OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: **dostawa oraz wdrożenie sprzętowych modułów bezpieczeństwa (HSM).**

1. **Termin realizacji zamówienia:**

1.1. Zamówienie podstawowe, o którym mowa w pkt 2.1, zgodnie ze złożoną ofertą zrealizowane zostanie w terminie do 30 dni kalendarzowych od dnia zawarcia Umowy.

1.2. Zamówienie opcjonalne: Wdrożenie rozwiązania w sieci Zamawiającego, zgodnie ze złożoną ofertą zrealizowane zostanie nie później niż w terminie 60 dni kalendarzowych od dnia złożenia zamówienia.

1.3. Zamówienia opcjonalne: Usługi Rozwoju, zgodnie ze złożoną ofertą zrealizowane zostaną w terminach podanych w ramach zleconej usługi rozwoju, jednak nie później niż w terminie 36 miesięcy od dnia zawarcia umowy.

1.4. Zamówienie opcjonalne: Dostarczenie dodatkowych HSM Sieciowych, zgodnie ze złożoną ofertą zrealizowane zostanie nie później niż w terminie 30 dni kalendarzowych od dnia złożenia zamówienia, jednak nie później niż w terminie 12 miesięcy od dnia zawarcia umowy.

1.5. Urządzenia HSM objęte będą 60 miesięcznym okresem gwarancji producenta, liczonym od daty dostawy, potwierdzonej protokołem odbioru.

2. **Zamówienie obejmuje:**

2.1. Zamówienie podstawowe:

2.1.1. Dostawę dwóch HSM Sieciowych, urządzenia wraz z wymaganymi licencjami;

2.1.2. Dostawę dwóch HSM USB;

2.1.3. Dostawę rozwiązania oraz urządzenia sprzętowego umożliwiającego wykonywania kopii zapasowych kluczy kryptograficznych (Backup HSM),

2.1.4. Przeprowadzenie instruktażu dla Administratorów Zamawiającego.

2.2. Zamówienie opcjonalne:

2.2.1. Wdrożenie rozwiązania w sieci Zamawiającego we współpracy z Administratorami Zamawiającego;

2.2.2. Usługi Rozwoju w maksymalnym wymiarze 1000 godzin.

2.2.3. Dostawę dwóch dodatkowych HSM Sieciowych, urządzenia wraz z wymaganymi licencjami zgodnie z opisem w pkt 3.4;

Dostawa urządzeń na własny koszt, do wskazanej lokalizacji Zamawiającego na terenie m.st. Warszawy.

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

3. Wymagania

3.1. Opis funkcjonalny rozwiązania

3.1.1. Zamawiający planuje uruchomić architekturę PKI składającą się z co najmniej 2 poziomów: urzędu certyfikacyjnego typu RootCA, pracującego w trybie offline, wystawiającego zaświadczenia certyfikacyjne dla niższego poziomu urzędów typu SubCA, RA, TSA, OCSP, itp.

3.1.2. Urząd certyfikacyjny RootCA wykonuje operacje na kluczu prywatnym przetwarzanym w na HSM podłączonym bezpośrednio do serwera, z wykorzystaniem interfejsu USB (HSM USB), backupowanym, odłączanym i przechowywanym w sejfie po wykonaniu operacji kryptograficznych.

3.1.3. Urzędy certyfikacyjne niższego poziomu wykonują operacje na kluczach prywatnych przetwarzanych w pracujących w klastrze wydajnych HSM'ach Sieciowych, z wykonaną kopią bezpieczeństwa – umożliwiającą odtworzenie kluczy na innym urządzeniu.

3.1.4. Dostarczony sprzęt oraz oprogramowanie muszą pozwolić na zbudowanie wysokodostępnej, rozłożonej geograficznie (pomiędzy dwa Centra Przetwarzania Danych Zamawiającego, zwane dalej CPD) infrastruktury HSM dla obsługi operacji kryptograficznych dla Urzędów Certyfikacji (dalej CA) w ramach PKI Zamawiającego.

