Załącznik nr 1 do SWZ
DZ.270.116.2023

Opis przedmiotu zamówienia

Dostawa 2 szt. urządzeń kryptograficznych wyposażonych w sprzętowy moduł HSM (Hardware Security Module) z instalacją i konfiguracją.

I. Skrótowy opis przedmiotu zamówienia:

Przedmiotem zamówienia jest realizacja przez Wykonawcę na rzecz PGL LP następujących dostaw i usług:

1. Dostawa 2 szt. urządzeń kryptograficznych wyposażonych w sprzętowy moduł HSM (Hardware Security Module) z niezbędnymi akcesoriami, oprogramowaniem, licencjami oraz dokumentacją, wraz z instalacją w szafach Rack w dwóch lokalizacjach:
   a) CP - Podstawowy centralny ośrodek przetwarzania danych Lasów Państwowych - Adres: ul. Grójecka 127, 02-124 Warszawa.
   b) CZ - Zapasowy centralny ośrodek przetwarzania danych Lasów Państwowych - Adres: Sękocin Stary, ul. Leśników 21C 05-090 Raszyn
2. Usługa wdrożenia urządzeń obejmująca instalację, konfigurację oraz integrację z infrastrukturą PKI Zamawiającego, w tym przeniesienie materiału kryptograficznego z obecnie używanych urządzeń HSM. Wymagania dotyczące oferowanych produktów i usług są przedstawione w kolejnych sekcjach niniejszego załącznika.

II. Szczegółowy opis przedmiotu zamówienia

W chwili obecnej Zamawiający posiada:

- Infrastrukturę klucza publicznego (PKI) – opartą o produkt Microsoft Certificate Services;
- System zarządzania kartami (CMS) – oparty o produkt HID® ActivID™ Credential Management System w wersji minimum: 5.12.

Nowo dostarczone urządzenia kryptograficzne mają zastąpić obecnie używane Safenet Luna K6.

1. Opis zakresu dostawy – wymagania dotyczące urządzeń kryptograficznych wyposażonych w moduł HSM (zwanych dalej również urządzeniami HSM bądź urządzeniami)

   1.1. Parametry ogólne każdego urządzenia

   1.1.1. Urządzenia muszą pochodzić z jednej linii produktowej, reprezentowanej przez jeden wybrany model (oba urządzenia muszą być identyczne);
   1.1.2. Urządzenie HSM musi umożliwiać generowanie kluczy kryptograficznych symetrycznych i asymetrycznych.
   1.1.3. Urządzenie HSM musi umożliwiać:

- fizyczną i logiczną ochronę kluczy kryptograficznych,
- kontrolę dostępu do kluczy kryptograficznych,
- wykonywanie operacji z użyciem kluczy kryptograficznych,
- archiwizację kluczy,
- odtwarzanie kluczy z kopii bezpieczeństwa.

1.1.4. Moduł HSM musi posiadać certyfikat FIPS 140-2 Level3 lub wyższy.

1.1.5. Moduł HSM musi posiadać certyfikat FIPS 140-3 (dopuszcza się moduły będące w trakcie certyfikacji).

1.1.6. Dopuszcza się, aby certyfikacje FIPS dotyczyły właściwego modułu HSM (karty kryptograficznej) wykorzystanego w urządzeniu sieciowym.

1.1.7. Moduł HSM musi spełniać wymogi rozporządzenia eIDAS oraz znajdować się na liście kwalifikowanych urządzeń do tworzenia podpisów i pieczęci Unii Europejskiej.

1.1.8. Klucze kryptograficzne muszą być przechowywane wewnątrz modułu HSM, urządzenie powinno pozwalać na przechowanie co najmniej 1800 kluczy RSA o długości 2048 bity.

1.1.9. Urządzenie powinno posiadać wydajność, co najmniej:
- 900 podpisów na sekundę kluczem RSA o długości 2048 bity.
- 1800 podpisów na sekundę kluczem ECC P256 bit.

1.1.10. Urządzanie musi mieć możliwość obsługi wielu serwerów oraz aplikacji z wielu lokalizacji poprzez sieć. Urządzenie powinno pozwalać na jednoczesną obsługę do 100 serwerów i aplikacji.

1.1.11. Z urządzeniem musi być dostarczona licencja do obsługi 6 serwerów/aplikacji klienckich.

1.1.12. System musi pozwalać na tymczasowe podłączenie, w razie konieczności, dodatkowych serwerów/aplikacji bez wymogu rozbudowywania jego licencji.

