OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Dostawa, montaż i uruchomienie trzech modułów kryptograficznych HSM (Hardware Security Module), wraz z gwarancją i wsparciem technicznym na okres 24 miesięcy.

II. Kody CPV

48800000-6 – systemy i serwery informacyjne
30233000-1 – Urządzenia do przechowywania i odczytu danych
72611000-6 – Usługi w zakresie wsparcia technicznego

III. Definicje

Na potrzeby niniejszego dokumentu, określenia poniższe będą miały następujące znaczenie:

1. **Awaria** – nieprawidłowe działanie Urządzeń, w tym Oprogramowania, w szczególności stan, w którym nie jest możliwe korzystanie z Urządzeń w sposób zgodny z jego przeznaczeniem, Umową, w tym OPZ, Dokumentacją lub celem Umowy.;
2. **Dni robocze** – wszystkie dni od poniedziałku do piątku w godzinach 09:00-17:00, oprócz dni ustawowo wolnych od pracy, na terytorium Rzeczpospolitej Polskiej;
3. **Lokalizacja** – miejsca zainstalowania Urządzeń na terenie miasta stołecznego Warszawy, które zostaną podane do wiadomości Wykonawcy niezwłocznie po zawarciu umowy;
4. **Urządzenia –** Urządzenia szczegółowo opisane w OPZ, które Wykonawca zobowiązany jest dostarczyć Zamawiającemu wraz z wyposażeniem, komponentami, akcesoriami, elementami zapewniającymi właściwą instalację i używanie zgodnie z przeznaczeniem.
5. **Urządzenie zastępcze -** Urządzenie o parametrach technicznych oraz funkcjonalnych nie gorszych od parametrów naprawianego Urządzenia.

IV. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż i uruchomienie trzech modułów kryptograficznych HSM (Hardware Security Module), wraz z gwarancją i wsparciem technicznym na okres 24 miesięcy.

V. Wymagania ogólne

1. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
2. Wymagane jest aby Wykonawca zapewnił wszystkie niezbędne elementy, konieczne do montażu, uruchomiania Urządzeń (tj. śrubki, nakrętki, kable zasilające, konieczne patchcordy (kable krosowe));
3. Zamawiający nie dopuszcza Urządzeń refabrykowanych, wymagana jest dostawa Urządzeń fabrycznie nowych, nieużywanych wraz z niezbędnym wyposażeniem producenta.
4. Gwarancja będzie świadczona w języku polskim.

5. Urządzenia zostaną dostarczone do dwóch Lokalizacji na terenie Warszawy, w których ma nastąpić realizacja zamówienia. Dokładne adresy zostaną podane niezwłocznie po zawarciu umowy.
6. Wykonawca zobowiązuje się w ramach realizacji przedmiotu zamówienia do dostarczenia Zamawiającemu Urządzeń opisanych w OPZ, w terminie maksymalnie 30 Dni Roboczych od daty zawarcia umowy[1].
7. Dostawa, montaż i uruchomienie Urządzeń zostanie wykonane w Lokalizacjach, w Dni Robocze, w godzinach pracy Zamawiającego (9:00-17:00)
8. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, itp. muszą być wystawione na docelowego użytkownika jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji lub inny organ pełniący funkcję organu założycielskiego lub nadzorującego wobec Zamawiającego lub następca prawny Ministra Cyfryzacji. Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z Urządzeń, dostarczonych na podstawie umowy.
9. Zamawiający wymaga aby Wykonawca posiadał status partnera producenta Urządzeń nie niższy niż drugi w kolejności licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta

VI. Szczegółowy opis zamówienia

Urządzenia (HSM) muszą spełniać następujące wymagania funkcjonalne:

