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

znak: AZP-2611-32/13

Warszawa, 16 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 dniu 5 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:

Załącznik Nr 1 do SIWZ - Opis Przedmiotu Zamówienia dla postępowania dostawa systemu Infrastruktury Klucza publicznego dla Narodowego funduszu zdrowia (PKINFZ)

4.2.16 NF.20 Sprzętowy moduł kryptograficzny (HSM)
dla modułu w wersji sieciowej ma:
...
f) obsługiwać algorytmy o długości co najmniej: RSA 4096 bit, ECDSA 256 bit, funkcja skrótu SHA-256 lub SHA-512,
...
Liczba sprzętowych modułów kryptograficznych musi zapewniać właściwą wydajność dla całego systemu, oraz spełnienie wymagań wysokiej dostępności.
dla modułu w wersji dla urzędów Root CA ma:
...
c) obsługiwać algorytmy o długości co najmniej: RSA 4096 bit, ECDSA 256 bit, funkcja skrótu SHA-256 lub SHA-512,
4.4.4 NF.35 Wymaganie wysokiej dostępności usługi
Usługi: FN.1 – FN.11 określone w ust. 3.2.1 do ust. 3.2.11, udostępniane z wykorzystaniem Ośrodka Podstawowego mają być dostępne w trybie wysokiej dostępności (HA) z możliwością rozłożenia ich obciążenia (Load Balancing).
Usługi FN.3 określone w ust. 3.2.3, FN.4 określone w ust. 3.2.4, FN.5 określone w ust. 3.2.5, FN.9 określone w ust. 3.2.9, FN.11 określone w ust. 3.2.11, udostępniane z wykorzystaniem Ośrodka Zapasowego mają być dostępne w trybie wysokiej dostępności (HA) z możliwością rozłożenia ich obciążenia (Load Balancing).
4.6.4 NF.62 Wydzielenie funkcjonalności
Każda ze zdefiniowanych grup funkcjonalności dla usług musi pozwalać na jej logiczne i fizyczne

wydzielenie z systemu i odseparowanie. Grupy funkcjonalności:
I grupa: FN.1; FN.2; FN.3; FN.4, wymienione w ust. 3.2.1, 3.2.2, 3.2.3, 3.2.4,
II grupa: FN.5, wymieniona w ust. 3.2.5,
III grupa: FN.6, wymieniona w ust. 3.2.6,
IV grupa: FN.7, FN.8, wymieniona w ust. 3.2.7 i 3.2.8,
V grupa: FN.9, wymieniona w ust. 3.2.9,
VI grupa: FN.10, wymieniona w ust. 3.2.10,
VII grupa: FN.11. wymieniona w ust. 3.2.11.
Każda ze zdefiniowanych grup musi być możliwa do zastąpienia w przyszłości przez inny produkt przy zachowaniu funkcjonalności całego rozwiązania.
oraz dotyczy odpowiedzi NFZ na pytania nr 35 z dnia 30.08.2130
Pytanie 35
...
Czy, przez jaki czas i w jakim zakresie powinny być przechowywane listy CRL urzędów CA o których mowa w od NF.21 do NF.26?
Odpowiedź:
Listy CRL maja być przechowywane przez okres 10 lat w zakresie umożliwiającym dostęp do tych danych z systemu.
oraz dotyczy odpowiedzi NFZ na pytania nr 102 z dnia 30.08.2130
Pytanie 102.
Dotyczy OPZ NF.71; W jaki sposób Zamawiający zamierza testować wykonany backup? Czy wykonawca musi dostarczyć takie środowisko?
Odpowiedź:
Testy poprawności wykonanego backupu będą odbywały się w środowisku testowym.
W związku z powyższym prosimy o wyjaśnienie następujących kwestii:

Pytanie nr 1

Czy uszkodzenie pojedynczego elementu sprzętowego (przy awarii typu: single point of failure – np. jednego modułu sieciowego HSM czy serwera) w ośrodku podstawowym może spowodować spadek wydajności ośrodka podstawowego w zakresie wydajności o których mowa w punkcie 4.3 (NF.21..NF.31) (jeżeli tak to prosimy o wskazanie o ile może spaść) czy raczej należy przyjąc że wydajność musi zostać utrzymana na poziomach określonych w punkcie 4.3 (NF.21..NF.31)?