1.1.13. Urządzenie musi pozwalać na tworzenie logicznych partycji do przechowywania materiału kryptograficznego.

1.1.14. Partycje muszą być niezależnie zarządzane (wymagane jest oddzielne uwierzytelnienie do każdej z partycji). Partycje muszą pozwalać na całkowitą separację materiału kryptograficznego i zarządzanie nim.

1.1.15. Z urządzeniem musi być dostarczona licencja umożliwiająca konfigurację, co najmniej 5 partycji.

1.1.16. Urządzenie musi pozwalać na jednoczesne (w tym samym urządzeniu) tworzenie partycji, które będą pozwalały na eksport klucza prywatnego (w formie zaszyfrowanej) oraz partycji, które będą zabraniały na poziomie sprzętowym eksportu klucza prywatnego.

1.1.17. 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)

1.1.18. Urządzenie powinno umożliwiać zdalną administrację za pomocą REST API. Z urządzeniem powinna być dostarczona licencja, umożliwiającą wykorzystanie tej funkcji wraz z dokumentacją.

1.1.19. Wraz z urządzeniami muszą zostać dostarczone dedykowane moduły (pad, czytnik) przeznaczone do wprowadzania poświadczeń uwierzytelnienia z użyciem kart lub tokenów (łącznie 2 moduły).

1.1.20. Wraz z urządzeniem musi zostać dostarczonych, co najmniej 10 kart lub tokenów przeznaczonych do silnego uwierzytelniania (łącznie 20 dla obu urządzeń).

1.1.21. Urządzenie wraz z dostarczonym oprogramowaniem musi pozwalać na wykorzystanie następujących interfejsów programistycznych API (Application Programming Interface):
- PKCS#11,
- Microsoft CAPI i CNG,
- Java(JCA/JCE),
- OpenSSL.

1.1.22. Z urządzeniem powinny zostać dostarczony pakiet dla twórców oprogramowania (SDK) dla platform Windows i Linux RH 64 bity.

1.1.23. Oprogramowanie klienckie dostarczone wraz urządzeniem powinno wspierać następujące platformy: Windows Server 2012 R2, 2016, 2019, 2022; Red Hat Enterprise Linux Server 8;

1.1.24. Urządzenie musi zostać dostarczone od producenta do Zamawiającego w sposób bezpieczny, który pozwali Zamawiającemu potwierdzić w sposób niezaprzeczalny, że nikt nie naruszył zawartości opakowania.

1.1.25. Moduł HSM musi posiadać możliwość ładowania kodu wykonywalnego, który jest uruchamiany wewnątrz 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.

1.1.26. Urządzenie kryptograficzne z modułem HSM musi znajdować się na liście wspieranych, przez producenta posiadanego przez LP oprogramowania HiD ActivID Credential Management System (https://docs.hidglobal.com/activid-cms-v5.12/operator/operator-guide/system-env.htm), urządzeń oraz współpracować z Microsoft CA.

1.2. Mechanizmy kryptograficzne

Urządzenia kryptograficzne z modułem HSM muszą obsługiwać algorytmy kryptograficzne:

1.2.1 asymetrczne – minimum: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES);

1.2.2 symetryczne – minimum: AES, AES-GCM, Triple DES, DES, ARIA, SEED,RC2, RC4, RC5, CAST;

1.2.3 funkcje skrótu (Hash), minimum: SHA1, SHA2 (224/256/384/512), SHA3 (224/256/384/512).

Urządzenie musi posiadać mechanizm uwierzytelniania per pojedynczy klucz kryptograficzny przechowywany na partycji:

1.2.4 Poświadczenia uwierzytelniania muszą być weryfikowany przez sam moduł HSM (a nie przez aplikację zewnętrzną).

1.2.5 Poświadczenia uwierzytelniania muszą być przechowywane wewnątrz modułu HSM.

1.3. Archiwizacja i odtwarzanie

1.3.1. System musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jego odtwarzanie.

1.3.2. System musi umożliwiać przechowywanie kopii bezpieczeństwa na dedykowanym zewnętrznym urządzeniu.

1.3.3. Wraz z urządzeniem musi zostać dostarczone dedykowane urządzenie

przeznaczone do backupu partycji, wyposażone w co najmniej 32 MB przestrzeni na dane oraz pozwalające na backup minimum 100 partycji tego samego typu. Dopuszcza się dostarczenie jednego takiego urządzenia na klaster złożony z dwóch urządzeń HSM.

1.3.4. Urządzenie do wykonywania kopii bezpieczeństwa musi posiadać wszystkie niezbędne licencje do wykonania kopii wszystkich partycji z urządzeń HSM w klastrze.

