PROJEKT – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Rozbudowa klastra modułów HSM (Hardware Security Module) wraz z usługami gwarancji i wsparcia technicznego na okres 36 miesięcy.

II. Kody CPV

48800000-6 – Systemy i serwery informacyjne
30233000-1 – Urządzenia do przechowywania i odczytu danych
72611000-6 – Usługi w zakresie wsparcia technicznego

III. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) **W ramach zamówienia podstawowego:**
   a) Rozbudowa posiadanego przez Zamawiającego klastra modułów HSM (Hardware Security Module) poprzez dostawę, montaż i uruchomienie kompletu urządzeń wraz z oprogramowaniem w lokalizacji (dwa miejsca na terenie miasta stołecznego Warszawy, których dokładne adresy zostaną podane do wiadomości Wykonawcy niezwłocznie po zawarciu Umowy), zgodnie z opisem wskazanym w pkt VI ppkt 2 OPZ albo równoważnych (zgodnie z opisem równoważności określonym w pkt VII i VIII OPZ) wraz z przekazaniem dokumentacji, w tym dokumentacji powykonawczej,
2) **W ramach Opcji:**
   a) Rozbudowa posiadanego przez Zamawiającego klastra modułów HSM (Hardware Security Module) poprzez dostawę, montaż i uruchomienie do dwóch kompletów urządzeń wraz z oprogramowaniem w lokalizacji (dwa miejsca na terenie miasta stołecznego Warszawy, których dokładne adresy zostaną podane do wiadomości Wykonawcy niezwłocznie po zawarciu Umowy), zgodnie z opisem wskazanym w pkt VI ppkt 3 OPZ albo równoważnych (zgodnie z opisem równoważności określonym w pkt VII i VIII OPZ), wraz z przekazaniem dokumentacji, w tym dokumentacji powykonawczej,
3) **Zapewnienie Gwarancji i Wsparcia Technicznego** dla Urządzeń, o której mowa w pkt. IX OPZ na okres 36 miesięcy,

IV. Termin realizacji

1. Wykonawca zapewni realizację przedmiotu zamówienia podstawowego w następujących terminach:
   a. Wykona dostawę, montaż i uruchomienie Urządzeń wraz z oprogramowaniem zgodnie z opisem wskazanym w pkt VI ppkt 2 OPZ albo równoważnych (zgodnie z opisem równoważności określonym w pkt VII i VIII OPZ) wraz z przekazaniem dokumentacji, w tym dokumentacji powykonawczej, w ciągu 30

dni roboczych od zawarcia Umowy;

2. Wykonawca zapewni realizację przedmiotu zamówienia dostarczonego w ramach Opcji w następujących terminach:
   a. Wykona dostawę montaż i uruchomienie Urządzeń wraz z oprogramowaniem zgodnie z opisem wskazanym w pkt VI ppkt 3 OPZ albo równoważnych (zgodnie z opisem równoważności określonym w pkt VII i VIII OPZ) wraz z przekazaniem dokumentacji, w tym dokumentacji powykonawczej, w ciągu 30 dni roboczych od zawarcia Umowy;
3. Gwarancja i Wsparcie Techniczne dla dostarczonych Urządzeń, zgodnie z opisem wskazanym w pkt IX OPZ będą świadczone przez okres 36 miesięcy.

V. Wymagania ogólne

1. Wykonawca wraz z dostawą urządzeń (a także później przy każdej zmianie tych danych), dostarczy Zamawiającemu do lokalizacji lub prześle Zamawiającemu na podany w Umowie adres e-mail**:**

