Warszawa, 26-08-2021 r.

ZAMAWIAJĄCY:
Uniwersytet Warszawski
Krakowskie Przedmieście 26/28
00-927 Warszawa
REGON: 000001258
NIP: 525-001-12-66

Nazwa projektu: „Wysoce konfigurowalne rozwiązanie eSignature dla szkolnictwa wyższego" (eSignForStudy). Numer INEA/CEF/ICT/A2020/2271208

ZAPYTANIE OFERTOWE

w postępowaniu o udzielenia zamówienia publicznego nr WMIM/ZP-371/38-07/2021
na dostawę sieciowego urządzenia serwerowego z modułem kryptograficznym (HSM)

I. Przedmiot zamówienia

Dostawa sieciowego urządzenia serwerowego z modułem kryptograficznym (HSM), do montażu w szafie stelażowej, zgodnego ze szczegółową specyfikacją techniczną zamieszczoną w p. II, do wykonywania eksperymentów przewidzianych w projekcie eSignForStudy.

II. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest sieciowe urządzenie serwerowe z modułem kryptograficznym (HSM) o następujących parametrach technicznych:

1. Wymagania ogólne
   a. Sprzętowy moduł kryptograficzny (HSM) sieciowego urządzenia serwerowego musi umożliwiać wykonywanie przynajmniej następujących operacji: generowanie kluczy kryptograficznych (symetrycznych i asymetrycznych), fizyczna i logiczna ochrona kluczy kryptograficznych, kontrola dostępu do kluczy kryptograficznych, akcelerowanie operacji z użyciem kluczy kryptograficznych, archiwizacja kluczy, odtwarzanie kluczy.
   b. Klucze kryptograficzne muszą być przechowywane wewnątrz modułu HSM.
   c. Moduł musi posiadać certyfikat FIPS 140-2 Level3 lub wyższy (dopuszcza się moduły będące w trakcie certyfikacji).
   d. Moduł musi posiadać certyfikat FIPS 140-3 (dopuszcza się moduły będące w trakcie certyfikacji).
   e. Dopuszcza się, aby certyfikacje dotyczyły właściwego modułu HSM (karty kryptograficznej) wykorzystanego w sieciowym urządzeniu serwerowym,
   f. Moduł musi posiadać certyfikację eIDAS (dopuszczalne jest, aby moduły były w trakcie uzyskiwania certyfikacji) oraz był wymieniony na liście kwalifikowanych urządzeń do tworzenia podpisów i pieczęci Unii Europejskiej (kwalifikowanych urządzeń do (https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD) z ważnością, do co najmniej 2025 roku.
   g. Urządzenie powinno posiadać wydajność co najmniej:
      i. 900 podpisów kluczem RSA o długości 2048 bit na sekundę.
      ii. 180 podpisów kluczem P256 bit dla algorytmu ECC.
   h. Urządzanie musi mieć możliwość obsługi wielu serwerów oraz aplikacji z wielu lokalizacji poprzez sieć. Urządzenie powinno pozwalać na jednoczesną obsługę do **1** serwera i aplikacji.

i. Urządzenie musi pozwalać na tworzenie logicznych partycji do przechowywania materiału kryptograficznego. Partycje muszą być niezależnie zarządzane (wymagane jest oddzielne uwierzytelnienie do każdej partycji). Partycje muszą pozwalać na całkowitą separację materiału kryptograficznego i zarządzania nim. Wymagane jest, aby urządzenie pozwalało na stworzenie przynajmniej 5 takich partycji.
j. Uwierzytelnienie do administracji urządzeniem, jak i do każdej partycji, powinno odbywać się z użyciem co najmniej hasła statycznego.
k. Urządzenie powinno pozwalać na całkowitą zdalną administrację bez konieczności asysty operatorów przy urządzeniu.
l. Urządzenie wraz z dostarczonym oprogramowaniem musi pozwalać na wykorzystanie następujących interfejsów programistycznych (API): PKCS#11, Microsoft CAPI i CNG, JCA/JCE, OpenSSL.
m. Z urządzeniem powinny zostać dostarczone pakiety dla twórców oprogramowania (tzw. SDK) dla platform Windows i Linux RedHat (lub Debian).
n. Oprogramowanie dostarczone wraz urządzeniem powinno wspierać następujące platformy: Windows Server 2012 R2, 2016, 2019; Windows 10; Red Hat Enterprise Linux Server 7 i 8 (lub Debian).
o. Moduł HSM musi posiadać możliwość ładowania własnego kodu wykonywalnego, który jest uruchamiany wnętrz modułu HSM i pozwala rozszerzyć funkcje urządzenia HSM. Wraz z urządzeniem musi zostać dostarczony pakiet dla programistów (SDK) pozwalający na tworzenie, kompilowanie i ładowanie takiego kodu

2. Algorytmy kryptograficzne – urządzenie musi wspierać przynajmniej następujące algorytmy:
   a. Kryptografia symetryczna: AES, DES, Triple DES.
   b. Kryptografia asymetryczna: RSA, ECDSA, Diffie-Hellman, DSA.
   c. Funkcje skrótu: SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512).
3. Wysoka dostępność i równoważnie obciążenia (HA i LB)
   a. Urządzenie wraz z dostarczonym oprogramowaniem, po dokupieniu drugiego urządzenie, musi umożliwiać pracę w trybie wysokiej dostępności w klastrze typu active-pasive i active-active.
   b. Urządzenie wraz z dostarczonym oprogramowaniem, po dokupieniu drugiego urządzenia, pracując w trybie active-active samo musi dokonywać równoważenie obciążenia pomiędzy węzłami klastra.
4. Archiwizacja i odtwarzanie
   a. Urządzenie musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jej odtwarzanie,
5. Moduł kryptograficzny HSM musi pozwalać na rejestrowanie w sposób weryfikowalny i niezaprzeczalny:
   - Wszystkich operacji związanych z administracją modułem HSM (logowanie, wylogowanie, zmiana polityk dostępu, zerowanie, itp.).
   - Wszystkich operacji wykonywanych na kluczach kryptograficznych (tworzenie, niszczenie, użycie).
   - Monitorowanie – moduł HSM musi pozwalać na obserwowanie stanu za pomocą protokołu SNMP następujących elementów urządzenia:
     - zasilaczy sieciowych,
     - wentylatorów,
     - stanu baterii urządzenia,
     - dysków twardych,
     - wykrycie stanu naruszenia zabezpieczeń.

