234250

Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa sieciowych modułów kryptograficznych HSM (Hardware Security Module).

1. **Przedmiot zamówienia**

1.1. Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i włączenie do eksploatacji 4 sieciowych modułów kryptograficznych HSM wraz z licencjami, akcesoriami i usługami towarzyszącymi, umożliwiających rozbudowę istniejącego środowiska HSM Zamawiającego.

1.2. Rozwiązanie musi zostać włączone do istniejącego klastra HSM Zamawiającego bez konieczności migracji kluczy i bez zmian po stronie aplikacji.

2. **Środowisko Zamawiającego - stan obecny:**

2.1. Zamawiający posiada środowisko, na które składają się:

2.1.1. Urządzenia HSM nShield XC Base – 4 szt.,

2.1.2. Licencje klienckie – 10 szt./urządzenie,

2.1.3. Licencje Elliptic Curve ['ECC'] Activation (FE1637L) – 1 szt./urządzenie.

3. **Zakres zamówienia**

3.1. Dostawa 4 szt. HSM w wersji sieciowej z pełnym okablowaniem i akcesoriami montażowymi.

3.2. Dostawa licencji i aktywacji wymaganych do pełnej funkcjonalności.

3.3. Montaż w szafie rack w lokalizacji Zamawiającego podłączenie do sieci, konfiguracja i instalacja dostarczonego sprzętu oraz oprogramowania, integracja z istniejącym klastrem.

3.4. Wykonanie testów odbiorczych i przekazanie dokumentacji powdrożeniowej.

3.5. Szkolenie administratorów i operatorów.

3.6. Świadczenie gwarancji i wsparcia serwisowego zgodnie z niniejszym OPZ.

4. **Wymagania minimalne dla pojedynczego urządzenia:**

4.1. Generowanie kluczy ECC algorytmem ECDSA o długości przynajmniej: 256, 384, 512 bitów przez Centrum Certyfikacji Zamawiającego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

4.2. Wykorzystanie kluczy ECC przez API z każdym środowiskiem przez PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI i CNG, nCore.

4.3. HSM musi spełniać wymagania normy eIDAS and Common Criteria EAL4+ rozszerzony przez AVA_VAN.5 oparty na wymaganym przez eIDAS profilu zabezpieczeń zdefiniowanym w normie EN 419 221-5.

4.4. HSM musi zapewnić ochronę przed nieuprawnionym dostępem i powinno znajdować się w bezpiecznej obudowie odpornej na nieuprawnioną ingerencję zewnętrzną nie większą niż 2U, dostosowaną do montażu w szafie stelażowej 19".

4.5. Dostarczone urządzenie musi posiadać wszystkie niezbędne elementy (szyny, uchwyty, śruby, itp.) do zamontowania urządzenia w szafie.

4.6. Urządzenie musi być wyposażone w podwójne zasilanie typu hot-swap.

4.7. Moduł HSM musi posiadać co najmniej dwa 2 interfejsy Ethernet o szybkości 1 Gb/s.

4.8. HSM musi zapewnić minimum:

4.8.1. 650 podpisów cyfrowych na sekundę, wykonywanych algortymem RSA z kluczem 2048 bitowym.

4.8.2. 2000 podpisów cyfrowych na sekundę, wykonywanych algortymem ECC z kluczem 256 bitowym.

4.9. Urządzenie musi wspierać oraz posiadać licencje na korzystanie z przynajmniej następujących algorytmów:

4.9.1. Kryptografia symetryczna: AES, AES-GCM, DES, Triple DES, MD5 HMAC.

4.9.2. Kryptografia asymetryczna: RSA, ECDSA zawierające NIST, Brainpool & secp256k1 curves, Diffie-Hellman.

4.9.3. Funkcje skrótu: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3 (224, 256, 384, 512 bit).

4.10. Urządzenie musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jej odtwarzanie. Backup materiału kryptograficznego powinien być wykonywany jako backup plików i nie może wymagać użycia dodatkowych urządzeń dedykowanych. Rozwiązanie powinno pozwalać na wykonywanie kopii bezpieczeństwa w sposób zdalny bez konieczności asysty operatorów bezpośrednio przy urządzeniu.

4.11. HSM powinien zapewniać wsparcie dla różnego rodzaju API, pozwalającego zintegrować urządzenie z każdym środowiskiem przez PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore.

4.12. Zarządzanie urządzeniem poprzez interfejs graficzny lub komendy wiersza poleceń.

4.13. Wsparcie środowisk wirtualnych: Microsoft Windows Hyper-V, VMware ESXi.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

4.14. Urządzenie musi obsługiwać oraz posiadać licencję na minimum 10 klientów.

4.15. Urządzenie HSM musi posiadać możliwość odtworzenia kluczy prywatnych w standardzie PKCS11, które nie mają możliwości eksportu z aktualnie eksploatowanych przez Zamawiającego urządzeń Thales nShield XC Base (parametr CKA_EXTRACTABLE = FALSE) bez ponoszenia dodatkowych kosztów przez Zamawiającego.

4.16. **Do urządzenia musi zostać dołączone minimum 5 kart chipowych SmartCards kompatybilnych dla dostarczonego pojedynczego urządzenia HSM. Karty muszą umożliwiać zarówno lokalny jak i zdalny dostęp do urządzenia.**

4.17. Urządzenie musi zapewnić możliwość zdalnego dostępu za pomocą dedykowanego czytnika dostarczonego razem z urządzeniem. Jeśli do uruchomienia funkcjonalności wymagana jest dodatkowa licencja, musi ona być dostarczona razem z urządzeniem.

4.18. Dostarczone urządzenie musi być nowe, posiadające wsparcie producenta przez okres minimum 4 lat od daty dostarczenia urządzenia.

4.19. Urządzenie musi posiadać certyfikację eIDAS and Common Criteria EAL4+ rozszerzony przez AVA_VAN.5 oparty na wymaganym przez eIDAS profilu zabezpieczeń zdefiniowanym w normie EN 419 221-5 przez okres co najmniej 4 lat od daty dostarczenia urządzenia.

5. **Zakres dokumentacji powdrożeniowej:**
   5.1. Opis konfiguracji dostarczonych urządzeń.
   5.2. Projekt okablowania sieci LAN.
   5.3. Procedury administracyjne takie jak:
      5.3.1. Zarządzanie uprawnieniami.
      5.3.2. Zarządzanie kopiami bezpieczeństwa.
      5.3.3. Monitorowanie działania urządzenia.
      5.3.4. Procedury zarządzania kluczami kryptograficznymi.

6. **Gwarancja.**

   6.1. Urządzenie musi być objęte serwisem gwarancyjnym przez okres minimum 36 miesięcy, od daty odbioru polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

   6.2. SLA 24x7, czas reakcji do 8h, wymiana uszkodzonego urządzenia do 24 godzin

   6.3. W ramach serwisu musi być zapewniony dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7, bez dodatkowych opłat

   6.4. Jeżeli usunięcie awarii urządzenia wymaga jego wymiany, wymiana na nowe urządzenie zostanie dokonana bez konieczności zwrotu uszkodzonego.

7. **Termin realizacji zamówienia –** do 20 dni roboczych od dnia zawarcia umowy, w tym dostawa, instalacja, konfiguracja, szkolenia i testy odbiorcze wraz z dokumentacją powdrożeniową.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706