KOMENDA GŁÓWNA POLICJI
WYDZIAŁ ZAMÓWIEŃ PUBLICZNYCH
BIURO FINANSÓW

02-672 Warszawa | Sekretariat 60-120 44 | fax. 601-18 57
ul. Domaniewska 36/38 | Naczelnik 60-121-02

FZ- 2313 /07 **Warszawa,2007-05- 18**

Wg rozdzielnika

Dot Zakup usługi transmisji danych GPRS/EDGE w ramach APN połączonego z siecią zamawiającego oraz dostawa i aktywacja kart SIM dla terminali mobilnych - sprawa nr 58/BŁiI/07/MK

Na podstawie art.36 ust. 4 i 6 ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych (Dz. U. Nr 164 poz. 1163) Zamawiający dokonuje modyfikacji treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ) L. dz. 1787/07 z dnia 24 kwietnia 2007r. w następującym zakresie:

1. Zmienia się brzmienie rozdziału VII pkt. 1 i pkt 2. SIWZ. Rozdział VII pkt. 1i pkt 2 otrzymuje brzmienie:

„ 1. Termin składania ofert upływa dnia **24 maja 2007 roku o godz 9.30.** Oferty, które wpłyną po tym terminie nie będą rozpatrywane i zostaną zwrócone bez otwierania – bez względu na datę wysłania, po upływie terminu przewidzianego na wniesienie protestu. Ofertę należy złożyć w siedzibie prowadzącego postępowanie, w pok. 531A w dwóch zamkniętych kopertach zapieczętowanych w sposób gwarantujący zachowanie w poufności jej treści oraz zabezpieczającej nienaruszalność do terminu otwarcia ofert.
Kopertę zewnętrzną, nie oznakowaną nazwą wykonawcy należy zaadresować:

BIURO FINANSÓW KGP

02-542 WARSZAWA, ul. Domaniewska 36/38

Oferta do przetargu, nr sprawy 58/BŁiI/07/MK

Nie otwierać przed dn. 24 maja 2007 r. do godz. 10.00
Koperta wewnętrzna , oprócz opisu jw., musi zawierać nazwę firmy, adres,

2. Otwarcie ofert nastąpi **dnia 24 maja 2007 r. godz. 10.00** w pok. 409, w siedzibie prowadzącego postępowanie.”

Jednocześnie na podstawie art. 38 ust. 1 i 2 oraz ust. 4 ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych (Dz. U. Nr 164 poz. 1163) Zamawiający przesyła wyjaśnienia na nadesłane przez uczestników postępowania pytania:

Pytanie nr 29:
W odpowiedzi na pytania zamawiający informuje, iż dysponuje routerami Cisco 3825 z portami fastethernet, czy zamawiający dopuszcza możliwość dostarczenia przez wykonawcę modułów HWIC z innym interfejsem (np. Serial, lub E1), które zainstalowane byłyby w posiadanych przez zamawiającego routerach? Czy w/wy, routery mają jeszcze wolne sloty na zainstalowanie dodatkowych interfejsów?

Odpowiedź na pytanie nr 29:
Zamawiający nie przewiduje instalowania dodatkowych kart w ww. routerach. Każdy z routerów jest wyposażony w 2 porty gigaethernet i 2 porty smart serial. Doprowadzone łącze przez wykonawcę do tych routerów musi być zakończone stykiem fastethernet.

Pytanie nr 30:
W odpowiedzi na pytanie nr 4 zamawiający użył słów ”dysponuje routerami” czy wykonawca może rozumieć, że zamawiający ma co najmniej dwa takie routery w lokalizacji Wiśniowa 58? Czy zamawiający dopuszcza możliwość instalacji dodatkowych interfejsów w obydwu tych routerach?

Odpowiedź na pytanie nr 30:
Zamawiający dysponuje 2 routerami Cisco 3825 i nie przewiduje możliwości instalacji dodatkowych interfejsów w tych urządzeniach.