Co-financed by the Connecting Europe Facility of the European Union

INEA/CEF/ICT/A2020/2271208

6. Specyfikacja fizyczna
   a. Urządzenie musi posiadać obudowę o wysokości nie większej niż 2U, dostosowaną do montażu w szafie stelażowej 19”. Dostarczone urządzenie musi posiadać wszystkie niezbędne elementy (szyny, uchwyty, śruby, itp.) do zamontowania urządzenia w szafie.
   b. Urządzenie powinno być wyposażone w podwójne zasilanie typu hot-swap.
   c. Urządzenie musi posiadać min. 2 interfejsy Ethernet o szybkości 1 Gb/s.
   d. Porty Ethernet urządzenia muszą wspierać agregację łącza (port bonding).

Gwarancje i licencje
Urządzenie ma być objęte: roczną gwarancją serwisową, jedną licencją kliencką z osobną roczną gwarancją serwisową.

III. Termin i miejsce wykonania usługi

1) Termin wykonania całości zamówienia do dnia: **18.10.2021 r.**
2) Miejsce dostarczenia sprzętu: Kampus Ochota, budynek Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego, ul Banacha 2.

IV. Zawartość oferty

Oferta powinna zostać sporządzona zgodnie z wytycznymi niniejszego Zapytania w języku polskim, z wymaganymi podpisami, w formie elektronicznej (skanu).

Oferta musi być podpisana przez osobę upoważnioną do reprezentowania firmy zgodnie z formą reprezentacji określoną w rejestrze handlowym lub innym dokumencie właściwym dla formy organizacji Wykonawcy.

Niezbędne informacje zawarte w ofercie na usługę to:

1) **Nazwa i adres wykonawcy** (wraz z numerem telefonu i adresem poczty elektronicznej oraz NIP),
2) **Nazwisko i dane teleadresowe osoby do kontaktu** w sprawie oferty,
3) **Termin wykonania** (jednak nie późniejszy niż **18.10.2021 r.**),
4) **Cena netto / VAT / cena brutto**. Do oceny oferty brana jest pod uwagę całkowita kwota brutto,
5) **Inne informacje**, które uznają Państwo za istotne z punktu widzenia realizacji usługi objętej ofertą.

Zaleca się sporządzenie oferty na formularzu ofertowym, którego wzór stanowi załącznik nr 1 do zapytania ofertowego. Oferty przygotowane na własnych drukach muszą zawierać wszystkie informacje zawarte w formularzu ofertowym.

V. Kryterium wyboru oferty:

100% cena za całkowitą usługę. Ofertom punkty będą przyznawane wg następującej zasady: cena najniższa z ofert/cena oferty badanej x 100.

VI. Termin składania ofert:

06.09.2021 r., godz. $12^{\underline{00}}$

VII. Miejsce i sposób składania ofert:

Oferty należy składać drogą elektroniczną na adres e-mail: jmd@mimuw.edu.pl, z tematem „Zapytanie ofertowe – urządzenie serwerowe z modułem kryptograficznym (HSM)”.

The sole responsibility of this publication lies with the project consortium. The European Union is not responsible for any use that may be made of the information contained therein.

Co-financed by the Connecting Europe Facility of the European Union

INEA/CEF/ICT/A2020/2271208

VIII. Osoba do kontaktu ze strony Zamawiającego:

Janina Mincer-Daszkiewicz, e-mail: jmd@mimuw.edu.pl.

IX. Uwagi końcowe

1. Zamawiający zastrzega sobie prawo do wezwania Wykonawców do złożenia wyjaśnień i uzupełnień dotyczących nadesłanych ofert.
2. Zamawiający zastrzega sobie prawo do przeprowadzenia rozmów z Wykonawcami przed dokonaniem wyboru oferty.
3. Zamawiający zastrzega sobie możliwość unieważnienia zapytania ofertowego bez podania przyczyny.
4. Zamawiający odrzuci oferty, których treść nie odpowiada treści zapytania ofertowego.
5. O wyniku dotyczącym wyboru najkorzystniejszej oferty, Wykonawcy zostaną poinformowani drogą mailową, najpóźniej w terminie 3 dni roboczych (rozumianych jako dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz sobót) od daty zakończenia składania ofert. W tym samym terminie do podmiotu wybranego w wyniku rozstrzygnięcia zapytania zostanie skierowane zaproszenie do realizacji zamówienia.
6. Należność za wykonany przedmiot umowy Zamawiający ureguluje przelewem w terminie 21 dni od daty otrzymania faktury wystawionej na podstawie protokołu zdawczo-odbiorczego podpisanego przez obie strony.

X. Załączniki

Załącznik nr 1: Wzór formularza ofertowego.

The sole responsibility of this publication lies with the project consortium. The European Union is not responsible for any use that may be made of the information contained therein.

Co-financed by the Connecting Europe Facility of the European Union

INEA/CEF/ICT/A2020/2271208