1.3.5. Dedykowane urządzenie zewnętrzne do wykonywania kopii bezpieczeństwa musi posiadać certyfikację FIPS-140-2 L3 (dopuszcza się, aby moduł był w trakcie certyfikacji) oraz zapewniać retencję danych przez okres 10 lat.

1.3.6. Rozwiązanie powinno pozwalać na wykonywanie kopii bezpieczeństwa w sposób zdalny – tj. bez konieczności asysty operatorów bezpośrednio przy urządzeniu i bez konieczności podłączania urządzenia do wykonywania kopii bezpośrednio do modułu HSM.

1.4. Logowanie i monitorowanie

Urządzenie HSM musi pozwalać na rejestrowanie w sposób weryfikowalny i niezaprzeczalny:

1.4.1. Wszystkich operacji związanych z administracją modułem HSM (logowanie, wylogowanie, zmiana polityk dostępu, zerowanie, itp.).

1.4.2. Wszystkich operacji wykonywanych na kluczach kryptograficznych (tworzenie, niszczenie, użycie).

1.4.3. Monitorowanie - urządzenie HSM musi pozwalać na obserwowanie stanu za pomocą protokołu SNMP następujących elementów urządzenia:
- zasilaczy sieciowych,
- wentylatorów,
- stanu baterii urządzenia,
- stanu dysków twardych/przestrzeni dyskowych,
- stanu fizycznego urządzenia (wykrycie naruszenia integralności fizycznej - tamper).

1.5. Specyfikacja fizyczna

Każde z dostarczonych przez Wykonawcę urządzeń HSM musi:

1.5.1. Posiadać obudowę o wysokości nie większej niż 2U, pozwalającą na montaż w szafie RACK 19”.

1.5.2. Zostać dostarczone wraz ze wszystkimi niezbędnymi do montażu elementami tj.: szyny, uchwyty, śruby, itp.

1.5.3. Być wyposażone w minimum 2 redundantne zasilacze typu hot-swap.

1.5.4. Posiadać minimum 4 interfejsy Ethernet. Każdy z nich o szybkości minimum 1 Gb/s.

1.5.5. Posiadać Porty Ethernet które wspierają agregację łącza (port bonding).

1.6. Warunki gwarancji i wsparcia technicznego

1.6.1. Okres gwarancji na dostarczone urządzenia HSM i elementy wynosi minimum 36 miesięcy.

1.6.2. Okres gwarancji będzie liczony od daty podpisania przez Zamawiającego, bez zastrzeżeń, Protokołu odbioru dostawy urządzeń.

1.6.3. Urządzenia muszą być objęte gwarancją producenta/autoryzowanego dystrybutora na terytorium Rzeczypospolitej Polskiej /oficjalnego dystrybutora urządzeń na terytorium Rzeczypospolitej Polskiej.

1.6.4. Wykonawca wykupi u producenta, na pełen okres gwarancji, rozszerzone wsparcie dla dostarczanych elementów:

- z warunkami SLA: 24 x 7 x 365, czasem reakcji: 1h dla zdarzeń krytycznych, 4h dla awarii niekrytycznych, 8h (roboczych) dla pozostałych; czasem naprawy: do dwóch dni roboczych; dla urządzeń HSM oraz dla dedykowanych modułów (pad, czytnik) przeznaczonych do wprowadzania poświadczeń uwierzytelnienia z użyciem kart lub tokenów.
- z warunkami SLA minimum: 8 x 5 x NBD, czasem reakcji 8 godzin roboczych; czasem naprawy do 20 dni, dla pozostałych urządzeń i komponentów.

1.6.5. Wykonawca doręczy Zamawiającemu poświadczenie wykupienia wsparcia opisanego w pkt. 1.6.4. wraz z dostawą urządzeń.

1.6.6. Wykonawca zapewni możliwość przyjmowania zgłoszeń o usterkach i awariach w działaniu urządzeń zgodnie z pkt 1.6.4

1.6.7. W okresie gwarancji Wykonawca zobowiązuje się do zapewnienia ciągłości realizacji serwisu gwarancyjnego, w miejscu instalacji urządzeń.

1.6.8. Wsparcie techniczne obejmuje naprawę urządzeń przez producenta lub autoryzowanego partnera serwisowego producenta.

1.6.9. Wykonawca odpowiada za prawidłową obsługę zgłoszeń serwisowych w tym za dotrzymanie terminu naprawy.

1.6.10. Wykonawca zapewni wsparcie techniczne w zakresie dostarczonych urządzeń na okres obowiązywania gwarancji, drogą telefoniczną i za pośrednictwem poczty elektronicznej (e-mail) na podany w Umowie nr telefonu i adres e-mail.