3.1.5. Całość rozwiązania ma być posadowiona w infrastrukturze Zamawiającego (ang. on-premises). Nie jest dopuszczalne, aby HSM lub jakikolwiek jego komponent wymagał komunikacji z elementami posadowionymi poza infrastrukturą zamawiającego.

3.1.6. Całość rozwiązania musi pochodzić z oficjalnego kanału dystrybucji producenta na rynek polski.

3.1.7. Dostarczony sprzęt musi być fabrycznie nowy, data produkcji urządzeń nie może być starsza niż 12 miesięcy licząc wstecz od dnia dostawy.

3.1.8. Całość rozwiązania musi pochodzić od jednego producenta i wszystkie urządzenia muszą być ze sobą kompatybilne (HSM USB, HSM Sieciowy oraz Backup HSM).

3.1.9. Produkty muszą pochodzić z aktualnych linii danego producenta, bez określonego końca produkcji i końca wsparcia.

3.1.10. Dostarczone licencje muszą być zapewnione na czas nieograniczony (licencje wieczyste).

3.2. Architektura i wysoka dostępność

3.2.1. Rozwiązanie ma składać się z 2 HSM USB oraz 2 (*lub 4*) urządzeń HSM Sieciowych zlokalizowanych po 1 (*lub 2*) w 2 CPD (*zamówienie podstawowe oraz opcjonalne*).

3.2.2. Urządzenia HSM Sieciowe muszą pozwolić zbudować wysokodostępny i wysokowydajny, geograficzny klaster HSM. Oferowane rozwiązanie musi pozwolić zbudować klaster składający się min. z 4 urządzeń fizycznych.

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

3.2.3. Klaster musi gwarantować wysoką wydajność (tj. skalowanie poprzez dodawanie kolejnych urządzeń) oraz niezawodność i odporność na awarię dowolnego urządzenia.

3.2.4. Każde urządzenie HSM Sieciowe musi posiadać własny adres IP wskazany przez Zamawiającego i umożliwiać obsługę połączeń/zapytań dla każdego z podłączonych serwerów (klientów). Awaria lub brak dostępu sieciowego do jednego urządzenia HSM nie może skutkować przerwą w dostępie do operacji kryptograficznych tj. klient musi automatycznie przełączyć na pozostałe, dostępne urządzenia w klastrze (łącznie z przełączeniem do drugiego CPD).

3.2.5. Urządzenia HSM Sieciowe muszą przechowywać bezpiecznie wszystkie przetwarzane klucze prywatne i udostępniać operacje kryptograficznie w trybie Active-Active. Rozwiązanie samo musi dokonywać równoważenie obciążenia pomiędzy węzłami klastra.

3.2.6. Dostarczone urządzenia muszą gwarantować wysoką niezawodność, tj. deklarowany przez producenta średni czas bezawaryjnej pracy (MTBF ang. mean time between failures) wynosić musi min. 10 lat.

3.2.7. Dostarczone rozwiązanie umożliwiające wykonywanie kopii zapasowych kluczy kryptograficznych musi pozwolić na wykonanie bezpiecznej kopii zapasowej kluczy kryptograficznych przetwarzanych w klastrze HSM i przechowywanie ich offline.

3.2.8. Klaster HSM Sieciowych oraz dostarczone licencje muszą pozwolić na obsługę Urzędów Certyfikacji oraz serwerów znaczników czasu (dalej TSA) w ramach PKI Zamawiającego składającego się z min. 16 serwerów z możliwością rozbudowy do min. 32 serwerów.

3.2.9. Dla każdego z obsługiwanych serwerów (CA oraz TSA) musi być możliwość utworzenia dedykowanej partycji (obszaru chronionego). Dostęp do każdej z partycji musi być przyznawany niezależnie i każda partycja musi posiadać swoją własną konfigurację.

3.2.10. Konfiguracja klastrowania musi być możliwa niezależnie dla każdej partycji.

3.3. Wymagania dla pojedynczego modułu HSM USB

Niżej opisano wymagania dla pojedynczego modułu HSM USB i dostarczonych z nim licencji.

