| L.p. | Nazwa parametru | Minimalne wartości wymagane przez Zamawiającego |
|---|---|---|
| 1 | **Podstawowe funkcjonalności** | Sieciowy, sprzętowy moduł kryptograficzny (HSM) musi umożliwiać wykonanie następujących operacji: generowanie kluczy kryptograficznych symetrycznych i asymetrycznych, fizyczną i logiczną ochronę kluczy kryptograficznych, kontrolę dostępu do kluczy kryptograficznych, wykonywanie operacji z użyciem kluczy kryptograficznych, archiwizację kluczy, klonowanie kluczy, odtwarzanie kluczy z kopii bezpieczeństwa.<br><br>Klucze kryptograficzne muszą być przechowywane wewnątrz urządzenia HSM. |
| 2 | **Certyfikacja** | Sprzęt musi posiadać certyfikat co najmniej FIPS 140-3 Level3 lub równoważny oraz CC EAL4+. |
| 3 | **Uwierzytelnianie** | Uwierzytelnienie do administracji modułem HSM, jak i do każdej partycji, musi odbywać się z użyciem mechanizmu silnego wieloskładnikowego 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).<br><br>Z urządzeniem musi być dostarczonych co najmniej 40 tokenów/kart i dwa urządzenia do zdalnego uwierzytelniania. |
| 4 | **Wydajność** | Sprzęt musi posiadać co najmniej wydajność (transakcji na sekundę):<br>- RSA-2048: 4500<br>- ECC P256: 8000<br>- AES-GCM: 8000 |
| 5 | **Algorytmy** | Sprzęt musi wspierać przynajmniej następujące algorytmy:<br>a) Kryptografia symetryczna: : RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES)<br>b) Kryptografia asymetryczna: RSA, Diffie-Hellman, ECDSA<br>c) Funkcje skrótu: SHA2 (SHA-224, SHA-256, SHA-384, SHA-512), SM3<br>d) Pełna obsługa zestawu kryptograficznego Suite B (NSA Suite B Cryptography)<br>e) Generator liczb pseudolosowych: zgodny ze standardem FIPS 140-2 (Federal Information Processing Standard publication 140-2) |
| 6 | **Parametry kluczy** | Sprzęt musi zapewniać parametry klucza dla kluczowych algorytmów:<br>- RSA: co najmniej 8192 bit, |
| 7 | **Administracja zdalna** | Sprzęt musi pozwalać na całkowitą zdalną administrację bez konieczności asysty operatorów przy urządzeniu (np. w celu przedkładania kart lub tokenów do slotu w urządzeniu) |
| 8 | **HA** | Sprzęt wraz z dostarczonym oprogramowaniem musi umożliwiać pracę w trybie wysokiej dostępności w klastrze typu active-pasive i active-active. |
| 9 | **Komunikacja** | Sprzęt wraz z dostarczonym oprogramowaniem musi pozwalać na zestawienie bezpiecznego kanału komunikacyjnego pomiędzy |

| | | |
|---|---|---|
| | | urządzeniem a serwerem uruchomionym w środowisku wirtualnym (np. VMware, Hyper-V, KVM). |
| 10 | **Audyt** | Sprzęt kryptograficzny HSM musi pozwalać na rejestrowanie w sposób weryfikowalny i niezaprzeczalny:<br>- wszystkich operacji związanych z administracją modułem HSM (logowanie, wylogowanie, zmiana polityk dostępu, zerowanie, itp.)<br>- wszystkich operacji wykonywanych na kluczach kryptograficznych (tworzenie, niszczenie, użycie). |
| 11 | **Kopie bezpieczeństwa** | System musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jego odtwarzanie.<br>Kopia bezpieczeństwa musi być wykonywana na dedykowane urządzenie zewnętrzne (np.: moduł), który może być przechowywane w innej lokalizacji.<br><br>Rozwiązanie musi 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 HSM. |
| 12 | **Obudowa** | Sprzęt musi posiadać obudowę o wysokości nie większej niż 1U, dostosowaną do montażu w szafie stelażowej 19”. Dostarczone urządzenie musi posiadać wszystkie niezbędne elementy (szyny, uchwyty, śruby, itp.) do zamontowania urządzenia w szafie. |
| 13 | **Zasilanie** | Sprzęt musi być wyposażone w dwa zasilacze z możliwością wymiany w trakcie działania (hot-swap). |
| 14 | **Interfejsy** | Moduł HSM musi posiadać cztery interfejsy Ethernet o szybkości co najmniej 1 Gb/s. |
| 15 | **API** | Sprzęt wraz z dostarczonym oprogramowaniem musi pozwalać na wykorzystanie co najmniej użytkowanych przez Zamawiającego interfejsów programistycznych (API): PKCS#11, Microsoft CAPI i CNG, Java(JCA/JCE), OpenSSL, |
| 16 | **Wspierane platformy** | Oprogramowanie klienckie dostarczone wraz z urządzeniem musi wspierać co najmniej użytkowane przez Zamawiającego platformy: Windows 11; Windows server 2019, 2022; Red Hat Enterprise Linux Server; SUSE Linux. |
| 17 | **Eksport klucza prywatnego** | Sprzęt musi umożliwiać realizację binarnego eksportu klucza prywatnego (utworzonego z odpowiednimi atrybutami pozwalającymi na taką operację). Chodzi o programistyczną możliwość generacji kluczy prywatnych dla zewnętrznych klientów i umieszczanie ich w zewnętrznych magazynach w formacie PKCS#12. |
| 18 | **Pula połączeń** | Sprzęt musi mieć możliwość obsługi wielu serwerów oraz aplikacji z wielu lokalizacji poprzez sieć. Urządzenie musi pozwalać na jednoczesną obsługę 2 serwerów i aplikacji. |
| 19 | **Licencje klienckie** | Ze Sprzętem musi być dostarczona licencja do obsługi aplikacji/systemów klienckich. |

| | | |
|---|---|---|
| | | Wykonawca dostarczy licencje pozwalające na podłączenie systemu 2 serwerów/aplikacji. |
| 20 | **Partycje logiczne** | Sprzęt 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 zarządzanie nim.<br>Wymagane jest, aby urządzenie pozwalało na utworzenie co najmniej 5 takich partycji. |
| 21 | **Monitorowanie** | Sprzęt musi pozwalać na monitorowanie stanu urządzeń przy pomocy protokołu SNMP. Monitorowane będą: stan zasilaczy, stan wentylatorów, stan fizyczny urządzenia (wykrycie naruszenia integralności fizycznej HSM). |
| 22 | **Okres wsparcia technicznego** | Wykonawca zapewni wsparcie techniczne na dostarczony Sprzęt na okres 60 miesięcy od dnia podpisania protokołu odbioru. |