   2.1. Pełną dokumentację (z wyjątkiem dokumentacji powykonawczej);
   2.2. Wersje instalacyjne oprogramowania, licencje (umowy licencyjne oraz wszystkie wymagane klucze licencyjne i aktywacyjne dotyczące oprogramowania, w tym niezbędne do uruchomienia urządzeń), a także dane dostępowe do konta w serwisie producenta urządzeń umożliwiające samodzielne pobieranie oprogramowania w ramach posiadanych licencji;
   2.3. Poświadczenie producenta urządzeń o posiadaniu przez Wykonawcę statusu partnera producenta urządzeń, z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał status partnera producenta urządzeń nie niższy niż drugi w kolejności licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta na terytorium Unii Europejskiej. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu poprzedzającym;
   2.4. Zestawienie wszystkich numerów telefonicznych na infolinie/linie techniczne producenta urządzeń, umożliwiających po podaniu numeru seryjnego urządzenia weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa);
   2.5. Zestawienie dostarczanych licencji w formacie .xlsx lub .pdf, obejmujące numer umowy z producentem, numer klienta, nazwę produktów, numery produktów, liczbę licencji oraz daty obowiązywania wsparcia technicznego;
   2.6. Dane umożliwiające zgłoszenie awarii oraz skorzystanie przez Zamawiającego z pełnego zakresu gwarancji i wsparcia technicznego, w tym co najmniej: numerów telefonicznych, adresów e-mail, adresu strony i danych dostępowych do dedykowanego portalu do zgłoszeń.

2. Wymagane jest, aby wraz z dostawą urządzeń Wykonawca zapewnił wszystkie niezbędne elementy, konieczne do montażu i uruchomiania urządzeń (takie jak śrubki, nakrętki, kable zasilające, konieczne patchcordy (kable krosowe), itp.).

3. Wymagane jest, aby wraz z dostawą urządzeń Wykonawca zapewnił niezbędne akcesoria jak:
    a) nośniki materiału kryptograficznego (tokeny, karty, etc.),
    b) niezbędne akcesoria dla obsługi urządzeń i wprowadzania kart i tokenów oraz kodów PIN,
    c) niezbędne urządzenia i akcesoria do umożliwienia wykonania bezpiecznego backupu materiału kryptograficznego i konfiguracji urządzeń.
4. Wykonawca wykona montaż urządzeń w każdej z lokalizacji oraz dokona ich uruchomienia w uzgodnieniu z Zamawiającym. Montażu i uruchomienia urządzeń w każdej z lokalizacji dokona inżynier posiadający certyfikat producenta urządzeń uprawniający do wykonywanych prac.
5. Po dokonaniu montażu i uruchomienia urządzeń w każdej z lokalizacji Wykonawca sporządzi i przekaże Zamawiającemu dokumentację powykonawczą.
6. Wykonawca ma obowiązek utylizacji wszelkich powstałych odpadów i opakowań związanych z realizacją przedmiotu zamówienia, chyba że Zamawiający postanowi inaczej.
7. Z uwagi na wymogi bezpieczeństwa obowiązujące w lokalizacjach, osoby wyznaczone przez Wykonawcę do realizacji przedmiotu zamówienia są zobowiązane do stosowania się do zasad obowiązujących w lokalizacjach oraz mogą być zobowiązane do okazania służbom ochrony obiektów, przed rozpoczęciem świadczenia prac, usług w danej lokalizacji, poświadczeń bezpieczeństwa dostępu do informacji niejawnych o klauzuli min. „poufne". Wykonawca może być również zobowiązany do przesłania Zamawiającemu drogą e-mail, na co najmniej 2 dni robocze przed dostawą urządzeń do każdej z lokalizacji, numerów rejestracyjnych pojazdów, którymi będą dostarczane urządzenia oraz numerów i serii dowodów osobistych osób wyznaczonych przez Wykonawcę do realizacji przedmiotu zamówienia, w celu identyfikacji i potwierdzenia tożsamości ww. osób przez służby ochrony obiektów. W przypadku odmowy wstępu do lokalizacji przez służby ochrony obiektu z powodu nieokazania przez daną osobę wymaganych poświadczeń bezpieczeństwa dostępu do informacji niejawnych o klauzuli min. „poufne" lub nieprzesłania Zamawiającemu danych wskazanych w zdaniu drugim powyżej, opóźnienie w realizacji przedmiotu zamówienia z tego wynikające będzie stanowiło zwłokę Wykonawcy.
8. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży na rzecz Skarbu Państwa – Ministra Cyfryzacji. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego użytkownika i licencjobiorcę urządzeń i oprogramowania jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji, z adresem korespondencyjnym przy ul. Królewskiej 27, 00-060 Warszawa, NIP 525-295-50-37, REGON 525189465. Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z przedmiotu zamówienia, w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją systemów na rzecz Ministra Cyfryzacji.
9. Przedmiot zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 5 ust 1 pkt 4 lit. d w zw. z art. 4 pkt. 1 Ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026. poz. 20 ze zm.), dalej: „Ustawa", należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym

samym, Przedmiot zamówienia musi być zgodny z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie może zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi państwa.