3.3.1. Interfejs USB 3.0 lub USB-C do wymiany danych umożliwiający podłączenie do serwera pełniącego funkcję RootCA.

3.3.2. Sprzętowy moduł kryptograficzny (HSM) musi umożliwiać wykonanie min. 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 oraz odtwarzanie kluczy z kopii bezpieczeństwa.

3.3.3. Klucze kryptograficzne muszą być przetwarzane wewnątrz urządzenia HSM.

3.3.4. Musi umożliwiać import istniejących certyfikatów i kluczy z plików w formacje p12 i pem.

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

3.3.5. Musi posiadać certyfikat FIPS 140-3 Level 3 lub wyższy. Dopuszcza się, aby certyfikacja dotyczyła właściwego modułu HSM (karty kryptograficznej) wykorzystanego w oferowanym urządzeniu.

3.3.6. Urządzenie musi wspierać algorytmy symetryczne: AES, AES-GCM, Triple DES, asymetryczne: RSA (2048/4096/8192 bit), DSA, Diffie-Hellman, ECDSA (224/256/384/512), ECDH, Ed25519, funkcje skrótu: SHA2 (224/256/384/512).

3.3.7. Wydajność podpisywania RSA 2048 bit minimum 2/s.

3.3.8. Uwierzytelnienie do administracji urządzeniem powinno odbywać się z użyciem co najmniej hasła.

3.3.9. Urządzenie musi pozwalać na konfigurację, która będzie zabraniała na poziomie sprzętowym eksportu klucza prywatnego.

3.3.10. Urządzenie musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jej odtwarzanie. Kopia bezpieczeństwa musi być przechowywana na zewnętrznym urządzeniu.

3.3.11. Moduł kryptograficzny HSM musi pozwalać na rejestrowanie:

- wszystkich operacji związanych z administracją modułem HSM (logowanie, wylogowanie, zmiana polityk dostępu, zerowanie, itp.),
- wszystkich operacji wykonywanych na kluczach kryptograficznych (tworzenie, niszczenie, użycie).

3.3.12. HSM wraz z dostarczonym oprogramowaniem musi pozwalać na zestawienie bezpiecznego kanału komunikacyjnego pomiędzy urządzeniem a aplikacjami klienckimi.

3.3.13. Dostarczone rozwiązania musi oficjalnie wspierać (przez Producenta) Systemy Operacyjne klientów: Windows Server 2022 i nowsze, Red Hat Enterprise Linux 9 i nowsze.

3.3.14. Musi wspierać przypisanie ról z różnymi poziomami uprawnień nadawanych do indywidualnych kont Administratorów oraz rozliczalność działań wykonywanych przez Administratorów.

3.3.15. Możliwość instalacji i przechowywania min. 20 par kluczy RSA 4096 bit oraz min. 20 par kluczy ECC 256.

3.3.16. Urządzenie musi pracować pod kontrolą dedykowanego, utwardzonego systemu operacyjnego producenta, zaprojektowanego do realizacji funkcji bezpieczeństwa sieciowego. Nie jest dopuszczalne stosowanie ogólnych systemów operacyjnych (np. Linux, Windows).

3.3.17. Musi być dostosowane do pracy ciągłej 24 godzin na dobę, 7 dni w tygodniu, 365 dni w roku.

3.3.18. Musi posiadać interfejs zarządzania w języku angielskim lub polskim.

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

3.3.19. Urządzenie HSM wraz z dostarczonym oprogramowaniem musi pozwalać na wykorzystanie następujących interfejsów programistycznych (API): PKCS#11, Microsoft CAPI i CNG, JCA/JCE, OpenSSL, REST API. Jeśli jest to konieczne wraz z urządzeniami HSM musi zostać dostarczone wymagane oprogramowanie (klient/biblioteki).

3.3.20. Posiadać certyfikat CE oraz RoHS.

3.4. Wymagania dla pojedynczego modułu HSM Sieciowego

Niżej opisano wymagania dla pojedynczego modułu HSM Sieciowego i dostarczonych z nim licencji.