1.6.11. Wykonawca będzie świadczyć na rzecz Zamawiającego pierwszą linię wsparcia w języku polskim w zakresie pomocy w rozwiązywaniu problemów i diagnozowania niesprawności urządzeń.

1.6.12. W okresie gwarancji Zamawiający będzie miał zapewniony dostęp do uaktualnień, poprawek oraz nowych wersji oprogramowania i firmware wchodzących w skład urządzeń. Zamawiający nie jest zobowiązany do ponoszenia dodatkowych kosztów z tego tytułu.

1.6.13. W okresie gwarancji Wykonawca zapewni, na żądanie Zamawiającego, pomoc w instalacji udostępnianych przez producenta urządzeń uaktualnień i poprawek. Zamawiający nie jest zobowiązany do ponoszenia dodatkowych kosztów z tego tytułu.

2. Opis zakresu usług

2.1. Usługa wdrożenia urządzeń HSM w infrastrukturze klucza PKI Zamawiającego

2.1.1. Instalacja i uruchomienie dostarczonych urządzeń HSM w dwóch lokalizacjach:

a) CP - Podstawowy centralny ośrodek przetwarzania danych Lasów Państwowych
   - Adres: ul. Grójecka 127, 02-124 Warszawa.
b) CZ - Zapasowy centralny ośrodek przetwarzania danych Lasów Państwowych
   - Adres: Sękocin Stary, ul. Leśników 21C 05-090 Raszyn

2.1.2. Przeniesienie materiału kryptograficznego z posiadanych przez Zamawiającego urządzeń kryptograficznych Luna K6 na dostarczone urządzenia HSM.

2.1.3. Integracja dostarczonych urządzeń HSM z posiadanym i wykorzystywanym przez Zamawiającego systemem PKI/CA.
2.1.4. Integracja dostarczonych urządzeń HSM z posiadanym i wykorzystywanym przez Zamawiającego Systemami ActivID.
2.1.5. Przeprowadzenie testów weryfikujących poprawność wykonanych prac.
2.1.6. Wykonanie dokumentacji powykonawczej migracji urządzeń HSM.

2.2. Dokumentacja

2.2.1. Projekt techniczny

1) Wykonawca przedstawi Zamawiającemu harmonogram realizacji przedmiotu umowy w terminie nie dłuższym niż 5 dni roboczych od daty zawarcia umowy.
2) Wykonawca przedstawi Zamawiającemu projekt techniczny w terminie nie dłuższym niż 20 dni roboczych od daty zawarcia umowy. Zakres informacji w projekcie technicznym uzgodniony będzie pomiędzy stronami.
3) Zamawiający w terminie nie dłuższym niż 5 dni roboczych od otrzymania projektu technicznego, przedstawi Wykonawcy ewentualne uwagi do projektu. Brak uwag do projektu technicznego musi być potwierdzony ze strony Zamawiającego.
4) Jeżeli konieczne będą kolejne uzgodnienia projektu technicznego, odbywać się one będą w kolejnych dwu dniowych iteracjach (po 2 dni robocze dla każdej ze stron) aż do zaakceptowania projektu technicznego przez Zamawiającego.

2.2.2. Procedury eksploatacyjne

Wykonawca dostarczy Zamawiającemu w formie elektronicznej, w języku polskim, uzgodnione z Zamawiającym procedury eksploatacyjne. W skład w/w procedur wchodzić będą minimum:

1) Procedura monitorowania stanu HSM,
2) Procedura wykonywania backupu materiałów kryptograficznych:
   a) z całego urządzenia HSM,
   b) z pojedynczej przestrzeni przechowywania materiałów kryptograficznych,
3) Procedura odtwarzania materiałów kryptograficznych z backupu:
   a) całego urządzenia HSM,
   b) pojedynczej przestrzeni przechowywania materiałów kryptograficznych,
4) Procedura kopiowania materiałów kryptograficznych z jednego urządzenia HSM na drugie,
5) Procedura importu materiałów kryptograficznych na urządzanie HSM,
6) Procedura exportu materiałów kryptograficznych z urządzenia HSM.

2.2.3. Dokumentacja powykonawcza

W skład dokumentacji powykonawczej wchodzą: projekt techniczny w tym konfiguracja urządzeń i oprogramowania oraz procedury eksploatacyjne. Wykonawca dostarczy Zamawiającemu w formie elektronicznej, w języku polskim, dokumentację powykonawczą, która będzie podlegała protokolarnemu odbiorowi wraz z dostarczonymi i skonfigurowanymi urządzeniami HSM.