Warszawa, 2026-08-14

ZPPZ.230.1.2025

(292920)

Do wszystkich Wykonawców

dotyczy: **Dostawa certyfikatu kwalifikowanej pieczęci elektronicznej, która będzie osadzona na urządzeniach kryptograficznych HSM (Hardware Security Module).** Identyfikator CeZ: 289259.

Z uwagi na fakt, iż do przedmiotowego **Zapytania** wpłynęły pytania od Wykonawców, Zamawiający przytacza treść pytań i udziela odpowiedzi.

Pytanie 1.

Czy 4 urządzenia HSM są połączone w klaster?

Odpowiedź 1.

Aktualnie Zamawiający oczekuje na dostawę urządzeń. Dostarczone urządzenia będą podzielone na różne środowiska: 2 urządzenia połączone w klaster na środowisku produkcyjnym oraz 2 urządzenia bez klastra na środowiska nieprodukcyjne.

Pytanie 2.

W jakim przedziale czasu będzie wykorzystywany wskazany wolumen znaczników czasu (min. 480 000) – miesięcznym/rocznym/dwuletnim?

Odpowiedź 2.

Znaczniki czasu (480 000) dotyczy rocznego okresu.

Pytanie 3.

Jaki jest oczekiwany maksymalny wolumen wydawanych znaczników czasu w określonej jednostce czasu?

Odpowiedź 3.

Maksymalnie 480 000 znaczników czasu w okresie / 12 miesięcy.

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

Pytanie 4.

Czy użytkowane rozwiązanie (biblioteka Szafir SDK) jest niezależne od dostawcy certyfikatu pieczęci, tzn. działa poprawie z dowolnym certyfikatem pieczęci kwalifikowanej dostarczonym przez dostawcę usług zaufania innego niż KIR (dostawca oprogramowania)?

Odpowiedź 4.

Tak, Zamawiający wykorzystywał pieczęć kwalifikowaną nie dostarczaną przez KIR.

Pytanie 5.

Czy Zamawiający posiada wsparcie dla użytkowanego rozwiązania (biblioteka Szafir SDK)?

Odpowiedź 5.

Tak, Zamawiający wykupuje wsparcie dla biblioteki Szafir SDK.

Pytanie 6.

Prosimy o podanie lokalizacji (miasta) w którym są zainstalowane urządzenia HSM.

Odpowiedź 6.

Urządzenia będą zainstalowane w 2 serwerowniach na terenie miasta Warszawa.

Pytanie 7.

Prosimy o potwierdzenie, że numery seryjne urządzeń HSM zaczynają się od: 46-Uxxxxx. Zgodnie z dokumentacją Producenta początek numeru seryjnego zaczynający się od 46 wskazuje, że urządzenia zostały wytworzone w fabryce posiadającej certyfikację Common Criteria.

Odpowiedź 7.

Zamawiający potwierdza, że numery seryjne urządzeń HSM zaczynają się od: 46-Uxxxxx.

Pytanie 8.

Prosimy o informację czy urządzenia posiadane przez Zamawiającego zostały skonfigurowane zgodnie z wymaganiami certyfikacji Common Criteria opisanymi w dokumencie "nShield5 Common Criteria Evaluated Configuration Guide" lub jeśli nie to prosimy o informację w jakim stanie są urządzenia HSM, czy zostały one zintegrowane z jakimiś systemami np. PKI?

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

Odpowiedź 8.

Aktualnie Zamawiający oczekuje na dostawę urządzeń. Prośba o przekazanie linku, wytycznych lub samego dokumentu nShield5 Common Criteria Evaluated Configuration Guide. Zamawiający dołoży wszelkich starań, aby urządzenia były skonfigurowane zgodnie z przekazanymi wytycznymi.

Pytanie 9.

Czy obsługa biblioteki Szafir SDK, o której mowa w OPZ jest wymogiem koniecznym, czy też wykonawca może zastąpić rozwiązanie własnym równorzędnym?

Odpowiedź 9.