VI. Szczegółowy opis przedmiotu zamówienia

1. Zamawiający użytkuje aktualnie klaster rozproszony składający się z poniższych urządzeń i oprogramowania:

#	Numer SKU	Ilość	Opis produktu
1.	908-000365-003-000	4	LUNA NETWORK HSM S790 (PED,MAXIMUM PERF,32MB,10 PARTITIONS,FM READY,GRK-16,SW7.2.0,FW 7.0.3/7.2.0)
2.	908-000451-003-000	2	LUNA BACKUP HSM B700 (32MB,100 PARTITIONS,FW 7.7.2,LG7-02)
3.	908-000396-001-002	16	PARTITION 5-PACK,LUNA NETWORK HSM 7 (FACTORY INSTALL)
4.	908-000455-001-000	4	LUNA NETWORK HSM S790-10G (PED,MAXIMUM PERF,32MB,10 PARTITIONS,FM READY,GRK-16,SW7.2.0,FW 7.0.3/7.2.0)
5.	908-000451-003-000	2	LUNA BACKUP HSM B700 (32MB,100 PARTITIONS,FW 7.7.2,LG7-02)
6.	908-000396-001-002	16	PARTITION 5-PACK,LUNA NETWORK HSM 7 (FACTORY INSTALL)
7.	909-000004-002-000	8	IKEY 1000 10-PACK,LUNA REMOTE PED;STM & AUDIT KEYS,PI,USB,ROHS
8.	909-000004-002-000	1	IKEY 1000 10-PACK,LUNA REMOTE PED;STM & AUDIT KEYS,PI,USB,ROHS
9.	908-000399-003-000	4	REMOTE PED (PED RF, FW2.9.0)
10.	908-000402-001-002	11	CLIENT LICENSES,LUNA NETWORK HSM 7
11.	908-000402-001-002	11	CLIENT LICENSES,LUNA NETWORK HSM 7
12.	908-000466-001-000	1	CRYPTO CMD CTR,MONITORING AND MANAGEMENT,50 PACK,PERPETUAL
13.	908-000466-001-000	1	CRYPTO CMD CTR,MONITORING AND MANAGEMENT,50 PACK,PERPETUAL

Posiadane urządzenia i oprogramowanie objęte są wsparciem technicznym. Zamawiający nie wymaga wsparcia technicznego dla posiadanych urządzeń i oprogramowania w ramach przedmiotu zamówienia.

2. W ramach zamówienia podstawowego Zamawiający wymaga dostarczenia, montażu i uruchomienia urządzeń wraz z oprogramowaniem w celu rozbudowy posiadanego klastra modułów HSM opartego o oprogramowanie i urządzenia Thales Luna S790 wraz z gwarancją i wsparciem technicznym, zgodnych z poniższym opisem:

#	Numer SKU	Ilość	Opis produktu
1.	908-000455-001-000	8	LUNA NETWORK HSM S790-10G (PED,MAXIMUM PERF,32MB,10 PARTITIONS,FM READY,GRK-16,SW7.2.0,FW 7.0.3/7.2.0)