1. W każdym z wymienionych poniżej wymagań jeżeli jest mowa o wsparciu dla algorytmów symetrycznych, dotyczy to przynajmniej wsparcia dla kryptografii oraz kluczy symetrycznych AES (128 i 256 bit), AES-GCM (128 i 256 bit), DES, Triple DES,
2. W każdym z wymienionych poniżej wymagań, jeżeli jest mowa o wsparciu dla algorytmów asymetrycznych, dotyczy to przynajmniej wsparcia dla kryptografii oraz kluczy asymetrycznych opartych o algorytmy:
   1) RSA-1024, RSA-2048, RSA-3072, RSA-4096,
   2) BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1 (wg specyfikacji IETF RFC 5639),
   3) NIST Curve P-256, NIST Curve P-384, NIST Curve P-521 (wg specyfikacji IETF: RFC 5480),
3. Urządzenie musi umożliwiać generowanie par kluczy kryptograficznych (symetrycznych i asymetrycznych),
4. Urządzenie musi umożliwiać fizyczną i logiczną ochronę kluczy kryptograficznych,
5. Urządzenie musi posiadać wbudowaną funkcjonalność kontroli dostępu do kluczy kryptograficznych,
6. Urządzenie musi umożliwiać wykonywanie operacji z użyciem kluczy kryptograficznych,
7. Urządzenie musi umożliwiać archiwizację kluczy, odtwarzanie kluczy z kopii bezpieczeństwa,
8. Klucze kryptograficzne muszą być przechowywane wewnątrz urządzenia,
9. Urządzenie musi umożliwiać przechowanie kluczy kryptograficznych,
10. Wymagana minimalna wydajność urządzenia to 12 podpisów kluczem RSA o długości 2048 bity na sekundę, 140 podpisów kluczem ECC przy użyciu krzywej parametrycznej NIST P256 o długości 2048 bity na sekundę,

[1] Stanowi kryterium oceny ofert

11. Urządzenie musi mieć możliwość obsługi wielu serwerów (min. 20 active i 8 passive) oraz aplikacji z wielu lokalizacji poprzez sieć,
12. Urządzenie musi umożliwiać tworzenie logicznych partycji do przechowywania materiału kryptograficznego.
13. Partycje muszą być niezależnie zarządzane (wymagane jest oddzielne uwierzytelnienie do każdej partycji).
14. Partycje muszą pozwalać na całkowitą separację materiału kryptograficznego i zarządzanie nim. Wymagane jest aby urządzenie pozwalało na rozbudowę do co najmniej 10 takich partycji,
15. Uwierzytelnienie do administracji modułem HSM, jak i do każdej partycji, powinno odbywać się z użyciem mechanizmu silnego uwierzytelniania (np. z użyciem kart inteligentnych lub tokenów) i wspierać mechanizm kworum M z N (do poprawnego uwierzytelnienia wymagane jest przedłożenie N poświadczeń z zestawu M poświadczeń, gdzie N=<M),
16. Urządzenie musi umożliwiać wykorzystanie interfejsów programistycznych (API) co najmniej: PKCS#11, Microsoft CAPI i CNG,
17. Urządzenie musi wspierać funkcje skrótu: SHA2 (SHA-224, SHA-256, SHA-384, SHA-512),
18. Urządzenie musi umożliwiać pracę w trybie wysokiej dostępności w klastrze typu active-pasive i active-active,
19. Urządzenie musi umożliwiać pracę w trybie wysokiej dostępności typu active-active w oparciu o wbudowany mechanizm równoważenia obciążenia pomiędzy węzłami klastra,
20. Urządzenie musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego w nim przechowywanego oraz na jego odtwarzanie,
21. Dostarczone rozwiązanie musi umożliwiać wykonywanie kopii bezpieczeństwa na dedykowany moduł zewnętrzny, który może być przechowywane w innej lokalizacji,
22. Dedykowany moduł zewnętrzny do wykonywania kopii bezpieczeństwa musi posiadać taki sam poziom certyfikacji jak HSM główny,
23. Rozwiązanie musi umożliwiać wykonywanie lokalnej kopii bezpieczeństwa konfiguracji i danych w sposób zdalny – tj. bez konieczności asysty operatorów bezpośrednio przy urządzeniu i bez konieczności podłączania modułu do wykonywania kopii bezpośrednio. Przez lokalną kopię bezpieczeństwa należy rozumieć kopie składowaną wewnątrz w dostarczonych urządzeniach,
24. Urządzenie musi pozwalać na zestawienie bezpiecznego kanału komunikacyjnego pomiędzy HSM a serwerem uruchomionym w środowisku wirtualnym (np. VMware, Hyper-V),
25. Dostarczone rozwiązanie musi zapewniać zestawienie bezpiecznego kanału komunikacyjnego pomiędzy aplikacją wykorzystującą interfejs PKCS#11 a partycją w module HSM – przy założeniu, że klucze do zabezpieczenia tej komunikacji muszą być przechowywane w postaci pliku na kliencie korzystającym z HSM lub w dedykowanym elemencie sprzętowym (karta, token),
26. Dostarczone rozwiązanie musi spełniać kryteria FIPS 140-2 Level 3 lub wyższy[2], dopuszcza się aby certyfikacja dotyczyła właściwego modułu HSM (karty kryptograficznej) wykorzystanego w urządzeniu sieciowym,
27. Dostarczone rozwiązanie musi spełniać kryteria Common Criteria EAL4 lub wyższy[3], dopuszcza się aby certyfikacja dotyczyła właściwego modułu HSM (karty kryptograficznej) wykorzystanego w urządzeniu sieciowym,