3.4.1. Obudowa maksymalnie 2U RACK 19 cali dostarczona wraz z szynami montażowymi i wszystkimi elementami niezbędnymi do montażu w szafie.

3.4.2. Min. 2 redundantne zasilacze (1+1) typu HotPlug o mocy umożliwiającej poprawną pracę urządzenia z pełną wydajnością w przypadku awarii jednego z nich, 240V AC.

3.4.3. Minimum 4 porty Gigabit Ethernet z obsługą agregacji interfejsów sieciowych.

3.4.4. Brak pojedynczego punktu awarii tj. wszystkie krytyczne komponenty urządzenia takie jak zasilacze i wentylatory muszą być redundantne i muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość pracy urządzenia. Komponenty te muszą być wymienialne w trakcie pracy urządzenia, bez przerywania dostępu do danych.

3.4.5. Sprzętowy moduł kryptograficzny (HSM) musi umożliwiać wykonanie min. 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 oraz odtwarzanie kluczy z kopii bezpieczeństwa.

3.4.6. Klucze kryptograficzne muszą być przechowywane wewnątrz urządzenia HSM.

3.4.7. Musi umożliwiać import istniejących certyfikatów i kluczy z plików w formacje p12 i pem.

3.4.8. Musi posiadać certyfikat FIPS 140-3 Level 3 lub wyższy. Dopuszcza się, aby certyfikacja dotyczyła właściwego modułu HSM (karty kryptograficznej) wykorzystanego w oferowanym urządzeniu.

3.4.9. Musi posiadać status urządzeń QSCD (ang. Qualified Signature or Seal Creation Device) zgodnych z rozporządzeniem eIDAS (musi znajdować się na liście kwalifikowanych urządzeń do tworzenia podpisów i pieczęci zgodnie z wymogami Unii Europejskiej: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd). Ważność certyfikacji min. 3 lata od dnia składania oferty. Dopuszcza się, aby certyfikacja dotyczyła właściwego modułu HSM (karty kryptograficznej) wykorzystanego w oferowanym urządzeniu.

3.4.10. Musi zapewniać automatyczną replikacją materiału kryptograficznego w ramach klastra urządzeń HSM.

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

3.4.11. Urządzenie musi wspierać algorytmy symetryczne: AES, AES-GCM, Triple DES, asymetryczne: RSA (2048/4096/8192 bit), DSA, Diffie-Hellman, ECDSA (224/256/384/512), ECDH, Ed25519, funkcje skrótu: SHA2 (224/256/384/512), SHA3 (224/256/384/512).

3.4.12. Urządzenie musi wspierać w pełni algorytmy kryptograficzne określone w Commercial National Security Algorithm Suite (CNSA Suite) w wersji 1.0 oraz 2.0 .

3.4.13. Wydajność podpisywania RSA 2048 bit (per każde urządzenie) minimum 2000/s.

3.4.14. Wydajność podpisywania ECC P256 (per każde urządzenie) minimum 2000/s.

3.4.15. Zapewniać logiczną ochronę kluczy kryptograficznych poprzez możliwość partycjonowania HSM lub inny podział funkcjonalny umożliwiający rozdzielenie chronionych obszarów: minimum 8 autonomicznych przestrzeni przeznaczonych do przechowywania kluczy kryptograficznych z możliwością niezależnego przyznania dostępu/uprawnień do każdej z nich oraz umożliwiać zarządzanie/administrowanie dostępem do każdej z przestrzeni kluczy – minimum w następujący sposób: dostęp administracyjny do całości przestrzeni kluczy oraz dostęp administracyjny do danej przestrzeni kluczy (administrator pojedynczej przestrzeni kluczy). Urządzenia musi umożliwiać rozbudowę do obsługi min. 16 partycji. Partycje muszą pozwalać na całkowitą separację materiału kryptograficznego i zarządzania nim.

3.4.16. Jednoczesna obsługa wielu serwerów oraz aplikacji z wielu lokalizacji poprzez sieć IPv4.

3.4.17. Zapewniona separacja dostępu pomiędzy partycjami lub innym podziałem funkcjonalnym. Dany serwer/klient może mieć dostęp tylko do partycji / obszaru do której ma uprawnienia.