Tak, obsługa biblioteki Szafir jest wymogiem koniecznym.

Pytanie 10.

Czy generowanie klucza na urządzeniach HSM i żądania o certyfikat pieczęci pozostaje po stronie Zamawiającego czy wykonawcy?

Odpowiedź 10.

Generowanie klucza na urządzeniach HSM i żądania o certyfikat pieczęci będzie wygenerowane przez Zamawiającego przy wsparciu wykonawcy.

Pytanie 11.

Czy generowanie klucza i żądania na HSM musi zostać wykonane narzędziami/aplikacjami zewnętrznymi, jeśli tak to czy Zamawiający posiada już jakieś tego typu, czy też narzędziami wbudowanymi w oprogramowanie Entrunst nShield?

Odpowiedź 11.

Według wiedzy Zamawiającego generowanie kluczy musi się odbyć wewnątrz urządzeń HSM posiadających certyfikat Common Criteria. Rolą Wykonawcy jest wskazanie jakich narzędzi należy użyć, aby spełnić wymagania formalne.

Pytanie 12.

Według jakich procedur ma zostać wygenerowany klucz i żądanie na HSM, czy Zamawiający określa procedurę wykonywania takiej czynności?

Odpowiedź 12.

Zamawiający oczekuje, że wszelkie procedury zostaną precyzyjnie określone przez Wykonawcę, a do każdego z kroków zostanie dostarczona odpowiednia dokumentacja / instrukcja, tak aby spełnić wszelkie wymagania formalne.

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

Pytanie 13.

Czy posiadany firmware i software na urządzeniach HSM Zamawiającego jest objęty certyfikacją Common Criteria?

Odpowiedź 13.

Zamawiający wskazał w zapytaniu urządzenia HSM na których będzie osadzona pieczęć, rolą wykonawcy jest weryfikacja urządzeń, przygotowanie wytycznych do ich konfiguracji – jeśli jest to wymagane i przeprowadzenie tej konfiguracji wspólnie z Zamawiającym w takim sposób, aby całość była objęta certyfikacją Common Criteria.

Pytanie 14.

Czy Zamawiający konfigurował sam urządzenia HSM czy też urządzania są do skonfigurowania przed przystąpieniem do prac?

Odpowiedź 14.

Urządzenia będą wstępnie skonfigurowane przez Zamawiającego, jeśli potrzebna będzie ich rekonfiguracja, zostanie ona przeprowadzona przez Zamawiającego według wskazówek wykonawcy.

Pytanie 15.

Jeśli urządzenia HSM są już skonfigurowane to czy Security World HSM jest jeden na wszystkie posiadane HSMy, czy też któreś urządzenia posiadają odrębne Security World'y?

Odpowiedź 15.

Urządzenia na chwilę obecną jeszcze nie są skonfigurowane. Docelowo będą oddzielne Security World’y dla środowiska produkcyjnego i środowisk nieprodukcyjnych.

Pytanie 16.

Jeśli urządzenia HSM są już skonfigurowane to czy Security World/y mają włączone następujące parametry:

-S – zablokowanie zdalnego udostępniania udziałów przez moduł

--mode=common-criteria-cmts – włączenie trybu zgodności z common-criteria-cmts

--pp-min=14 – ustawienie minimalnej długości haseł dla kart Administratora i Operatora

--pp-strength – ustawienie dodatkowych ograniczeń na złożoność haseł. Co najmniej:(1 duża litera, 1 mała litera, 1 liczba, 1 znak)

no-p – zablokowanie odzyskiwania haseł do kart w Security World

Odpowiedź 16.

Urządzenia na chwilę obecną jeszcze nie są skonfigurowane.

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

Pytanie 17.

Jak Zamawiający planuje chronić klucz dedykowany do certyfikatu pieczęci osadzony na urządzeniach HSM (zestaw kart OCS, Soft Token, Inne)?

Odpowiedź 17.

Klucze będą chronione przez zestaw kart OCS.

2026-08-14 (-) Adrian Michałuszko

Osoba sporządzająca: Marika Czarnecka

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