NFZ | Narodowy Fundusz Zdrowia
Centrala w Warszawie
Biuro Administracyjno-Gospodarcze

znak: A2P-2611-32/13

Warszawa, 20 września 2013 r.

Do wszystkich zainteresowanych

dotyczy: postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest „Dostawa systemu Infrastruktury Klucza Publicznego na potrzeby systemu RUM II oraz innych systemów wymagających PKI dla Centrali NFZ"

W dniu17 września 2013 r. do Centrali Narodowego Funduszu Zdrowia wpłynęły zapytania o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia. Na podstawie z art. 38 ust. 1 ustawy Prawo Zamówień Publicznych Zamawiający udziela następujących odpowiedzi:

W związku z zapisami SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA (SIWZ) prosimy o odpowiedź na pytanie dotyczące następujących zapisów:

Dot. odpowiedzi Zamawiającego z dnia 09.09.2013 na pytania nr 34, 35 oraz 36.
W związku z niejasnymi i nieprecyzyjnymi odpowiedziami prosimy o wyjaśnienie następujących kwestii:

1. Wykonawca na podstawie opisu zawartego w OPZ ani na podstawie odpowiedzi nr 34, 35,36, nie jest w stanie ustalić czy Zamawiający wymaga od Wykonawcy zapewnienia na poziome ciągłym przez system PKINFZ generacji kluczy w modułach sieciowych HSM z wydajnością 20 + 4 na sekundę dla usług związanych z wydawaniem certyfikatów czy raczej oczekuje że sieciowe moduły HSM okresowa będą generowały jedynie klucze urzędów CA. Wyjaśnienie tej kwestii jest bardzo istotne, gdyż wymagania postawione na urządzenia HSM a szczególności na urządzenia sieciowe HSM, powodują iż paleta dostępnych na rynku urządzeń HSM ogranicza się do kilku modeli, z których każdy umożliwia maksymalna wydajność generacji kluczy w trybie zgodności z uzyskanym certyfikatem na poziomie 1 klucza RSA2048 na sekundę co powoduje, że Wykonawca nie ma pewności czy może dostarczyć min. dwa takie moduły dla każdego ośrodka, które zapewnią generację 1 klucza RSA2048 /sekundę czy raczej powinien ich dostarczyć minimum 25 dla każdego ośrodka (uwzględniając odpowiednią redundancją/nadmiarowością) aby osiągnąć wydajność generacji kluczy na poziome 24/sekundę.

Odpowiedź:

Zamawiający udziela odpowiedzi zgodnie z treścią pytań oraz treścią wymagań do których odnoszą się zadawane pytania.

Zamawiający nie oczekuje w ramach dostarczonego systemu PKINFZ zagwarantowania (przez urządzenia HSM) generowania kluczy RSA 2048 bit na poziomie 24 klucze /sekundę. W ocenie Zamawiającego wymaganie NF.23 (i udzielane w związku z tym odpowiedzi na pytania nr 34, 35 i 36), zgodnie z treścią tego wymagania nie determinuje warunku spełnienia tego wymagania, w sposób który wymuszałby konieczności generowania kluczy przez HSM RSA2048 w takiej wydajności.

Zamawiający Potwierdza, że na potrzeby weryfikacji spełnienia warunków funkcjonalnych i wydajnościowych związanych z testami systemu, Zamawiający nie będzie weryfikował wydajności Systemu PKINFZ w zakresie generowania kluczy kryptograficznych.

2. Z odpowiedzi na pytanie nr 6 z dnia 13.09.2013 można rozumieć, że należy przyjąć do kalkulacji oferty certyfikowany moduł kryptograficzny HSM (którego certyfikat nie zawiera konieczności użycia sprzętowego modułu instalowanego w serwerze) oraz dowolny moduł sprzętowy (z wymienionych w pytaniu). Proszę o potwierdzenie czy taka jest intencja Zamawiającego? Jeśli nie to proszę o precyzyjną odpowiedź na postawione pytania.

Odpowiedź:

Zgodnie z odpowiedzią na pytanie nr 6 z dnia 13.09.2013 Zamawiający nie zaakceptuje dowolnego modułu sprzętowego. Zamawiający zaakceptuje jedynie moduł sprzętowy (przechowujący klucze, zamontowany w urządzeniu na którym uruchomiona jest dana usługa) jeśli moduł sprzętowy (token sprzętowy) będzie zgodny z warunkami certyfikacji i certyfikatem potwierdzającym wymagany poziom bezpieczeństwa [NF.20 e)] dla sprzętowego modułu kryptograficznego (HSM) w wersji sieciowej. Certyfikacja wymagana jest dla Sprzętowego modułu kryptograficznego (HSM) w wersji sieciowej, który uzyskał stosowny certyfikat i wymagania dla certyfikacji urządzenia wprost przewidywały wykorzystanie urządzenia HSM w wersji sieciowej. Wymagania dla urządzenia (sprzętowego modułu kryptograficznego HSM w wersji sieciowej) posiadającego stosowny certyfikat przewidują i wymagają zastosowanie modułu sprzętowego (tokenu sprzętowego) umieszczonego w serwerze komunikującym się przez sieć z urządzeniem HSM, dla zapewnienia szyfrowania połączenia i uwierzytelnienia tego serwera względem urządzenia HSM w wersji sieciowej. To wymaganie związane jest z certyfikacją urządzenia jakim jest „Sprzętowy moduł kryptograficzny (HSM) w wersji sieciowej" .