3.4.18. Jeżeli podział na partycje / obszary chronione wymaga dostarczenia licencji, należy uwzględnić licencje do obsługi minimum 8 partycji / obszarów chronionych.

3.4.19. HSM musi pozwalać na całkowitą zdalną administrację bez konieczności asysty operatorów przy urządzeniu (np. w celu przedkładania kart lub tokenów do slotu w urządzeniu).

3.4.20. Uwierzytelnienie do administracji urządzeniem, jak i do każdej partycji, powinno odbywać się z użyciem co najmniej hasła.

3.4.21. 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 (dla takich partycji jedyna możliwość zabezpieczenia klucza to kopia zapasowa na Backup HSM).

3.4.22. Urządzenie musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jej odtwarzanie. Kopia bezpieczeństwa musi być przechowywana na dedykowanym zewnętrznym urządzeniu tj. dostarczony Backup HSM.

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

3.4.23. Możliwość wysyłania logów do centralnego systemu zbierania logów lub SIEM za pomocą protokołu Syslog (zgodnie z RFC 5424).

3.4.24. Moduł kryptograficzny HSM musi pozwalać na rejestrowanie:

- wszystkich operacji związanych z administracją modułem HSM (logowanie, wylogowanie, zmiana polityk dostępu, zerowanie, itp.),
- wszystkich operacji wykonywanych na kluczach kryptograficznych (tworzenie, niszczenie, użycie).

3.4.25. HSM wraz z dostarczonym oprogramowaniem musi pozwalać na zestawienie bezpiecznego kanału komunikacyjnego pomiędzy urządzeniem a aplikacjami klienckimi.

3.4.26. Urządzanie musi mieć możliwość obsługi wielu serwerów oraz aplikacji poprzez sieć IP. Jeżeli obsługa serwerów (klientów) wymaga dostarczenia licencji, należy uwzględnić licencje do obsługi minimum 16 serwerów.

3.4.27. Dostarczone rozwiązania musi oficjalnie wspierać (przez Producenta) Systemy Operacyjne klientów: Windows Server 2022 i nowsze, Red Hat Enterprise Linux 9 i nowsze.

3.4.28. Musi wspierać przypisanie ról z różnymi poziomami uprawnień nadawanych do indywidualnych kont Administratorów oraz rozliczalność działań wykonywanych przez Administratorów.

3.4.29. Możliwość instalacji i przechowywania min. 480 certyfikatów RSA 4096 bit oraz min. 480 certyfikatów ECC 256.

3.4.30. Urządzenie musi pracować pod kontrolą dedykowanego, utwardzonego systemu operacyjnego producenta, zaprojektowanego do realizacji funkcji bezpieczeństwa sieciowego. Nie jest dopuszczalne stosowanie ogólnych systemów operacyjnych (np. Linux, Windows).

3.4.31. Musi obsługiwać komunikację za pomocą IPv4.

3.4.32. Komunikacja sieciowa dla między klientami a urządzeniem oraz dla zarządzania urządzeniem musi być szyfrowana za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpiecznie tj. np. TLS 1.3.

3.4.33. Musi umożliwić aktualizację daty i czasu z serwera NTPv4.

3.4.34. Musi udostępniać parametry pracy HSM za pomocą protokołu SNMPv3 w celu monitoringu technicznego pracy urządzenia min. w zakresie:

- zasilaczy,
- wentylatorów,
- dysków twardych,
- wykrycie stanu naruszenia zabezpieczeń.

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

3.4.35. Musi być dostosowane do pracy ciągłej 24 godzin na dobę, 7 dni w tygodniu, 365 dni w roku.

3.4.36. Musi posiadać interfejs zarządzania w języku angielskim lub polskim.

3.4.37. Urządzenie HSM wraz z dostarczonym oprogramowaniem musi pozwalać na wykorzystanie następujących interfejsów programistycznych (API): PKCS#11, Microsoft CAPI i CNG, JCA/JCE, OpenSSL, REST API. Jeśli jest to konieczne wraz z urządzeniami HSM musi zostać dostarczone wymagane oprogramowanie (klient/biblioteki).