Pytanie nr 31:
Czy wymienione przez zamawiającego w odpowiedzi na pytanie nr 12 urządzenia MTN i MTP są już wyposażone w aplikacje umożliwiające nawiązywanie połączenia do APNu?

Odpowiedź na pytanie nr 31:
Tak. W terminalach wykorzystywane są standardowe mechanizmy systemu Windows - "Połączenia sieciowe". Ponadto oba typy terminali tj. MTP Sunit d10 oraz MTN Symbol MC70, są wyposażone w modem GSM Siemens MC75

Pytanie nr 32:
Czy Wykonawca ma rozumieć wymóg przedstawienia mapy zasięgu w formie papierowej i cyfrowej jako element dokumentacji powykonawczej?

Odpowiedź na pytanie nr 32:
Mapa w formie cyfrowej i papierowej musi być dołączona jako element dokumentacji powykonawczej

Pytanie nr 33:
W punkcie IV szczegółowego opisu przedmiotu zamówienia w podpunkcie 9 zamawiający oczekuje od wykonawcy przedstawienia roamingu transmisji GPRS poza własną sieć w przypadku braku zasięgu GPRS dostawcy. W chwili obecnej powyższy wymóg nie jest możliwy do spełnienia przez żadnego z operatorów funkcjonujących na terenie Polski w zakresie gwarantującym skorzystanie z sieci innego operatora w przypadku braku zasięgu własnej sieci. Zawarte obecnie pomiędzy operatorami umowy dostępowe do sieci nie gwarantują poszerzenia skutecznego zasięgu GPRS/EDGE na terenie kraju z wykorzystaniem sieci innego operatora. W związku z tym sugerujemy usunięcie powyższego punktu z SIWZ.

Odpowiedź na pytanie nr 33:
Zamawiający nie wymaga obligatoryjnie roamingu transmisji GPRS poza własną sieć operatora, jeśli taka możliwość nie istnieje. Wymóg ten nie jest także w żaden sposób dodatkowo punktowany.

Pytanie nr 34:
Prosimy o ponowne rozważenie pytania nr 16 o rozszerzenie i doprecyzowanie odpowiedzi na to pytanie. Odpowiedź: „ Zamawiający wyjaśnia, że w przypadku tych kart nie są wymagane żadne kody PIN. Karta po włożeniu do modemu musi pracować bez podawania jakichkolwiek kodów PIN” – nie usuwa

wątpliwości zwłaszcza w takim zakresie jak: Czy wyłączenie blokady kodem PIN ma być wyłączeniem bezterminowym czy też sposób konfiguracyjny blokada ta może być przywracana.

Odpowiedź na pytanie nr 34:

Wyłączenie blokady PIN w stosunku do 2200 szt. kart zgodnie ze specyfikacją ma być wyłączeniem bezterminowym.

Pytanie nr 35:

Prosimy o doprecyzowanie odpowiedzi na pytanie 17. W szczególności prosimy o doprecyzowanie odpowiedzi na drugą część pytania nr 17 a mianowicie: „Prosimy o doprecyzowanie polityki bezpieczeństwa odnośnie generowania par kluczy RSA i operacji na tych kluczach". Prosimy także o doprecyzowanie polityki bezpieczeństwa związanej z wymianą kluczy i certyfikatów.

Odpowiedź na pytanie nr 35:

Zamawiający wyjaśnia, że operacje takie jak: wygenerowanie pary kluczy RSA, zapis klucza prywatnego, realizację podpisu RSA oraz zapis certyfikatu realizowane są przez kartę SIM, a dokładnie przez kryptoprocesor RSA umożliwiający wykonanie operacji RSA dla kluczy znajdujących się na karcie. Dla nowych kart SIM Zamawiający przewiduje wykonanie tych operacji centralnie w siedzibie Zamawiającego. Natomiast proces zdalnej wymiany certyfikatów Zamawiający wyjaśnił w odpowiedzi nr 26 (pismo FZ-2154/07 z 11.05.2007 r.)