2.	020-160001-014-000	8	HSM,ENHANCED MAINTENANCE SERVICE,3 YEAR for 908-000365-003-000
3.	908-000451-003-000	4	LUNA BACKUP HSM B700 (32MB,100 PARTITIONS,FW 7.7.2,LG7-02)
4.	020-160001-014-000	4	HSM,ENHANCED MAINTENANCE SERVICE,3 YEAR for 908-000451-003-000
5.	908-000399-003-000	8	REMOTE PED (PED RF, FW2.9.0)
6.	909-000004-002-000	2	IKEY 1000 10-PACK,LUNA REMOTE PED;STM & AUDIT KEYS,PI,USB,ROHS
7.	020-160001-014-000	2	HSM,ENHANCED MAINTENANCE SERVICE,3 YEAR for 909-000004-002-000
8.	908-000402-001-002	22	CLIENT LICENSES,LUNA NETWORK HSM 7
9.	020-160001-014-000	22	HSM,ENHANCED MAINTENANCE SERVICE,3 YEARS for 908-000402-001-002
10.	912-00003-901-000	16	POWER CORD,220 VAC,EURO
11.	908-000414-001-003	80	CRYPTO CMD CTR, MONITORING AND MANAGEMENT PER PARTITION, PERPETUAL (51-200)
12.	020-160001-013-000	80	HSM,STANDARD MAINTENANCE SERVICE,3 YEARS for 908-000414-001-002

albo równoważnych, zgodnie z opisem równoważności określonym w pkt VII, VIII i IX OPZ, wraz z przekazaniem dokumentacji, w tym dokumentacji powykonawczej.

3. W ramach Opcji Zamawiający wymaga dostarczenia, montażu i uruchomienia urządzeń wraz z oprogramowaniem w celu rozbudowy posiadanego klastra modułów HSM opartego o oprogramowanie i urządzenia Thales Luna S790 wraz z gwarancją i wsparciem technicznym, zgodnych z poniższym opisem (gdzie opis odnosi się do pojedynczego kompletu urządzeń):

#	Numer SKU	Ilość	Opis produktu
1.	908-000455-001-000	2	LUNA NETWORK HSM S790-10G (PED,MAXIMUM PERF,32MB,10 PARTITIONS,FM READY,GRK-16,SW7.2.0,FW 7.0.3/7.2.0)
2.	020-160001-014-000	2	HSM,ENHANCED MAINTENANCE SERVICE,3 YEAR for 908-000365-003-000
3.	908-000451-003-000	1	LUNA BACKUP HSM B700 (32MB,100 PARTITIONS,FW 7.7.2,LG7-02)
4.	020-160001-014-000	1	HSM,ENHANCED MAINTENANCE SERVICE,3 YEAR for 908-000451-003-000
5.	908-000399-003-000	2	REMOTE PED (PED RF, FW2.9.0)
6.	908-000402-001-002	11	CLIENT LICENSES,LUNA NETWORK HSM 7
7.	020-160001-014-000	11	HSM,ENHANCED MAINTENANCE SERVICE,3 YEARS for 908-000402-001-002
8.	912-00003-901-000	4	POWER CORD,220 VAC,EURO
9.	908-000414-001-002	20	CRYPTO CMD CTR, MONITORING AND MANAGEMENT PER PARTITION, PERPETUAL (21-50)

10.	020-160001-013-000	20	HSM,STANDARD MAINTENANCE SERVICE,3 YEARS for 908-000414-001-002

albo równoważnych, zgodnie z opisem równoważności określonym w pkt VII, VIII i IX OPZ, wraz z przekazaniem dokumentacji, w tym dokumentacji powykonawczej.

VII. Kryteria stosowane w celu oceny równoważności

(1) Zamawiający przez „rozwiązanie równoważne" rozumie urządzenia wraz z oprogramowaniem zapewniające, bez dodatkowych nakładów finansowych po stronie Zamawiającego, minimalne funkcjonalności wskazane w pkt VIII OPZ poniżej.

(2) Zamawiający w zakresie każdego elementu przedmiotu zamówienia wymienionego w pkt VI powyżej, wskazał poniżej kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania rozwiązania równoważnego, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne wszystkich kryteriów równoważności.

(3) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych przypadkach) nie będzie poprawnie współpracować z posiadanymi przez Zamawiającego modułami HSM lub spowoduje zakłócenia w ich funkcjonowaniu, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania posiadanych przez Zamawiającego modułów HSM, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

(4) Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych w pkt VI OPZ, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej, ani w warstwie oprogramowania. W szczególności dotyczy to aplikacji wykorzystywanych oraz utrzymywanych przez Zamawiającego.