3.4.38. Posiadać certyfikat CE oraz RoHS.

3.5. Wymagania dla Backup HSM

Urządzenie Backup HSM ma służyć do bezpiecznego przechowywania kopia bezpieczeństwa materiałów kryptograficznych przetwarzanych na HSM i musi spełniać poniższe wymagania:

3.5.1. Dedykowane urządzenie zewnętrzne do wykonywania kopii bezpieczeństwa.

3.5.2. Musi posiadać taki sam poziom certyfikacji jak urządzenia HSM: FIPS-140-3 Level3 – zabezpieczony materiał kryptograficzny nie obniża poziomu zabezpieczeń materiału przetwarzanego w urządzeniach HSM USB i/lub HSM Sieciowe.

3.5.3. Zapewniać retencję danych przez okres min. 10 lat.

3.5.4. 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 HSM.

3.5.5. Urządzenie musi umożliwić wykonania kopi zapasowej dla min. 480 certyfikatów RSA 4096 oraz 480 certyfikatów ECC 256 jednocześnie.

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

3.6. Instruktaż dla Administratorów Zamawiającego

3.6.1. Instruktaż oraz wdrożenie możliwe są w formie stacjonarnej, hybrydowej oraz sesji zdalnych (MS Teams) – do uzgodnienia na etapie wdrożenia pomiędzy koordynatorami Umowy. Zamawiający nie przewiduje dostępu zdalnego dla Wykonawcy, prace prowadzone będą we współpracy z inżynierami Zamawiającego (stacjonarnie lub sesje MS Teams).

3.6.2. Instruktaż dla Administratorów Zamawiającego musi pozwolić na samodzielnie zarządzenie rozwiązaniem, instalację, strojenie konfiguracji, aktualizację oraz rozwiazywanie typowych problemów. Warsztaty muszą zostać przeprowadzone na poziomie gwarantującym samodzielną administrację i konfigurowanie dostarczonego oprogramowania i urządzeń oraz rozwiązywanie typowych problemów.

3.6.3. Instruktaż musi zostać przeprowadzony dla min 8 pracowników Zamawiającego i musi trwać min 10 dni roboczych, każdy po 8h.

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

3.6.4. Instruktaż będzie prowadzony w języku polskim.

3.7. Gwarancja

3.7.1. Należy wycenić gwarancję dla całości rozwiązania (sprzęt oraz oprogramowanie) na okres 60 miesięcy.

3.7.2. W ramach gwarancji należy ująć naprawę lub wymianę sprzętu oraz dostęp do aktualizacji i nowych wersji oprogramowania.

3.7.3. Gwarancja musi być świadczona przez Producenta, dystrybutora lub jego autoryzowany serwis.

3.7.4. Zamawiający wymaga zapewnienia możliwości dokonywania zgłoszeń bezpośrednio w polskiej organizacji serwisowej producenta urządzeń.

3.7.5. W okresie świadczenia gwarancji producenta, bez dodatkowych opłat, Wykonawca zapewni Zamawiającemu stały dostęp (24 godziny na dobę przez 7 dni w tygodniu) do nowych wersji i aktualizacji kodu maszynowego (firmware) publikowanych na stronie internetowej producenta urządzeń.

3.7.6. Serwis gwarancyjny musi być realizowany w języku polskim przez producenta lub dystrybutora na Polskę oferowanych urządzeń.

3.8. Zakres opcjonalny Usługi Wdrożenia

3.8.1. Wykonawca we współpracy z Administratorami Zamawiającego zaprojektuje (przygotuje projekt techniczny) oraz wdroży rozwiązanie w sieci Zamawiającego:

- projekt techniczny (przedwdrożeniowy) - opis architektury,
- konfiguracja klastra / rozwiązania wysokodostępowego, zapewniającego właściwą redundancję i wykorzystanie zasobów urządzeń,
- konfiguracja partycji lub innego rozwiązania pozwalającego na bezpieczną separację kluczy kryptograficznych,
- instalacja i konfiguracja klienta HSM,
- najlepsze praktyki dla PKI zbudowanego w oparciu o Windows Server,
- procedury i instrukcje zawierające specyfikacje operacji wykonywanych w ramach ceremonii generowania kluczy dla urzedów RootCA i SubCA.
- dokumentacja powykonawcza.