Pytanie nr 36:

Prosimy o ponowne rozpatrzenie pytania nr 18 (doprecyzowanie parametrów kooprocesora kryptograficznego) – (odpowiedź na pytanie 18 odnosi się do klucza i algorytmu kryptograficznego pomijając „parametry pracy" samego kooprocesora (np: czy zamawiający stawia przed tym koprocesorem określone wymagania wydajnościowe?)

Odpowiedź na pytanie nr 36:

Zamawiający nie stawia wymagań wydajnościowych w stosunku do koprocesora w karcie SIM.

Pytanie nr 37:

Odpowiedź na pytanie 19 doprecyzowuje warunki pracy prosimy jednakże o doprecyzowanie czy taki tryb pracy i składowania przekłada się na określone „warunki brzegowe" takie jak przedstawiono w punkcie 10 rozdział V.

Odpowiedź na pytanie nr 37:

Zamawiający wymaga aby karta SIM pracowała obligatoryjnie w zakresie temperatur -25^{o} st. C ÷ + 55^{o} C, natomiast warunki brzegowe składowania karty powinny obejmować wskazany w specyfikacji zakres.

Pytanie nr 38:

Do odpowiedzi na pytanie nr 21: Jeśli zamawiający zmodyfikował SIWZ skreślający punkt 16 rozdział V – prosimy o doprecyzowanie w jaki sposób powinno następować uwierzytelnienie użytkowników urządzeń mobilnych w systemie KSIP.

Odpowiedź na pytanie nr 38:

Uwierzytelnienie użytkowników urządzeń mobilnych opiera się oparciu o podpis cyfrowy z wykorzystaniem kluczy kryptograficznych i certyfikatów przechowywanych na karcie SIM. Dostęp użytkowników takich urządzeń do określonych zasobów systemu KSIP zakłada wykorzystywanie mechanizmów infrastruktury PKI.

Pytanie nr 39:

Do odpowiedzi na pytanie nr 22: W punkcie 17 rozdział V zamawiający stwierdza, iż dostarczane karty powinny być zgodne z Java 2.1.1. – czy zgodność tę należy rozumieć tak, iż karty powinny być zgodne

Java w wersji co najmniej 2.1.1 (i karty zgodne np. z Java 2.2 kompatybilne wstecz do Javy 2.1.1 zaspokajają oczekiwania zamawiającego?)

Odpowiedź na pytanie nr 39:

Karty zgodne z Java w wersji 2.1.1 spełniają oczekiwania Zamawiającego. Po stronie wykonawcy leży obowiązek zachowania zgodności ze standardem z Java w wersji 2.1.1.

Pytanie nr 40:

Do odpowiedzi na pytanie 24 – prosimy o dospecyfikowanie oprogramowania Centaur – przynajmniej w takim zakresie aby możliwe było zaprojektowanie i przygotowanie współpracy czytnika PC/SC z tymże oprogramowaniem (udostępniane API, implementowane protokoły etc.)

Odpowiedź na pytanie nr 40:

Zamawiajmy wyjaśnia, iż posiadane oprogramowanie Centaur współpracuje ze standardowymi czytnikami PC/SC. Ten wymóg dotyczy również dostarczanych kart SIM. Nie jest wymagane zaprojektowanie czytnika do współpracy z oprogramowaniem Centaur.

Pytanie nr 41:

Do odpowiedzi na pytanie 25: zaprojektowanie aplikacji wymaga znajomości sposobu komunikacji z aplikacją Mobil-eGina – prosimy zatem o specyfikację tej aplikacji zawierającą: udostępniane API, implementowane protokoły, realizowana funkcjonalność.

Odpowiedź na pytanie nr 41:

Komunikacja aplikacji Mobil-eGina z kartą SIM odbywa się z wykorzystaniem biblioteki CSP (Crypto Service Provider) dla systemu Windows Mobile 5.0

Pytanie nr 42:

Do odpowiedzi na pytanie 27. Prosimy o doprecyzowanie i rozszerzenie tej odpowiedzi – udzielona odpowiedź nie wyjaśnia w sposób pozwalający na rzetelne przygotowanie oferty sposobu w jaki karta SIM powinna sprawdzać ważność certyfikatu.