(5) Wszelkie niezbędne prace adaptacyjne (jeśli wystąpi potrzeba ich wykonania), zostaną zrealizowane przez Wykonawcę na jego koszt. Wykonawca dostarczy dokumentację przeprowadzonych prac adaptacyjnych.

(6) Wykonawca zapewni Zamawiającemu odpowiednie szkolenia z zakresu obsługi rozwiązania równoważnego w zakresie nie mniejszym niż 24 godziny robocze dla minimum 4 użytkowników rozwiązania równoważnego.

(7) W przypadku zaoferowania rozwiązania równoważnego należy zapewnić urządzenia w ilości zapewniającej identyczną wydajność i funkcjonalność, co całość klastra po rozbudowie o wskazane urządzenia referencyjne, określone w pkt VI OPZ.

VIII. Wymagania funkcjonalne dla przedmiotu zamówienia

Każde urządzenie działające w ramach klastra musi spełniać następujące wymagania funkcjonalne:

1. Wszystkie poniższe parametry należy traktować jako parametry minimalne.
2. W każdym z wymienionych poniżej wymagań, jeżeli jest mowa o wsparciu dla algorytmów symetrycznych, dotyczy to przynajmniej wsparcia dla kryptografii oraz kluczy symetrycznych AES (128 i 256 bit), AES-GCM (128 i 256 bit), Triple DES.
3. W każdym z wymienionych poniżej wymagań, jeżeli jest mowa o wsparciu dla algorytmów asymetrycznych, dotyczy to przynajmniej wsparcia dla kryptografii oraz kluczy asymetrycznych opartych o algorytmy:
    a) RSA-2048, RSA-3072, RSA-4096,
    b) BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1 (wg specyfikacji IETF RFC 5639),
    c) NIST Curve P-256, NIST Curve P-384, NIST Curve P-521 (wg specyfikacji IETF: RFC 5480).
4. HSM umożliwia generowanie par kluczy kryptograficznych asymetrycznych oraz kluczy symetrycznych.
5. HSM umożliwia fizyczną i logiczną ochronę kluczy kryptograficznych.
6. HSM posiada wbudowaną funkcjonalność kontroli dostępu do użycia kluczy kryptograficznych.
7. HSM umożliwia wykonywanie operacji z użyciem kluczy kryptograficznych.
8. HSM umożliwia archiwizację kluczy, odtwarzanie kluczy z kopii bezpieczeństwa.
9. Klucze kryptograficzne muszą być przechowywane zarówno wewnątrz, jak i na zewnątrz Urządzenia. Wymaganie dotyczy kluczy aktywnie wykorzystywanych przez systemy komunikujące się z HSM (np. aplikacje).
10. Pojemność pamięci wewnętrznej kluczy pozwala na przechowywanie co najmniej 5000 kluczy dowolnego rodzaju wyspecyfikowanych w pkt VIII.3. powyżej.
11. Minimalna wydajność HSM to 8000 podpisów na sekundę kluczem RSA o długości 2048 bitów, 14000 podpisów na sekundę kluczem ECC przy użyciu krzywej parametrycznej NIST P256, 7000 podpisów na sekundę kluczem ECC przy użyciu krzywej parametrycznej NIST P384.
12. HSM musi mieć możliwość równoległej obsługi żądań serwerów i aplikacji poprzez sieć. Jeżeli producent rozwiązania stosuje różne licencje dla danej funkcjonalności należy zapewnić licencję umożliwiającą równoległą obsługę żądań serwerów i aplikacji poprzez sieć bez określania ilości podłączonych do HSM maszyn wirtualnych/aplikacji korzystających z kluczy HSM.
13. HSM 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.
14. HSM musi posiadać co najmniej 10 partycji i umożliwiać rozszerzenie do co najmniej 90.
15. Uwierzytelnienie do administracji modułem HSM, jak i do każdej partycji, musi odbywać się z użyciem mechanizmu silnego uwierzytelniania (np. z użyciem kart inteligentnych lub tokenów).
16. HSM musi pozwalać na wykorzystanie następujących interfejsów programistycznych (API): PKCS#11, Microsoft CAPI i CNG, JCA/JCE, OpenSSL.
17. HSM musi posiadać możliwość uruchomienia dodatkowych modułów funkcjonalnych wewnątrz HSM wytworzonych za pomocą dołączonego SDK lub dostarczonych przez firmy trzecie.
18. HSM musi wspierać funkcje skrótu: SHA2 (SHA-224, SHA-256, SHA-384, SHA-512).

