KOMENDA GŁÓWNA POLICJI
BIURO FINANSÓW

02-642 Warszawa
ul. Domaniewska 36/38

Dyrektor 60-131-23
Z-ca Dyrektora 60-131-75

fax. 601-26-94
845-10-76

Warszawa, 22.02 2008 r.

FZ - 972 /08

Do wykonawców
ubiegających się o udzielenie
zamówienia publicznego

dot. postępowania o udzielenie zamówienia publicznego na zawarcie umowy ramowej na okres 4 lat, na zakup usług transmisji danych GPRS/EDGE w ramach APN połączonego z siecią Zamawiającego oraz dostawa i aktywacja kart SIM dla terminali mobilnych użytkowanych w Policji - sprawa nr 242/BŁiI/07/BP

Zgodnie z art. 38 ust. 2 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (Dz.U. z 2007r. Nr 223, poz. 1655 - ustawa Pzp) poniżej podaję treść pytań, które wpłynęły do Zamawiającego oraz udzielonych na nie odpowiedzi.

Pytanie1:
Czy Zamawiający dokona zmiany komparycji umowy ramowej poprzez wprowadzenie danych jednego podmiotu po stronie wykonawcy?
Odpowiedź 1:
Zamawiający dokona zmiany komparycji umowy ramowej poprzez wprowadzenie danych jednego podmiotu po stronie wykonawcy.

Pytanie 2:
Proszę o szczegółowy opis interfejsu CSP i PKCS#11.
Odpowiedź 2:
Interfejsy MSCSP i PKCS#11 muszą być zgodne z opisami standardów.

Pytanie 3:
Proszę o wskazanie referencyjnego dokumentu opisującego normę lub standard CSP i PKCS#11.
Odpowiedź 3:
Dokumenty opisujące wyżej wymienione standardy znajdują się na stronach Microsoftu oraz RSA Laboratories.
Adresy stron:
http://msdn2.microsoft.com/en-us/library/aa380252%28VS.85%29.aspx#csp_functions
http://www.rsa.com/rsalabs/node.asp?id=2133
ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf

Pytanie 4:
Proszę o wyspecyfikowanie funkcji bibliotek CSP i PKCS#11, które mają być wykorzystywane przez urządzenie MTN i/lub oprogramowanie Centaur PR i Mobil E-gina.
Odpowiedź 4:
Biblioteki CSP i PKCS#11 mają spełniać standard w pełnym zakresie

Pytanie 5:
Proszę o szczegółową specyfikację aplikacji Mobil e-Gina.
Odpowiedź 5:
Specyfikacja aplikacji nie jest niezbędna do realizacji dostawy uniwersalnych bibliotek CSP i PKCS#11. Jeśli dostarczone biblioteki MSCSP i PKCS#11 będą zgodne ze standardami, będą współpracowały z Mobile e-Gina.

Pytanie 6:
Proszę o dokładne opisanie specyfikacji sposobu implementacji funkcji kryptograficznych wykorzystywanych przez aplikacje e-Gina.
Odpowiedź 6:
Specyfikacja aplikacji nie jest niezbędna do realizacji dostawy uniwersalnych bibliotek CSP i PKCS#11. Jeśli dostarczone biblioteki MSCSP i PKCS#11 będą zgodne ze standardami, będą współpracowały z Mobile e-Gina.

Pytanie 7:
Prosimy o wyjaśnienie jak ma być realizowane wylogowanie w przypadku zwykłego użytkownika i administratora PIN?
Odpowiedź 7:
Są to funkcjonalności Mobile e-Gina. Specyfikacja tej aplikacji nie jest niezbędna do realizacji dostawy uniwersalnych bibliotek CSP i PKCS#11. Jeśli dostarczone biblioteki MSCSP i PKCS#11 będą zgodne ze standardami, będą współpracowały z Mobile e-Gina.

Pytanie 8:
Prosimy o wyjaśnienie jak ma przebiegać zmiana kodu PIN przez zwykłego użytkownika?
Odpowiedź 8:
Są to funkcjonalności Mobile e-Gina. Specyfikacja tej aplikacji nie jest niezbędna do realizacji dostawy uniwersalnych bibliotek CSP i PKCS#11. Jeśli dostarczone biblioteki MSCSP i PKCS#11 będą zgodne ze standardami, będą współpracowały z Mobile e-Gina.

Pytanie 9:
Prosimy o wyjaśnienie jak ma przebiegać odblokowanie kodu PIN przez administratora PIN?
Odpowiedź 9:
Są to funkcjonalności Mobile e-Gina. Specyfikacja tej aplikacji nie jest niezbędna do realizacji dostawy uniwersalnych bibliotek CSP i PKCS#11. Jeśli dostarczone biblioteki MSCSP i PKCS#11 będą zgodne ze standardami, będą współpracowały z Mobile e-Gina.