Tym samym użycie i wykorzystanie określonego modułu sprzętowego (do przechowywania kluczy używanych dla zapewnienia szyfrowania połączenia i uwierzytelnienia, zamontowanego w urządzeniu na którym uruchomiona jest dana usługa) musi być zgodne z wymaganiami jakie zostały dookreślone dla uzyskania certyfikacji do określonego poziomu , o której mowa w NF.20 e).

Wybór modułu sprzętowego (przechowującego klucze używane dla zapewnienia szyfrowania i uwierzytelnienia, zamontowanego w urządzeniu na którym uruchomiona jest dana usługa) jest ograniczony poprzez certyfikację modułu w wersji sieciowej [NF.20 e)]. Certyfikacja modułu kryptograficznego HSM w wersji sieciowej wymusza zastosowanie takiego trybu pracy HSM z zastosowaniem modułu sprzętowego (tokenu sprzętowego) i określa warunki w jakich zostanie utrzymana certyfikacja.

Zamawiający wymaga dostarczenie takiego rozwiązania (sprzętowych modułów kryptograficznych HSM w wersji sieciowej wraz z modułami sprzętowymi -tokenami sprzętowymi) które zapewni utrzymanie poziomu certyfikacji dla modułu w wersji sieciowej

[NF.20 e)] podczas zestawiania szyfrowanego połączenia z wykorzystaniem modułu sprzętowego i równocześnie zapewni spełnienie wymagania NF.8 i NF.76. w zakresie uwierzytelnienia. W ocenie zamawiającego jedynie moduł sprzętowy umieszczony w sposób trwały w serwerze w postaci dedykowanej dla sieciowego modułu kryptograficznego HSM karty kryptograficznej PCI/PCIe, spełnia wymagania związane z zapewnieniem uwierzytelnienia serwera względem HSM zgodnego z oczekiwanym poziomem certyfikacji.

3. Kto (Zamawiający czy Wykonawca) powinien zapewnić "odpowiednie" łącze do sieci publicznej (np. sieci Internet w celu udostępnienia realizacji procesu weryfikacji ważności certyfikatów w oparciu o usługę OCSP [FN.5,51-58] i listy CRL [Repozytorium FN.4,6,48] i serwis do unieważniania certyfikatów [FN.23, NF.6, 9,21,22]?

Odpowiedź:

Zamawiający spełni wymagania dotyczące łączy w zakresie w jakim wymagania te będą wynikały z opracowanego projektu na etapie realizacji.

4. Czy Zamawiający dopuszcza zaoferowanie przez Wykonawców systemu operacyjnego, który jest rozwijany w modelu open source, o ile producent serwera na którym będzie ten system zainstalowany umieszcza system na swojej liście kompatybilności ze serwerem?

Odpowiedź:

Zamawiający dopuszcza zaoferowanie przez Wykonawców systemu operacyjnego, który jest rozwijany w modelu open source przy spełnieniu wszystkich wymagań dotyczących systemu PKINFZ zawartych w załączniku nr 8 i 9 do SIWZ (Umowa i OPZ) w tym wymagań związanych z wymaganym poziomem dostępności systemu oraz spełnieniem warunków w zakresie usuwania błędów.

Z uwagi na fakt, że przedstawione wyjaśnienia mają wpływ na interpretację zapisów SIWZ, Zamawiający zmienia wyznaczony termin składania ofert i przedłuża go do dnia 30 września 2013 r.
W związku z powyższym:

- zapis Specyfikacji w pkt 10 **OPIS SPOSOBU PRZYGOTOWANIA OFERT ppkt 12** otrzymuje następujące brzmienie:
  Sporządzoną ofertę należy opakować w kopertę oznaczoną dokładną nazwą i adresem wykonawcy oraz napisem „POSTĘPOWANIE NR AZP – 2611 – 32/13. OFERTA – „Budowa, wdrożenie i serwis systemu Infrastruktury Klucza Publicznego na potrzeby systemu RUM II oraz innych systemów wymagających PKI dla Centrali NFZ". NIE OTWIERAĆ PRZED 30.09.2013 r. GODZ. 10:30.".

- zapis Specyfikacji w pkt 11 **MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT ppkt 1** otrzymuje następujące brzmienie:
  Oferty należy składać w zamkniętych kopertach w Narodowym Funduszu Zdrowia Centrala w Warszawie, przy ul. Grójeckiej 186, 02-390 Warszawa, pok. 0.03 **w terminie do dnia 30.09.2013 r. do godz. 10:00.**
- zapis Specyfikacji w pkt 11 **MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT ppkt 5** otrzymuje następujące brzmienie:
  Otwarcie ofert odbędzie **się w dniu 30.09.2013 r. o godz. 10:30** w Narodowym Funduszu Zdrowia Centrala w Warszawie przy ul. Grójeckiej 186, pok. 0.03.

Waldemar Rybak

Przewodniczący Komisji