19. HSM musi umożliwiać pracę w trybie wysokiej dostępności w klastrze typu active-pasive i active-active. Urządzenia muszą umożliwiać rozbudowę klastra do minimum 12 węzłów.
20. HSM musi umożliwiać pracę w trybie wysokiej dostępności typu active-active w oparciu o mechanizm równoważenia obciążenia pomiędzy węzłami klastra.
21. HSM musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w HSM i na jego odtwarzanie.
22. Urządzenie musi umożliwiać wykonywanie kopii bezpieczeństwa na dedykowany, dostarczony wraz z Urządzeniem moduł zewnętrzny dopuszczając możliwość dostarczenia po jednym module zewnętrznym do backupu kluczy dla każdych dwóch Urządzeń HSM.
23. Urządzenia muszą być zgodne z FIPS 140-3 Level 3 lub równoważną.
24. Zamawiający wskazuje następujące warunki równoważności dla normy FIPS 140-3 i uzna za normę równoważną opisywanej, normę która:
    1) Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
    2) Została wydana przez NIST (ang. National Institute of Standards and Technology) lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji,
    3) Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
    4) Została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa.
25. Urządzenie musi być certyfikowane jako zgodne z eIDAS Protection Profile (PP) EN 419 221-5 jako kwalifikowany dostawca podpisu oraz kwalifikowane urządzenie do kreacji pieczęci. Wykonawca dołączy stosowne certyfikaty potwierdzające spełnienie wymagania, wydane przez niezależne instytucje.
26. Urządzenie umożliwia wykorzystanie algorytmów ML-DSA i ML-KEM. Wykorzystywanie tych algorytmów nie może ograniczać funkcjonalności takich jak klonowanie, backup i odzyskiwanie partycji czy tworzenie grup wysokiej dostępności.
27. HSM musi posiadać obudowę o wysokości nie większej niż 2U, dostosowaną do montażu w szafie rack 19”.
28. HSM musi być dostarczony ze wszystkimi niezbędnymi elementami montażowymi (szyny, uchwyty, śruby, Pin Entry Device – po jednym na Urządzenie, itp.).
29. HSM musi być wyposażony co najmniej w dwa zasilacze z możliwością wymiany w trakcie działania (hot-swap).
30. HSM musi posiadać dwa interfejsy Ethernet o szybkości co najmniej 1Gb/s oraz dwa interfejsy Ethernet o szybkości 10Gb/s. Do interfejsów 10Gb/s zostaną dostarczone odpowiednie wkładki.
31. Urządzenie charakteryzuje się deklarowanym MTBF na poziomie co najmniej 100 000 godzin.
32. Urządzenia muszą umożliwiać monitorowanie stanu Urządzenia poprzez protokół SNMP.
33. Oprogramowanie dostarczone wraz z Urządzeniem musi umożliwiać zarządzanie wieloma Urządzeniami poprzez centralną graficzną konsolę zarządzania umożliwiającą m.in. przegląd stanu Urządzeń i komponentów,

zarządzanie partycjami w ilości nie mniejszej niż oferowanej, monitorowanie wydajności, aktualizację oraz przesyłanie powiadomień poprzez email.

IX. Zasady świadczenia usług gwarancji i wsparcia technicznego

1. Wykonawca zobowiązany jest zapewnić wsparcie techniczne i gwarancję producenta urządzeń lub autoryzowanego partnera serwisowego współpracującego z producentem, działającego w imieniu tego producenta, dla dostarczonych urządzeń, przez okres 36 miesięcy od dnia odbioru wskazanego w protokole odbioru końcowego.