Pytanie 10:
Prosimy o wyjaśnienie jak mają być nadawane wartości ID kluczy w kontenerach CSP tak, aby później można było sięgać do materiału kryptograficznego przez PKCS (standard CSP nie przewiduje możliwości podania identyfikatora importowanego klucza)?
Odpowiedź 10:
Zamawiający nie określa wzajemnej współpracy komponentów dostarczonych przez Wykonawcę.

Pytanie 11:
Prosimy o wyjaśnienie, w jaki sposób ma działać usuwanie kontenerów CSP w trybie silent?
Odpowiedź 11:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu CSP.

Pytanie 12:
Prosimy o wyjaśnienie, w jaki błąd CSP powinien być zwracany przy próbie logowania, gdy PIN jest niepoprawny?
Odpowiedź 12:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu CSP.

Pytanie 13:
Prosimy o wyjaśnienie, w jaki błąd CSP powinien być zwracany przy próbie logowania, gdy PIN jest zablokowany?
Odpowiedź 13:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu CSP.

Pytanie 14:
Prosimy o wyjaśnienie w jakie powinny być dopuszczalne długości kodów PIN/PUK oraz z jakich znaków mogą się składać kody PIN/PUK ?
Odpowiedź 14:
Zamawiający wymaga, aby długość kodów PIN/PUK była w przedziale 4 do 8 znaków (cyfr i liter), przy czym większa długość jest również dopuszczalna.

Pytanie 15:
Prosimy o wyjaśnienie w jaki sposób mają być obsługiwane sytuacje, w których do komputera podłączone jest wiele czytników PCSC ?
Odpowiedź 15:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu CSP.

Pytanie 16:
Prosimy o wyjaśnienie, jaki błąd zwrócić w PKCS#11 przy generowaniu/dodawaniu więcej niż jednego obiektu tego samego typu (klucz prywatny/publiczny, certyfikat) do slotu?
Odpowiedź 16:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu PKCS#11.

Pytanie 17:
Prosimy o zdefiniowanie czy możliwa jest początkowa inicjacja slotu kodem PUK – funkcja C_InitToken (oraz zdefiniowanie czy możliwa jest reinicjalizacja)
Odpowiedź 17:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu PKCS#11.

Pytanie 18:
Prosimy o wyjaśnienie dokładnej semantyki zarządzania kodami PIN/PUK, która realizowana jest przez funkcje C_InitToken, C_InitPin, C_Login?
Odpowiedź 18:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu PKCS#11.

Pytanie 19:
Czy wykorzystujemy użytkownika SO do odblokowywania kodów PIN, jeżeli to czy wymagamy, aby logował się kodem PUK?
Odpowiedź 19:
Zamawiający nie określa wzajemnej współpracy komponentów dostarczonych przez wykonawcę.

Pytanie 20:
Prosimy o wyjaśnienie, w jakie powinny być dopuszczalne długości kodów PIN/PUK oraz z jakich znaków mogą się składać kody PIN/PUK?
Odpowiedź 20:
Zamawiający wymaga, aby długość kodów PIN/PUK była w przedziale 4 do 8 znaków (cyfr i liter), przy czym większa długość jest również dopuszczalna.

Pytanie 21:
Jakie typy sesji powinny być obsługiwane?
Odpowiedź 21:
Powinny być obsługiwane sesje RO i RW.

Pytanie 22:
W jaki sposób mają być obsługiwane sytuacje, w których do komputera podłączone jest wiele czytników PCSC ?
Odpowiedź 22:
Odpowiedzi na pytanie należy szukać w specyfikacji standardu CSP.

Pytanie 23:
Proszę o podanie pełnej specyfikacji aplikacji wykorzystujących funkcje biblioteki CSP i PKCS#11 z uwagi na to, iż ogólnie pojęty standard CSP i PKCS#11nie precyzuje szczegółowo niektórych funkcji kryptograficznych i sposobu implementacji tych funkcji.
Odpowiedź 23:
MS CSP i PKCS#11 są standardami, dlatego też celem pozyskania opisu funkcji należy sięgnąć do opisu standardu.
Mobil e-Gina oraz Centaur komunikują się z kartą z wykorzystaniem wspomnianych bibliotek. Zatem jeśli biblioteki będą przygotowane zgodnie ze standardem wspomniane aplikacje będą współpracowały z kartami.

Pytanie 24:
Czy oprogramowanie i sprzęt, z którym współpracować biblioteki CSP i PKCS będzie modyfikowane (i ile razy) w czasie trwania umowy?
Nowe wersje oprogramowania Mobile e-gina , Centaur PR lub zmiany urządzenia MTN mogą skutkować koniecznością modyfikacji bibliotek CSP.
Odpowiedź 24:
Warunkiem współdziałania z urządzeniami będącymi na wyposażeniu Policji jest dostawa zgodnych ze standardami MS CSP i PKCS#11 bibliotek, które będą współpracowały z kartami.