[2] Stanowi kryterium oceny ofert

[3] Stanowi kryterium oceny ofert

28. Dostarczone rozwiązanie musi być certyfikowane na zgodność z Normą EN 419221-5 oraz EN 419221-6:2019 oraz być zgodnym ze standardami ETSI EN 319401, EN 319411, EN 319421[4],
29. Urządzenie musi posiadać obudowę o wysokości nie większej niż 1U, dostosowana do montażu w szafie stelażowej 19”,
30. Urządzenie musi być dostarczony wraz ze wszystkimi niezbędnymi elementami umożliwiającymi jego montaż w szafie (szyny, uchwyty, śruby, etc.)
31. Urządzenie musi być wyposażone w dwa dedykowane zasilacze, umożliwiającą ich wymianę w trakcie działania (hot-swap),
32. Montaż urządzenia i jego uruchomienie zostanie zrealizowane przez Wykonawcę w Lokalizacji wskazanej przez Zamawiającego, w uzgodnionym wcześniej terminie.
33. Wraz z urządzeniem musi zostać dostarczony pakiet dla twórców oprogramowania (SDK) dla platform Windows i Linux 64 bity,

VII. Podstawowe warunki świadczenia gwarancyjnego i wsparcia technicznego :

1. Dostarczone Urządzenia i załączone oprogramowanie wbudowane zostaną objęte 24 miesięcznym wsparciem producenta.
2. Zamawiający dopuszcza świadczenie wsparcia technicznego przez autoryzowanego partnera producenta.
3. Zgłoszenia przyjmowane będą w systemie 7/12/365 przez dedykowany portal producenta, mailowo lub telefonicznie.
4. Za chwilę dokonania zgłoszenia Awarii, Strony uznają datę i godzinę poinformowania przez Zamawiającego o wystąpieniu Awarii, przez jeden z kanałów, o których mowa w pkt 3 powyżej. W przypadku zgłoszenia Awarii przez więcej niż jeden kanał, za chwilę dokonania zgłoszenia uznaje się datę i godzinę zgłoszenia wcześniejszego.
5. Do obowiązków Wykonawcy należy usuwanie Awarii Urządzenia najpóźniej w przeciągu 12 godzin chwili zgłoszenia Awarii, co zostanie potwierdzone protokołem usunięcia Awarii
6. Uszkodzone nośniki danych stanowią własność Zamawiającego i nie podlegają zwrotowi Wykonawcy w ramach wymiany. Pozostałe uszkodzone elementy Wykonawca zobowiązany jest odebrać na swój koszt
7. Wykonawca dostarczy Zamawiającemu w terminie 3 dni roboczych od dnia dostarczenia Urządzeń do pierwszej Lokalizacji, wszelkie dane dostępowe niezbędne do zgłaszania Awarii oraz korzystania ze wsparcia technicznego i gwarancji.
8. W razie nieusunięcia Awarii Urządzenia w terminie, Wykonawca dostarczył na czas naprawy urządzenie zastępcze o parametrach technicznych nie gorszych od parametrów technicznych Urządzenia naprawianego oraz zapewniających nie gorszy poziom bezpieczeństwa do Lokalizacji, w której znajduje się Urządzenie
9. Osoby świadczące gwarancję i wsparcie techniczne mogą być zobowiązane do okazania służbom ochrony obiektów, przed rozpoczęciem świadczenia usług w danej Lokalizacji, poświadczenia bezpieczeństwa dostępu do informacji niejawnych na poziomie co najmniej „POUFNE”) na pod rygorem odmowy dopuszczenia wspomnianych osób do świadczenia wsparcia technicznego z przyczyn leżących po stronie Wykonawcy.

[4] Stanowi kryterium oceny ofert