2. **Serwis gwarancyjny realizowany będzie na następujących zasadach:**
   1) realizowany zdalnie lub stacjonarnie w Lokalizacjach, w których znajdują się Urządzenia, których dotyczy Awaria, w języku polskim. Zamawiający nie jest zobowiązany do dostarczenia Urządzeń do Wykonawcy lub producenta Urządzeń w celu usunięcia Awarii. Uszkodzone elementy Urządzeń, podlegające naprawie poza Lokalizacjami, Wykonawca zobowiązany jest odebrać na swój koszt i ryzyko, z zastrzeżeniem pkt 9 i 10 poniżej;
   2) Zamawiający jest uprawniony do dokonywania zgłoszeń w trybie 24 godziny na dobę, 7 dni w tygodniu za pośrednictwem dedykowanego portalu producenta Urządzeń lub poczty elektronicznej oraz telefonicznie w godzinach od 9:00 do 17:00 w Dni Robocze;
   3) obsługa zgłoszeń dokonanych za pośrednictwem dedykowanego portalu producenta Urządzeń lub poczty elektronicznej będzie świadczona w języku polskim lub angielskim, a zgłoszeń dokonanych telefonicznie będzie świadczona w języku polskim;
   4) za chwilę dokonania zgłoszenia Awarii, Strony uznają datę i godzinę poinformowania przez Zamawiającego o wystąpieniu Awarii, przez jeden z kanałów, o których mowa w pkt 2 powyżej. W przypadku zgłoszenia Awarii przez więcej niż jeden kanał, za chwilę dokonania zgłoszenia uznaje się datę i godzinę zgłoszenia wcześniejszego;
   5) czas usunięcia Awarii nie dłuższy niż 24 godziny od dokonania zgłoszenia przez Zamawiającego. Prawidłowość usunięcia Awarii zostanie potwierdzona w protokole usunięcia Awarii;
   6) Wykonawca zapewni usunięcie Awarii poprzez naprawę lub wymianę uszkodzonych Urządzeń na nowe, wolne od wad, objęte gwarancją, o nie gorszych parametrach od Urządzeń podlegających wymianie oraz zapewniających nie gorszy poziom bezpieczeństwa, i przeniesienie ich własności na Zamawiającego, oraz ich dostarczenie, montaż i uruchomienie w Lokalizacji, w której znajdowały się uszkodzone Urządzenia, w terminie, o którym mowa w pkt 5;
   7) W przypadku braku możliwości dotrzymania czasu usunięcia Awarii, o którym mowa w pkt 5, Wykonawca zapewni dostarczenie, montaż i uruchomienie w Lokalizacji, w terminie wskazanym w pkt 5, na czas usuwania Awarii, w pełni sprawnego urządzenia zastępczego, objętego gwarancją, o nie gorszych parametrach niż Urządzenia naprawiane oraz zapewniającego nie gorszy poziom bezpieczeństwa, oraz przygotuje i dostarczy Zamawiającemu dokumenty informujące o wykonanej zamianie w ramach gwarancji. W takim przypadku czas usunięcia Awarii to 60 Dni Roboczych od dokonania zgłoszenia Awarii przez Zamawiającego;