Jednocześnie na podstawie art. 38 ust. 4 ustawy Pzp Zamawiający informuje o następujących modyfikacjach specyfikacji istotnych warunków zamówienia (SIWZ) przedmiotowego postępowania:

I. W załączniku numer 2 do SIWZ:

1. Modyfikuje się zapisy komparycji projektu umowy ramowej, poprzez skreślenie jej dotychczasowych zapisów i wprowadzenie w to miejsce zapisów o następującej treści:

„U M O W A R A M O W A n r .....
zawarta w Warszawie w dniu .....pomiędzy:

Skarbem Państwa - Komendą Główną Policji z siedzibą w Warszawie przy ul. Puławskiej 148/150, zwaną w treści umowy „Zamawiającym", reprezentowaną przez:

.....

a

firmą ..... z siedzibą w ..... przy ul. ....., wpisaną do ..... pod numerem ....., zwaną dalej „Wykonawcą", reprezentowaną przez:

.....

zwanymi dalej również „Stronami".

2. .§ 5 ust. 7 projektu umowy ramowej otrzymuje następujące brzmienie: „Umowę ramową sporządzono w czterech, jednobrzmiących egzemplarzach, z których trzy egzemplarze otrzymuje Zamawiający, jeden egzemplarz Wykonawca""
3. W §1 projektu umowy ramowej skreśla się ust. 7 i 8.
4. W § 2 projektu umowy ramowej skreśla się ust. 7, 8, 9 i 10 tej umowy.
5. W § 4 projektu umowy ramowej skreśla się ust. 1, 2 oraz 3 i wprowadza się zapis o następującej treści:
„Zamawiający przewiduje naliczanie kar umownych za niewykonanie lub nienależyte wykonanie przedmiotu konkretnej umowy w sprawie zamówienia publicznego w wysokości określonej w tej umowie"

II. W Rozdziale XVI SIWZ „WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY"

Modyfikuje się zapisy rozdziału XVI SIWZ, poprzez skreślenie jego dotychczasowych zapisów i wprowadzenie w to miejsce zapisu o następującej treści

„Zamawiający nie będzie wymagał od Wykonawcy, którego oferta zostanie wybrana wniesienia zabezpieczenia należytego wykonania umowy."

Jednocześnie zgodnie z art. 38 ust. 6 i 7 ustawy Prawo zamówień publicznych Zamawiający przedłuża termin składania ofert i wprowadza następujące zmiany w SIWZ:

IX. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT:

Miejsce i termin składania ofert

1. Ofertę wraz ze wszystkimi wymaganymi oświadczeniami lub dokumentami, należy umieścić w zamkniętej kopercie, zapieczętowanej w sposób gwarantujący zachowanie poufności jej treści oraz zabezpieczający jej nienaruszalność do terminu otwarcia ofert.
2. Koperta powinna być zaadresowana (dokładna nazwa i adres Zamawiającego) oraz opisana według poniższego wzoru:

Biuro Finansów KGP 02-542 Warszawa ul. Domaniewska 36/38 Komenda Główna Policji **Przetarg nr 242/BŁiI/07/BP** Oferta na zawarcie umowy ramowej na okres 4 lat na zakup usług transmisji danych GPRS/EDGE w ramach APN połączonego z siecią Zamawiającego oraz dostawa i aktywacja kart SIM dla terminali mobilnych użytkowanych w Policji. nie otwierać przed godz. 11:00 dnia 12.03.2008 r.

3. Koperta poza oznakowaniem jak wyżej powinna być opatrzona dokładną nazwą i adresem Wykonawcy.
4. Ofertę należy złożyć do dnia 12.03.2008 r. do godz. 10.30 w Biurze Finansów KGP, 02-542 Warszawa, ul. Domaniewska 36/38, pokój 531 A, tel. 0-22/601-32-04, w godz. 8.30 – 15.30 (od poniedziałku do piątku).
5. Wykonawca (na żądanie) otrzyma pisemne potwierdzenie złożenia oferty.
6. Konsekwencje złożenia oferty niezgodnie z ww. opisem (np. potraktowanie oferty jako zwykłej korespondencji i nie dostarczenie jej do miejsca składania ofert w terminie określonym w SIWZ) ponosi Wykonawca.
7. Oferta złożona po terminie zostanie zwrócona Wykonawcy bez otwierania po upływie terminu przewidzianego na wniesienie protestu.

Miejsce i tryb otwarcia ofert

1. Publiczna sesja otwarcia ofert odbędzie się w siedzibie Zamawiającego w Warszawie przy ul. Domaniewskiej 36/38, w dniu 12.03.2008 r. o godz. 11:00.

Pozostałe zapisy SIWZ pozostają bez zmian.

DYREKTOR
BIURA FINANSÓW
KOMENDY GŁÓWNEJ POLICJI
ELŻBIETA WÓJCIK