Odpowiedź na pytanie nr 42:

Zamawiający informuje, że ważność certyfikatu zapisanego na karcie SIM będzie sprawdzana przez serwer uwierzytelnienia w trakcie dostępu użytkownika poprzez przeglądarkę MTN do danego systemu teleinformatycznego Policji. Karta SIM jako taka nie sprawdza we własnym zakresie ważności certyfikatu podczas logowania, natomiast dokonuje tego Mobil-e GINA, zainstalowana w MTN. Weryfikacja ważności certyfikatu polega na sprawdzeniu, czy jest on podpisany przez zaufane Centrum Certyfikacji w ramach PKI Policji.

Pytanie nr 43:

Prosimy o doprecyzowanie kluczowych funkcjonalności jakie posiada aplikacja MobGina tak, aby możliwe było zrozumienie jej zastosowania we wnioskowanym systemie a w szczególności:

a) czy aplikacja ta składa się z modułu aplikacji serwerowej i aplikacji klienckiej
b) jeśli zaistniał przypadek a) to czy oba moduły zapewniają komunikacje z użyciem TLS
c) jakich funkcjonalności dostarcza MobGina zainstalowana w urządzeniu mobilnym wspiera w kontekście komunikacji z karta SIM poprzez bibliotekę MS CSP
d) w jaki sposób (o ile w ogóle) MobGina wspiera wykonywanie połączenia urządzenia mobilnego z serwerem?

Odpowiedź na pytanie nr 43:

Aplikacja Mobil-eGina nie posiada modułu aplikacji serwerowej, jest aplikacją instalowaną tylko na urządzeniu mobilnym Symbol MC70. Aplikacja ta odpowiada za uwierzytelnienie użytkownika urządzenia mobilnego z wykorzystaniem podpisu cyfrowego, również w procesie logowania do systemu operacyjnego. Wykorzystuje MS CSP do wszystkich operacji związanych z kluczami i certyfikatami.

Ponadto komunikuje się wyłącznie z modułem personalizacji w celu realizacji procesu zdalnej wymiany certyfikatów z wykorzystaniem protokołu TLS.

Pytanie nr 44:
Prosimy o doprecyzowanie znaczenia wyrażenia „posługującej się protokołem WebServices we współpracy z przeglądarką Internet Explorer" w punkcie V.29 na stronie 11 a w szczególności o jakiej współpracy z przeglądarką IE informuje zleceniodawca.

Odpowiedź na pytanie nr 44:
Proces automatycznej wymiany certyfikatów realizowany jest przez Mobil-eGina za pośrednictwem SOAP RPC, który dodatkowo może być wspomagany przez przeglądarkę WWW np. poprzez manualne zainicjowanie procesu wymiany certyfikatu.

Pytanie nr 45:
W jaki sposób aplikacja MobGina instalowana w urządzeniu mobilnym ma uczestniczyć w procesie uwierzytelniania z wykorzystaniem serwera Proxy Radius po stronie serwera.

Odpowiedź na pytanie nr 45:
Aplikacja Mobil-eGina może pełnić funkcje CSP biorąc udział w procesie uwierzytelnienia pomiędzy urządzeniem mobilnym a serwerem Proxy Radius. Zamawiający niezależnie od realizowanej obecnie funkcjonalności przez aplikację oczekuje dostawy karty SIM z odpowiednią biblioteką CSP realizującą operacje kryptograficzne na karcie zgodnie ze standardem CSP.

Pytanie nr 46:
Czy moduł personalizacji ma zarządzać poza kwestiami ważności certyfikatu na kartach SIM , także blokowaniem i odblokowywaniem całych kart SIM (w przypadku np. kradzieży terminala)? Czy może funkcjonalność ta ma być realizowana na blokadzie certyfikatu karty SIM.

Odpowiedź na pytanie nr 46:
Moduł personalizacji odpowiada za automatyczną usługę zdalnej wymiany certyfikatów dla użytkowników urządzeń mobilnych posiadających certyfikaty wystawione w policyjnym systemie Centrum Certyfikacji. Zamawiający nie wymaga dodatkowych funkcjonalności realizowanych przez moduł personalizacji polegającej m.in. na blokowaniu i odblokowywaniu kart SIM.