8) w przypadku, gdy dane Urządzenia ulegną Awarii po raz trzeci Wykonawca zapewni usunięcie Awarii poprzez wymianę uszkodzonych Urządzeń na nowe, wolne od wad, objęte gwarancją, o nie gorszych parametrach od Urządzeń podlegających wymianie oraz zapewniających nie gorszy poziom bezpieczeństwa, przenosząc ich własność na Zamawiającego, oraz dostarczy, zamontuje i uruchomi nowe Urządzenia w Lokalizacji na własny koszt i ryzyko, w terminie 25 Dni Roboczych liczonych od dnia zgłoszenia trzeciej Awarii, przy czym na czas do dnia wymiany na nowe Urządzenia Wykonawca zapewni urządzenie zastępcze, zgodnie z pkt 7 powyżej;
9) wydanie Urządzeń poza Lokalizacje w celu usunięcia Awarii lub zwrot urządzeń zastępczych będą mogły nastąpić dopiero po trwałym usunięciu danych ze wszystkich nośników danych zainstalowanych w Urządzeniach np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez gwaranta w obecności Zamawiającego i zdeponowaniu ich u Zamawiającego. W przypadku braku możliwości demontażu nośnika danych z Urządzenia, zgodnie ze standardami certyfikacji wymienionej w punkcie VIII.24 OPZ dla urządzeń HSM, Urządzenie serwisowane będzie tak, aby serwisanci oraz producent nie mieli dostępu do kluczy kryptograficznych nawet po odesłaniu Urządzenia do serwisu;
10) w przypadku stwierdzenia uszkodzenia dysku twardego, będzie on wymieniony na nowy, wolny od wad, bez konieczności jego zwrotu przez Zamawiającego i bez konieczności dokonywania dodatkowej ekspertyzy tego dysku poza Lokalizacjami. Wszelkie nośniki danych, na których znajdują się dane Zamawiającego pozostają u Zamawiającego i nie podlegają zwrotowi w ramach wymiany gwarancyjnej. W przypadku braku możliwości demontażu nośnika danych z Urządzenia, zgodnie ze standardami certyfikacji FIPS dla urządzeń HSM, Urządzenie serwisowane będzie tak, aby serwisanci oraz producent nie mieli dostępu do kluczy kryptograficznych nawet po odesłaniu Urządzenia do serwisu gwarancyjnego;
11) po usunięciu Awarii Urządzenia, Wykonawca zapewni wsparcie w odtwarzaniu danych w Urządzeniu, tak aby możliwe było korzystanie ze wszystkich funkcjonalności Urządzenia w taki sam sposób jak bezpośrednio przez Awarią. Zapewnienie backupu i jego dostarczenie pozostaje po stronie Zamawiającego;
12) warunki świadczenia serwisu gwarancyjnego nie mogą ograniczać praw Zamawiającego do:
    a) instalowania i wymiany w Urządzeniach standardowych kart i urządzeń zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego;
    b) rozporządzania zakupionymi Urządzeniami;
    c) w razie sprzedaży lub innej formy przekazania Urządzeń, gwarancja zostaje przeniesiona na nowego właściciela Urządzeń.

3. **W ramach wsparcia technicznego Zamawiający ma w szczególności prawo do:**
    1) nieograniczonego dostępu i pobierania wszystkich udostępnionych przez producenta aktualizacji, sterowników, komunikatów, baz sygnatur, Dokumentacji, baz wiedzy, instrumentów zgłaszania błędów dotyczących funkcjonowania Oprogramowania w sposób nieograniczający praw Zamawiającego do korzystania z tego Oprogramowania;
    2) aktualizacji wolnych od mechanizmów blokujących funkcje Oprogramowania, wirusów, koni trojańskich, robaków i innych szkodliwych programów, wszelkich serwisów elektronicznych udostępnianych przez producenta Oprogramowania, w tym do repozytoriów, forów dyskusyjnych i

bazy wiedzy zawierających wykazy znanych symptomów nieprawidłowego działania oraz sposobów naprawy;

3) obsługi świadczonej przez inżyniera serwisu w języku polskim, realizowanej zdalnie lub jeśli będzie to konieczne w Lokalizacji, w której Urządzenie, którego dotyczy wsparcie techniczne, zostało zainstalowane, całodobowo w Dni Robocze;
4) udzielania Zamawiającemu przez inżyniera serwisu, w szczególności konsultacji, rozstrzygania wątpliwości lub rozwiązania bieżących problemów Zamawiającego z obsługą Urządzeń i Oprogramowania;
5) dokonywania zgłoszeń dotyczących funkcjonowania Oprogramowania w trybie 24 godziny na dobę, 7 dni w tygodniu, za pośrednictwem dedykowanego portalu producenta lub poczty elektronicznej oraz telefonicznie w godzinach od 9:00 do 17:00 w Dni Robocze;
6) informowania Zamawiającego przez Wykonawcę o pojawieniu się aktualizacji w terminie nie dłuższym niż 7 dni od dnia ich publikacji przez producenta Oprogramowania oraz w przypadku krytycznych poprawek bezpieczeństwa (tzw. 0-Day patches) w terminie 24 godzin od chwili ich opublikowania.