Odpowiedź:

Odpowiedź zawiera się w opublikowanej w dniu 07.08.2013 na stronie Zamawiającego odpowiedzi na pytanie nr 5.

Pytanie nr 2

W związku z odpowiedzią na pytanie nr 35 o treści **"Listy CRL maja być przechowywane przez okres 10 lat w zakresie umożliwiającym dostęp do tych danych z systemu"** oraz koniecznością oszacowania pojemności nośników danych (o których mowa w NF.77) na okres 6-ciu lat prosimy o doprecyzowanie częstotliwość generacji CRL dla urzędów CA X.509 (w tym dla RootCA i SubCA dla kart KUZ i SM).

Odpowiedź:

Częstotliwość generacji list CRL zostanie sprecyzowana na etapie projektowania. Należy jednak założyć, że będzie generowana nie częściej niż raz dziennie.

Pytanie nr 3

Czy na potrzeby oszacowania pojemności nośników danych można przyjąć, że system będzie generował na potrzeby każdego urzędu CA (wydającego certyfikaty typu X.509) jedną „pełną" listę CRL dziennie?

Odpowiedź:
Częstotliwość i warunki generacji list CRL zostaną sprecyzowane na etapie projektowania. Należy jednak założyć, że będą generowane nie częściej niż raz dziennie.

Pytanie nr 4
Ze względu na konieczność oszacowania pojemności nośników danych prosimy o wyjaśnienie czy każde z repozytoriów (Repozytorium LDAP i Repozytorium HTTP) o których mowa w wymaganiach FN.6, FN.59, NF.10, NF.31 musi przechowywać komplet certyfikatów wydanych przez wszystkie urzędy CA (3x40 mln + 2x300 tys. = ok. 120 mln certyfikatów)?
Odpowiedź:
Zamawiający oczekuje aby całe Repozytorium przechowywało komplet aktywnych certyfikatów wydanych przez wszystkie urzędy.

Pytanie nr 5
Czy usługa „Repozytorium HTTP" będzie udostępniana w sieci publicznej (np. Internet) i czy powinna posiadać własne PROXY?
Odpowiedź:
Odpowiedź zawiera się w opublikowanej w dniu 30.08.2013 na stronie Zamawiającego odpowiedzi na pytanie nr 11 (32 strona).

Pytanie nr 6
Czy usługa „Repozytorium LDAP" będzie udostępniana w sieci publicznej (np. Internet) i czy powinna posiadać własne PROXY?
Odpowiedź:
Odpowiedź zawiera się w opublikowanej w dniu 30.08.2013 na stronie Zamawiającego odpowiedzi na pytanie nr 11 (32 strona).

Pytanie nr 7
Prosimy o wyjaśnienie czy wydajność usługi o której mowa w NF.24 na poziomie 4 certyfikaty na sekundę dotyczy każdego z dwóch rodzajów certyfikatów osobno (łącznie 8 certyfikatów na sekundę) czy raczej chodzi o wydajność łączną (sumaryczną) dla obu rodzaju certyfikatów?
Odpowiedź:
Odpowiedź zawiera się w opublikowanej w dniu 09.09.2013 na stronie Zamawiającego odpowiedzi na pytanie nr 34.

Pytanie nr 8
W związku z odpowiedzią na pytanie nr 102 prosimy o wyjaśnienie czy środowisko testowe w związku z koniecznością testowego odtwarzania backup'u systemu produkcyjnego w środowisku testowym może być podłączone (np. przez sieć LAN lub SAN) do wspólnego systemu backup'u ze środowiskiem produkcyjnym, czy raczej zamawiający przewiduje przenoszenie taśm z backup'em ze środowiska produkcyjnego do testowego i prowadzenia prób odtwarzania w ten sposób? Jeżeli Zamawiający przewiduje przenoszenie taśm w celu przetestowania backupu to prosimy o informację czy w związku z tym Zamawiający będzie wymagał aby Wykonawca dostarczył odpowiednia bibliotekę taśmową dla środowiska testowego, umożliwiającą testowanie procedur które dla środowiska produkcyjnego powstaną właśnie z uwzględnieniem biblioteki taśmowej dla tego środowiska.
Odpowiedź:
Zamawiający przewiduje przenoszenie taśm z backup'em ze środowiska produkcyjnego do testowego i prowadzenia prób odtwarzania w ten sposób, w celu przetestowania backupu. W związku z tym Zamawiający będzie wymagał aby Wykonawca dostarczył odpowiednią bibliotekę

taśmową dla środowiska testowego, umożliwiającą testowanie procedur, które dla środowiska produkcyjnego powstaną właśnie z uwzględnieniem biblioteki taśmowej dla tego środowiska.

Pytanie nr 9

Prosimy o wyjaśnienie od jakiego momentu/daty/zdarzenia macierze o których mowa w NF.77 muszą utrzymać dane przez 6 lat?

Odpowiedź:

Dostarczone macierze przeznaczone do przechowywania danych muszą posiadać pojemność umożliwiającą przechowanie danych w okresie min 6 lat pracy produkcyjnej systemu.

Pytanie nr 10

Czy po uszkodzeniu dowolnego elementu wykorzystanego do realizacji usług pracujących w trybie wysokiej dostępności HA (w rozumieniu NF.35) system ma samodzielnie/automatycznie (bez udziału obsługi człowieka) podjąć dalsze działanie wykorzystując pozostałe sprawne elementy z zapewnieniem wydajności określonej w wymaganiach w od NF.21 do NF.30 czy raczej na potrzeby takiej „wyjątkowej" sytuacji Zamawiający dopuszcza, że System lub jego moduł przerwie swoją pracę i będzie oczekiwał na interwencje operatora (np. na rekonfigurację i ręczne przesterowanie), która spowoduje przywrócenie poprawnej pracy systemu w oparciu o pozostałe sprawne elementy. Jakimi kryteriami Zamawiający będzie się kierował przy ocenie czy dostarczone rozwiązanie spełnia te (NF.35) wymagania dla usług, które mają pracować w trybie wysokiej dostępności HA?

Odpowiedź:

Przyjęte przez Wykonawcę rozwiązania techniczne i organizacyjne dotyczące dostarczanego systemu muszą umożliwić spełnienie wymagań w zakresie wymaganego poziomu dostępności systemu (NF.34) oraz zapewnić wydajność określoną w wymaganiach w od NF.21 do NF.30.
Zamawiający wymaga spełnienia wymagania NF.35 w zakresie zapewnienia wysokiej dostępności usług. Zakres realizacji tego wymagania w odniesieniu do poszczególnych usług oraz wymaganego poziomu dostępności systemu zdefiniowanych w wymaganiu NF.34, decyduje o wyborze rozwiązania proponowanego przez Wykonawcę. Funkcjonalność ta zostanie zweryfikowana podczas testów systemu. Zamawiający oczekuje realizacji usług pracujących w trybie wysokiej dostępności z możliwością samodzielnego/automatycznego przełączenia przynajmniej w zakresie usług które są świadczone w sposób ciągły. Zamawiający nie będzie wymagał funkcjonalności samodzielnego/automatycznego przełączenia w odniesieniu do części systemu realizującego funkcjonalność RootCA i RootCA CVC.

Pytanie nr 11

Ze względu na brak zdefiniowania pojęć „tryb wysokiej dostępności HA" i „możliwość rozłożenia obciążenia LoadBalancing" (wymienionych w NF.35) zarówno w umowie jak i OPZ (np. w definicjach) prosimy o doprecyzowanie w Umowie lub OPZ obu definicji, które wyjaśnią w szczególności jakimi kryteriami Zamawiający będzie się kierował przy ocenie czy dostarczone rozwiązanie spełnia te wymagania w odniesieniu do poszczególnych środowisk (produkcyjnego i testowego), ośrodków (podstawowy i zapasowy), komponentów składowych (sprzęt oprogramowanie) oraz odpowiednio funkcjonalności i grup wymagań funkcjonalnych.

Odpowiedź:

Zamawiający wymaga spełnienia wymagania NF.35 w zakresie zapewnienia wysokiej dostępności usług z możliwością rozłożenia ich obciążenia. Zakres realizacji tego wymagania w odniesieniu do poszczególnych usług oraz wymaganego poziomu dostępności systemu zdefiniowanych w wymaganiu NF.34, decyduje o wyborze rozwiązania proponowanego przez Wykonawcę.

Pytanie nr 12

Czy ze względu na wymóg zapewnienia **dla ośrodka zapasowego dla środowiska produkcyjnego** dla wybranych wskazanych w NF.35 usług (takich jak FN.3,4,5,9,11) oraz przy założeniu że pojedyncze urządzenie zapewnia niezbędną wydajność, Zamawiający analogicznie do odpowiedzi na pytania nr 16 i 17, z dnia 08.08.2013 będzie wymagał dostarczenia minimum dwóch macierzy dyskowych (o których mowa w NF.77) oraz minimum dwóch sieciowych modułów kryptograficznych (o których mowa w NF.20), czy raczej zaakceptuje dostarczenie do ośrodka zapasowego jednej macierzy i jednego sieciowego modułu kryptograficznego?

Odpowiedź:

Zamawiający zgodnie z wymaganiami zawartymi w OPZ wymaga dostarczenia rozwiązania dla ośrodka zapasowego uwzględniającego wymagania wysokiej dostępności, Zamawiający wymaga dostarczenie minimum dwóch macierzy i dwóch sprzętowych modułów kryptograficznych do ośrodka zapasowego, w celu spełnienia wymagania wysokiej dostępności dla ośrodka zapasowego (dla wybranych wskazanych w NF.35 usług).

Pytanie nr 13

Czy ze względu na zapewnienie wysokiej dostępności HA (w rozumieniu NF.35) w kontekście usług określonych w FN.1, FN.2, FN.3 i FN.4, Zamawiający **zarówno dla ośrodka podstawowego i zapasowego dla środowiska produkcyjnego** będzie wymagał, aby każdy urząd Root CA (w tym Root CA [FN.37] i RootCA CVC [FN.66]) był oparty o minimum dwa sprzętowe moduły HSM (o których mowa w NF.20 -moduł w wersji dla Root CA), co łącznie wymaga dostarczenia dla tych urzędów (typu RootCA) dla obu ośrodków minimum 8 modułów HSM? Jeżeli interpretacja Zamawiającego jest odmienna to prosimy o wyjaśnienie jak należy interpretować przytoczone wymagania OPZ w tym zakresie i jaka minimalna ilość modułów HSM (o których mowa w NF.20 – moduł w wersji dla Root CA) powinna zostać dostarczona.

Odpowiedź:

Zamawiający nie wymaga aby urzędy Root CA i Root CA CVC w ośrodku zapasowym były zbudowane w trybie zapewniającym wysoką dostępność. Usługi wymienione do pracy w trybie wysokiej dostępności dla ośrodka zapasowego nie zawierają wymagania w odniesieniu do RootCA i Root CA CVC.

Pytanie nr 14

Czy dostarczone w ramach postępowania urządzenia HSM (o których mowa w NF.20) będą musiały wykonywać podczas eksploatacji systemu operacje na kluczach ECDSA czy raczej można przyjąć że zamawiający nie będzie ich wykorzystywał oraz, że zgodnie z wymaganiami NF.20 f) i wersja dla RootCA, c) muszą one tylko posiadać taką funkcjonalność ale zamawiający jeżeli będzie jej wymagał w przyszłości będzie mógł ją aktywować za dodatkową opłatą?

Odpowiedź:

Zgodnie z Wymaganiem NF.20 dostarczony w ramach realizacji Systemu PKINFZ sprzętowy moduł kryptograficzny (HSM) ma obsługiwać algorytmy o długości co najmniej: RSA 4096 bit, ECDSA 256 bit, funkcja skrótu SHA-256 lub SHA-512 niezależnie czy urządzenia HSM (o których mowa w NF.20) będą musiały od pierwszego dnia działania systemu wykonywać operacje na kluczach ECDSA.

Przewodniczący Komisji
Waldemar Rybak