3.8.2. Spotkania wdrożeniowe będą prowadzone w języku polskim.

3.8.3. Dokumentacja (powykonawcza oraz projekt techniczny) oraz musi być przygotowana w postaci dokumentów MS Word (format .docx). Wszystkie dokumenty muszą być przygotowane w polskiej wersji językowej, z wyjątkiem dokumentacji do wdrażanych produktów, która może być dostarczona w języku angielskim.

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

3.9. Zakres opcjonalny Usługi Rozwoju

3.9.1. Zamawiający może uruchomić zlecenie Realizacji Usług Rozwoju, w terminach podanych w ramach zleconej usługi rozwoju, jednak nie później niż w terminie 36 miesięcy od dnia zawarcia umowy obejmujących swoim zakresem rozbudowę, zmianę konfiguracji, wdrażanie nowych funkcjonalności w obszarze urządzeń i systemów.

3.9.2. Łączna liczba godzin przeznaczona na prace w ramach Usługi Rozwoju nie może przekroczyć ilości maksymalnej, o której mowa w pkt. 2.2.2. powyżej.

3.9.3. Wykonawca nie ma prawa do roszczenia o zlecenie mu pełnej puli godzin Usług Rozwoju.

3.10. Zasady zlecania i rozliczenia Usług Rozwoju

3.10.1. Zamawiający przekaże Wykonawcy propozycję zlecenia realizacji Usług Rozwoju, w którym określi zakres prac oraz oczekiwany termin wykonania Usług Rozwoju.

3.10.2. Wykonawca w terminie do 5 Dni Roboczych od otrzymania propozycji zlecenia Zamawiającego wystosuje do Zamawiającego odpowiedź zawierającą wskazanie liczby roboczogodzin koniecznych do wykonania określonych Usług Rozwoju, wskazanie osób, które po stronie Wykonawcy będą odpowiedzialne za realizację Usług Rozwoju oraz potwierdzenie terminu realizacji zleconych prac lub propozycję nowego terminu realizacji zlecenia.

3.10.3. Zamawiający po otrzymaniu odpowiedzi Wykonawcy może:

- Zlecić Wykonawcy realizację Usług Rozwoju zgodnie z treścią propozycji zlecenia i odpowiedzi Wykonawcy.
- Złożyć oświadczenie o rezygnacji z realizacji danych Usług Rozwoju.
- Zaprosić Wykonawcę do negocjacji celem ustalenia zakresu, pracochłonności i terminu realizacji Usług Rozwoju.

3.10.4. Zlecenia realizacji Usług Rozwoju mogą być składane przez Zamawiającego pisemnie lub elektronicznie. Potwierdzenie zlecenia prac rozwojowych lub rezygnacja z ich wykonania wymaga formy pisemnej lub elektronicznej na adres upoważnionego przedstawiciela Wykonawcy wskazany Umowie.

3.10.5. Zamawiający może zlecać realizację Usług Rozwoju w siedzibie Zamawiającego lub w innym miejscu zaakceptowanym przez Zamawiającego.

3.10.6. W godziny pracy Konsultantów nie będzie wliczony czas dojazdu Konsultanta do siedziby Zamawiającego.

3.10.7. Wykonawca jest zobowiązany do dołączenia do protokołu odbioru Usług Rozwoju rozliczenie czasu pracy Konsultantów w formacie edytowalnym zawierającej, co najmniej:

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

- Datę realizacji zadania.
- Godzinę rozpoczęcia realizacji godzinę zakończenia realizacji.
- Liczbę godzin.
- Realizowane zadanie.
- Imię i nazwisko Konsultanta realizującego zadanie.

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