Pytanie nr 47:
Prosimy doprecyzować w punkcie 16 rozdziału V siwz „karta SIM musi umożliwiać uwierzytelnianie użytkowników urządzeń mobilnych w systemie KSIP" a w szczególności jakie metody uwierzytelniania wymaga system KSIP oraz jaki interfejs system KSIP wystawia w tym celu dla aplikacji wspomagającej proces uwierzytelniania.

Odpowiedź na pytanie nr 47:
Metoda uwierzytelnienia i interfejs zostały opisane w odpowiedzi na pytanie nr 38, 42, 44.

Pytanie nr 48:
Czy proces generowania nowego certyfikatu dla urządzenia mobilnego (karty SIM) ma być wykonywany po stronie karty SIM która ma za zadanie wygenerować nowy certyfikat i zsynchronizować go z serwerem, czy tez w odwrotny sposób – certyfikat jest generowany po stronie serwera i jest zapisywany zdalnie na kartę SIM?.

Odpowiedź na pytanie nr 48:
Certyfikaty są generowane w Centrum Certyfikacji.

Pytanie nr 49:
Prosimy o doprecyzowanie sformułowania w punkcie 33 rozdział V siwz a mianowicie „karta udostępniana przez oba interfejsy (PKCS#11 i MS CSP) musi umożliwiać pracę wielo aplikacyjną (jednoczesne używanie karty przez wiele aplikacji)".

Odpowiedź na pytanie nr 49:

Biblioteki PKCS#11 i MS CSP muszą być zgodne ze standardami co zapewnia możliwość pracy karty z wieloma aplikacjami.

Jednocześnie Zamawiający na podstawie art. 38 ust. 4 u Pzp, modyfikuje treść Specyfikacji Istotnych Warunków Zamówienia (SIWZ) L. dz. 1787/07 z dnia 24 kwietnia 2007r. poprzez zmianę brzmienia następujących punktów rozdziału V załącznika nr 1 do siwz:

1. **Skreśla się brzmienie punktu 10 rozdziału V załącznika nr 1 do siwz. Punkt 10 rozdziału V otrzymuje brzmienie: ”**Karta SIM musi umożliwiać pracę w zakresie temperatur od -25˚C do 55˚C i mieć możliwość składowania w zakresie temperatur od -40˚C do 80˚C przy kondensacji pary wodnej 5-90% (wilgotność względna).”
2. **Skreśla się brzmienie punktu 12 rozdziału V załącznika nr 1 do siwz. Punkt 12 rozdziału V otrzymuje brzmienie: ”**Karta SIM musi umożliwiać pracę w zakresie temperatur od -15˚C do 50˚C przy kondensacji pary wodnej 5-90% (wilgotność względna).”
3. **Skreśla się brzmienie punktu 23 rozdziału V załącznika nr 1 do siwz. Punkt 23 rozdziału V otrzymuje brzmienie: ”**Dla dostarczonych kart Wykonawca musi dołączyć bibliotekę CSP *(Cryptographics Service Provider)* dla systemu *Windows Mobile* i urządzenia przenośnego *Symbol MC 70*.”
4. **Skreśla się brzmienie punktu 24 rozdziału V załącznika nr 1 do siwz. Punkt 24 rozdziału V otrzymuje brzmienie: ”**Dla dostarczonych kart Wykonawca musi dostarczyć bibliotekę PKCS#11 w. 2.01 lub nowszą, dla systemu *Windows Mobile* i urządzenia przenośnego *Symbol MC 70*.”
5. **Skreśla się brzmienie punktu 25 rozdziału V załącznika nr 1 do siwz. Punkt 25 rozdziału V otrzymuje brzmienie: „**Wykonawca musi dostarczyć moduł personalizacji kart SIM”.

Zastępca Naczelnika
Wydziału Zamówień Publicznych
Biura Finansów KGP

mł. insp. Adam Królikowski