Załącznik do zapytania o wycenę

Szczegółowy opis przedmiotu zamówienia

1. Przedmiot zamówienia:

Zakup i dostawa 2 szt. modułów HSM (Hardware Security Module) wraz z usługą serwisu i wsparcia technicznego producenta.

1) Wymagania dla HSM.

Lp.	Wymagalne minimalne parametry techniczne
1.	Sieciowy, sprzętowy moduł kryptograficzny (HSM) (zwany dalej Urządzeniem, Rozwiązaniem lub Modułem) 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, odtwarzanie kluczy z kopii bezpieczeństwa.
2.	Moduł musi posiadać certyfikat FIPS 140-2 Level3 lub wyższy.
3.	Urządzenie musi posiadać wydajność, co najmniej: a) Generowanie klucza RSA 2048 bit – 1 na sekundę, b) 70 podpisów na sekundę kluczem RSA o długości 2048 bity, c) Generowanie klucza ECDSA 256 bitów – 150 na sekundę, d) 500 podpisów na sekundę kluczem ECDSA o długości 256 bitów secp256r1.
4.	Urządzenie musi wspierać przynajmniej następujące algorytmy: a) AES, DES, 3DES, RSA, DSA, Diffie-Hellman, ECDSA, ECDH, b) Funkcje skrótu: SHA1, SHA2 (SHA-256, SHA-384, SHA-512), c) Generator liczb pseudolosowych: zgodny ze standardem FIPS 140-2.
5.	Urządzenie musi zapewniać parametry klucza dla kluczowych algorytmów: a) RSA: co najmniej 8192 bit, b) ECC: co najmniej 384 bit, c) AES: co najmniej 256 bit.
6.	Moduł kryptograficzny HSM musi pozwalać na rejestrowanie w sposób weryfikowalny i niezaprzeczalny: a) Wszystkich operacji związanych z administracją modułem HSM (logowanie, wylogowanie, zmiana polityk dostępu, zerowanie, itp.), b) Wszystkich operacji wykonywanych na kluczach kryptograficznych (tworzenie,

	niszczenie, użycie),
7.	Moduł HSM musi pozwalać na obserwowanie (monitorowanie) stanu za pomocą protokołu SNMP.
8.	Urządzenie musi pozwalać na całkowitą zdalną administrację bez konieczności asysty operatorów przy urządzeniu (np. w celu umieszczania kart lub tokenów w slocie Urządzenia).
9.	Urządzenie musi umożliwiać pracę w trybie wysokiej dostępności w klastrze typu active-pasive i active-active.
10.	Urządzenie pracując w trybie active-active samo musi dokonywać równoważenia obciążenia pomiędzy węzłami klastra.
11.	Urządzenie musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jego odtwarzanie.
12.	HSM musi posiadać obudowę o wysokości nie większej niż 1U, dostosowaną do montażu w szafie rack 19”. Dostarczone Urządzenie musi posiadać wszystkie niezbędne elementy (szyny, uchwyty, śruby, itp.) do zamontowania urządzenia w szafie.
13.	Urządzenie musi posiadać dwa zasilacze.
14.	Urządzenie musi posiadać dwa interfejsy Ethernet o szybkości 1 Gb/s.
15.	Porty Ethernet urządzenia muszą wspierać agregację łącza.
16.	Rozwiązanie musi pozwalać na wykorzystanie następujących interfejsów programistycznych (API): PKCS#11, Microsoft CAPI i CNG, Java(JCA/JCE), CXI, SQLEKM.
17.	Urządzenie musi umożliwiać realizację binarnego eksportu klucza prywatnego (utworzonego z odpowiednimi atrybutami pozwalającymi na taką operację), tj. programistyczną możliwość generowania kluczy prywatnych dla zewnętrznych klientów i umieszczanie ich w zewnętrznych magazynach w formacie PKCS#12.
18.	Urządzenie musi posiadać funkcjonalność separacji uprawnień/dostępu z użyciem mechanizmu RBAC.
19.	Urządzenie musi wspierać mechanizm multi-tenancy. Zamawiający planuje uruchomienie przynajmniej dwóch niezależnych od siebie tenantów.

2) Wymagania dot. gwarancji, wsparcia oraz licencji.

1.	Gwarancja, serwis i wsparcie techniczne	1. Długość gwarancji zgodnie z ofertą, lecz nie krócej niż 24 miesiące.

	producenta	2. Gwarancja i serwis realizowany zdalnie przez producenta rozwiązania, z czasem reakcji w zależności od poziomu krytyczności awarii/błędy (szczegóły niżej), możliwość zgłaszania awarii poprzez dedykowany i zabezpieczony kanał komunikacji elektronicznej. 3. Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez system zgłoszeniowy producenta. 4. Gwarancja i serwis realizowany w trybie 24x7x365 2h Remote Response Time (lub krócej) w przypadku krytycznego poziomu błędu/awarii oraz 24x7x365 48h (roboczych) Remote Response Time (lub krócej) w przypadku błędu niekrytycznego. 5. Zakres wsparcia technicznego a) Dostęp do pomocy technicznej; b) Dostęp do poprawek i nowych wersji oprogramowania i/lub systemu; c) Dostęp do dokumentacji technicznej; d) Dostęp do konta wsparcia urządzenia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta. e) Szczegółowe warunki wsparcia technicznego, o którym mowa powyżej regulować powinny umowy licencyjne lub inne stosowne umowy lub warunki wydane lub zaakceptowane przez producenta Rozwiązania, przy czym umowy takie, ani warunki nie mogą ograniczać wskazanych powyżej wymagań, ani stać z nimi w sprzeczności. 6. Jeżeli którakolwiek opisana powyżej funkcjonalność wymaga dodatkowych licencji to należy je dostarczyć wraz z Urządzeniem.
2.	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR