Warszawa, dnia 08.06.2015 r.

MINISTERSTWO SPRAWIEDLIWOŚCI
Al. Ujazdowskie 11
00-567 WARSZAWA
Centrala tel. 521-28-88

BA-F-3710-27/15

Do Wykonawców

Dotyczy: postępowania o udzielenie zamówienia publicznego na „Zaprojektowanie, dostawę i wdrożenie systemu bezpiecznego zdalnego dostępu do sieci teleinformatycznej".
Znak sprawy postępowania nadany przez Zamawiającego: **BA-F-II-3710-27/15.**

Ministerstwo Sprawiedliwości, jako Zamawiający w przedmiotowym postępowaniu o udzielenie zamówienia publicznego, działając zgodnie z art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2013 r. poz. 907 z późn. zm.), zwanej dalej „ustawą", w związku z art. 38 ust. 1 i 1 a ustawy, przekazuje treść zapytań wraz z wyjaśnieniami treści Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej „SIWZ":

Pytanie 1.
Do pkt. 1.10. Czy pod pojęciem „samodzielna zdalna recertyfikacja" należy rozumieć operację generowania certyfikatu przed upływem ważności dotychczasowego?

Odpowiedź:
Zamawiający uprzejmie wyjaśnia i informuje, że pod pojęciem samodzielna zdalna recertyfikacja, należy rozumieć operację generowania certyfikatu przed upływem ważności dotychczasowego, jak również po upływie ważności certyfikatu.

Pytanie 2.
Czy Zamawiający dopuszcza również realizację punktu 1.14 oraz 1.9-1.11 przy pomocy zewnętrznego portalu dostępnego przy użyciu przeglądarki sieci web? Opisane wymaganie znacząco ogranicza bowiem liczbę potencjalnych rozwiązań, a co za tym idzie konkurencję.

Odpowiedź:
Zamawiający uprzejmie informuje, że dopuszcza realizację punktów 1.9-1.11 oraz 1.14 przy pomocy zewnętrznego portalu dostępnego przy użyciu przeglądarki sieci WEB.

Pytanie 3.
Pytanie dotyczy wymagań osobowych tj. „co najmniej 1 osoba na stanowisku inżyniera ds. wdrożenia i utrzymania spełniająca poniższe wymagania posiada znajomość technologii PKI jaka będzie wykorzystana w projekcie potwierdzoną posiadaniem aktualnego certyfikatu poświadczającego zdanie egzaminu".
Firma Microsoft, będąca producentem rozwiązania Microsoft CA użytkowanego przez Zamawiającego od roku 2003 nie prowadzi certyfikacji dedykowanej dla systemów klasy PKI. Na chwilę obecną w ścieżce certyfikacyjno-szkoleniowej MCSE: Server Infrastructure są zawarte elementy PKI opartego o Windows Server 2012. W związku z powyższym prosimy Zamawiającego o potwierdzenie, że okazanie przez Wykonawcę wyżej wymienionego certyfikatu będzie uznane za spełnienie tego wymagania.

Odpowiedź:
Zamawiający uprzejmie informuje, że potwierdza, że okazanie przez Wykonawcę aktualnego certyfikatu poświadczającego zdanie egzaminu w ścieżce certyfikacyjno-szkoleniowej MCSE Windows Server 2012 zawierającego elementy PKI, będzie uznane za spełnienie tego wymagania.

Niniejszym zwracam się z uprzejmą prośbą o udzielenie odpowiedzi na poniższe pytania dotyczące wymagań określonych w **Załączniku nr 1 do Umowy OPIS PRZEDMIOTU ZAMÓWIENIA** – pytania 4-14.

Pytanie 4.
Pkt. 1.2
Czy certyfikat ma być przechowywany na tokenie USB wymienionym w p. 3 OPZ ?

Odpowiedź:
Certyfikat ma być przechowywany na tokenie USB wymienionym w punkcie 3 OPZ.

Pytanie 5.
Pkt. 1.3
W oparciu o jakie rozwiązania techniczne (urządzenie, producent, model, wersja) w infrastrukturze Zamawiającego będą realizowane połączenia VPN ?

Odpowiedź:
Urządzenie bezpieczeństwa firewall urządzenie: PaloAltoPalo 5050, producent: AltoNetworks wersja 6.06 (GlobalProtect wersja 2.04).

Pytanie 6.
Pkt. 1.16
Jakie systemy operacyjne są zainstalowane na stacjach objętych systemem? Czy stacje są wyposażone w moduły TPM ?

Odpowiedź:
Stacje klienckie objęte systemem mają zainstalowany system operacyjny Microsoft Windows 8.1 Pro i są wyposażone w moduły TPM.

Pytanie 7.
Pkt. 2.
a) Czy w kontekście punktu 1.3 Wykonawca ma dostarczyć licencje na VPN ?
b) Czy w kontekście punktu 1.4 Wykonawca ma dostarczyć licencje na NAC ?
c) Czy w kontekście punktu 1.14 Wykonawca ma dostarczyć licencje na oprogramowanie MS Office ?

Odpowiedź:
Ad. a) Wykonawca nie musi dostarczać licencji na VPN.
Ad. b) Wykonawca nie musi dostarczać licencji na NAC.
Ad. c) Wykonawca nie musi dostarczać licencji na MS Office.

Pytanie 8.
Pkt. 6.
Prosimy o podanie danych szczegółowych dotyczących Network HSM (producent, model). Czy Zamawiający zapewnia niezbędne licencje do podłączenia kolejnych aplikacji?

Odpowiedź:
Networks HSM producent: Thales e-Security model: nShield Connect 500+. Zamawiający dysponuje jedną niewykorzystaną licencją kliencką dla HSM. Zamawiający nie zapewnia niezbędnych licencji do podłączenia kolejnych aplikacji.

Pytanie 9.
Pkt. 8.2
Prosimy o informację na podstawie jakich kryteriów zostanie określony właściwy priorytet w przypadku wystąpienia Problemu?

Odpowiedź:
Wysoki – system nie pracuje, brak możliwości pracy z systemem dla wszystkich użytkowników, całkowita awaria w ramach jednego procesu biznesowego.
Średni – zakłócenia procesów biznesowych, użytkownicy nie mogą wykonywać wszystkich transakcji w ramach danego procesu, znaczące przestoje w pracy systemu.
Niski – krótkie przestoje w pracy systemu, spadek wydajności systemu. Wnioski Zamawiającego, prośba o analizę, zapytanie.

Pytanie 10.
Pkt. 10
Czy Zamawiający ma na myśli dedykowany numer wyłącznie na potrzeby tego projektu, czy chodzi o numer dedykowany dla zespołu wsparcia serwisowego Wykonawcy?

Odpowiedź:
Dedykowany numer telefoniczny do bezpośredniego specjalisty serwisowego Wykonawcy.

Pytanie 11.
Pkt. 12
Czy Zamawiający przewiduje również możliwość zdalnego dostępu VPN dla Wykonawcy, w celu świadczenia usługi wsparcia?

Odpowiedź:
Zamawiający nie przewiduje zdalnego dostępu VPN dla Wykonawcy w celu świadczenia usługi wsparcia.

Pytanie 12.
Pkt. 16.5
Jaki system kopii bezpieczeństwa wykorzystuje obecnie Zamawiający (producent, nazwa oprogramowania, wersja).

Odpowiedź:
Zamawiający wykorzystuje obecnie system kopii bezpieczeństwa producenta: EMC, nazwa: Networker, wersja: 8.1.1.6.Build.321.

Pytanie 13.
Pkt. 16.11
Czy w zakres wdrożenia wchodzi uruchomienie narzędzi do monitorowania wymienionych parametrów?

Odpowiedź:
W zakres wdrożenia nie wchodzi uruchomienie narzędzi do monitorowania.

Pytanie 14.
Pkt. 18
Czy niezbędne platformy sprzętowe i systemowe dla części centralnej systemu dostarcza Zamawiający?

Odpowiedź:
Zamawiający dostarczy zasoby w postaci maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows Serwer 2012 R2.

Pytanie 15.
Zamawiający w Specyfikacji Istotnych Warunków Zamówienia w Rozdziale V pkt. 3 ppkt. b wymaga, aby osoba na stanowisku inżyniera ds. wdrożenia i utrzymania posiada znajomość technologii PKI jaka będzie wykorzystana w projekcie potwierdzoną posiadaniem aktualnego certyfikatu poświadczającego zdanie egzaminu i posiadała aktualny certyfikat poświadczający znajomość technologii Microsoft - poziom MCSE lub równoważny.

Czy przy spełnieniu znajomości znajomość technologii PKI jaka będzie wykorzystana, potwierdzonej posiadaniem aktualnego certyfikatu poświadczającego zdanie egzaminu Zamawiający dopuszcza, aby osoba na stanowisku inżyniera ds. wdrożenia i utrzymania posiadała inne certyfikaty, w tym znajomość technologii Microsoft - poziom MCSA?

Odpowiedź:
Posiadanie przez osobę na stanowisku inżyniera ds. wdrożenia i utrzymania jedynie certyfikatu MCSA, przy spełnieniu warunku znajomości technologii PKI nie spełnienia kryterium Zamawiającego. Egzamin certyfikacyjny MCSA obejmuje mniejszy zakres wiedzy i nie może być uznany za równoważny z certyfikatem MCSE.

Pytanie 16.
Zwracamy się z uprzejmą prośbą o wskazanie wartości zamówienia w Postępowaniu. Jednocześnie informujemy, ze zgodnie z par 2 ust. 1 pkt 3) Rozporządzenia Prezesa Rady Ministrów z dnia 26 października 2010 r. w sprawie protokołu postępowania o udzielenie zamówienia publicznego (Dz. U. z 2010 r., Nr 223, poz. 1458), wartość zamówienia jest obligatoryjną informacją, którą Zamawiający zamieszcza w Protokole Postępowania.

Odpowiedź:
Zamawiający uprzejmie informuje, że wartość zamówienia wynosi **561 892,50 zł** netto, w tym:

- wartość zamówienia podstawowego wynosi **480 250,00 zł** netto,
- wartość zamówienia uzupełniającego wynosi **81 642,50 zł** netto.

Jednocześnie, Zamawiający uprzejmie wyjaśnia i informuje, że zgodnie z zapisami pkt. 2 ust. 2 protokołu postępowania w trybie przetargu nieograniczonego określonego na druku zp-pn, wartość zamówienia można wypełnić po otwarciu ofert, zatem nie na obecnym etapie postępowania.

Pytanie 17.
Prosimy o podanie modelu Network HSM wykorzystywanego przez Zamawiającego wraz z wyszczególnieniem posiadanych przez urządzenie interfejsów komunikacyjnych (np. CSP , PKCS#11).

Odpowiedź:
Networks HSM producent: Thales e-Security model: nShield Connect 500+. Wspierane interfejsy aplikacyjne: PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI, CNG, nCore.

Pytanie 18.
Czy Zamawiający zakłada wykorzystanie innych poziomów PKI (SubCA) budowanych w oparciu o technologie inne niż Microsoft CA, czy zakładane jest wykorzystanie RootCA do wydawania certyfikatów dla użytkowników końcowych?

Odpowiedź:
Zamawiający zakłada zbudowanie innych poziomów CA, podległych w stosunku do istniejącego RootCA. Dopuszcza się wykorzystanie podległych SubCA wykonanych w technologii innej niż Microsoft. Serwer RootCA wystawia certyfikaty wyłącznie dla urzędów podległych.

Pytanie 19.
Czy udostępnienie użytkownikowi kodu PUK do tokenu jest dopuszczalnym schematem realizacji zdalnego resetu hasła/PINU do tokenów? Jeśli nie, to jakie wymagania powinna spełniać ta funkcjonalność?

Odpowiedź:
Udostępnienie użytkownikowi kodu PUK nie jest dopuszczalnym schematem realizacji zdalnego resetu hasła/PINU do tokenów. Zdalny resetu hasła/PINU do tokenów może być realizowany np. poprzez wykorzystane portalu webowego, Szczegółowe ustalenia będą określone na etapie uzgadniania projektu.

Pytanie 20.
Czy udostępnienie użytkownikowi kodu PUK do tokenu jest dopuszczalnym schematem realizacji funkcjonalności zdalnego odblokowywania zablokowanych tokenów realizowanego samodzielnie przez użytkowników? Jeśli nie, to jakie wymagania powinna spełniać ta funkcjonalność?
Pobranie kluczy deszyfrujących może być realizowane np. poprzez wykorzystane portalu webowego, Szczegółowe ustalenia będą określone na etapie uzgadniania projektu.

Odpowiedź:
Udostępnienie użytkownikowi kodu PUK nie jest dopuszczalnym schematem realizacji funkcjonalności zdalnego odblokowywania zablokowanych tokenów realizowanego samodzielnie przez użytkowników. Odblokowywanie zablokowanych tokenów może być realizowane np. poprzez wykorzystane portalu webowego, Szczegółowe ustalenia będą określone na etapie uzgadniania projektu.

Pytanie 21.
Jakie są wymagania funkcjonalne dotyczące procesu pobrania "online" starych kluczy deszyfrujących podczas próby odszyfrowania wiadomości w oprogramowaniu "outlook"? Czy proces ma być transparentny dla użytkownika, czy użytkownik ma być wyłączni informowany w jaki sposób może pobrać klucz do deszyfrowania?

Odpowiedź:
Pobranie kluczy deszyfrujących może być realizowane np. poprzez wykorzystane portalu webowego. Wykorzystywany mechanizm powinien umożliwiać użytkownikowi zidentyfikowanie i pobranie konkretnego klucza do deszyfrowania. Szczegółowe ustalenia będą określone na etapie uzgadniania projektu.

Wyjaśnienia treści SIWZ są wiążące dla wszystkich Wykonawców i należy je uwzględnić przy sporządzaniu i składaniu oferty.

Zastępujący Dyrektora Generalnego
Ministerstwa Sprawiedliwości

Jan Paziewski
Dyrektor Departamentu Budżetu
i Efektywności Finansowej