wykorzystaniem systemu obsługi zgłoszeń w języku polskim. Wykorzystanie systemu obsługi zgłoszeń Wykonawcy będzie traktowane z takim samym priorytetem, jak z wykorzystaniem poczty elektronicznej lub drogą telefoniczną.
      b) świadczenia pomocy w zakresie obsługi Zgłoszeń przy wykorzystaniu zdalnego dostępu do systemu Zamawiającego. Koszt zakupu wymaganych w środowisku Zamawiającego urządzeń do zabezpieczenia zdalnego dostępu do systemu Zamawiającego będzie po stronie Wykonawcy. W przypadku braku możliwości rozwiązania problemu poprzez zdalny dostęp, jest wymagana wizyta Wykonawcy w siedzibie Zamawiającego.
      c) w ramach obsługi Zgłoszeń, do obowiązków Zamawiającego będzie należało udostępnienie Wykonawcy wszystkich informacji i dokumentów, które okażą się niezbędne do należytej obsługi Incydentu (m.in. precyzyjnych opisów objawów Incydentu, informacji o działaniach podjętych przez Zamawiającego, logów itp.).
      d) w ramach obsługi Zgłoszenia Zamawiający zapewni kontakt z Przedstawicielem Zamawiającego (dla Zgłoszenia o krytycznym priorytecie w trybie 24/7) oraz zdalny dostępy do infrastruktury Zamawiającego.
      e) czas oczekiwania na otrzymanie lub uzupełnienie przez Zamawiającego niezbędnych informacji i opisów Incydentów nie będzie wliczany do czasu obsługi Zgłoszeń.
3. Wykonawca jest zobowiązany do wykonania Usługi z należytą starannością zgodnie ze standardami obowiązującymi w branży informatycznej.
4. Czas obsługi Zgłoszeń gwarantowany przez Wykonawcę wynosi:
   a) Czas reakcji powyżej 30 minut do 1 godziny dla Zgłoszeń o krytycznym priorytecie, czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 4 godzin;
   b) Czas reakcji do 24 godzin dla Zgłoszeń o wysokim priorytecie, czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 48 godzin;
   c) Czas reakcji do 48 godzin dla Zgłoszeń o średnim priorytecie, czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 96 godzin;
   d) Czas reakcji do 96 godzin dla Zgłoszeń o niskim priorytecie, czas naprawy lub zastosowania tymczasowego rozwiązania zastępczego do 336 godzin (14 dni kalendarzowych licząc od wystąpienia zgłoszenia).

e) W czasie reakcji przewidzianym dla poszczególnych rodzajów Zgłoszeń Wykonawca odpowiada za potwierdzenie przyjęcia Zgłoszenia, zdiagnozowanie prawdopodobnej przyczyny problemu i przedstawienie wstępnej procedury naprawy.
f) Jeżeli zaistnieje taka potrzeba, wymiana wadliwego urządzenia musi nastąpić w terminie:
    a. W przeciągu 1 miesiąca dla sytuacji, gdzie wadliwe jest jedno urządzenie na środowisku produkcyjnym;
    b. W przeciągu 1 tygodnia dla sytuacji, gdzie wadliwe jest jedno urządzenie na środowisku testowym;
    c. W przeciągu 1 tygodnia, jeżeli jednoczenie są wadliwe dwa urządzenia na środowisku produkcyjnym.
    d. W przeciągu 1 dnia, jeżeli wadliwe są co najmniej 3 urządzenia na środowisku produkcyjnym. Liczba dostarczonych urządzeń musi zapewnić poprawne działanie środowiska Zamawiającego.

Zasady rozliczeń:

1. Cześć A - Dostawa sprzętu: Wynagrodzenie będzie płatne w terminie do 30 dni od daty otrzymania przez Zamawiającego faktury, wystawionej przez Wykonawcę po podpisaniu przez Strony bez zastrzeżeń Protokołu Odbioru Technicznego Sprzętu.

2. Cześć B – Wdrożenie: Wynagrodzenie będzie płatne w terminie do 30 dni od daty otrzymania przez Zamawiającego faktury, wystawionej przez Wykonawcę po podpisaniu przez Strony bez zastrzeżeń Protokołu Odbioru Wdrożenia.

3. Cześć C - Usługa wsparcia technicznego: Wynagrodzenie będzie płatne z dołu, w równych częściach po upływie każdego trzymiesięcznego okresu rozliczeniowego świadczenia usługi w terminie do 30 dni od dnia dostarczenia prawidłowo wystawionej faktury za dany okres rozliczeniowy. Świadczenie usługi wsparcia technicznego rozpocznie się po podpisaniu przez Strony bez zastrzeżeń Protokołu Odbioru Wdrożenia.