KOMENDA GŁÓWNA POLICJI
BIURO FINANSÓW
WYDZIAŁ ZAMÓWIEŃ PUBLICZNYCH

ul. Domaniewska 36/38; 02-672 Warszawa; tel. 22 60 120 44; fax 22 60 118 57
zamowieniakgp@policja.gov.pl

F2-7457/13

Warszawa, 15.11. 2013 r.

L.dz. ...../13

dot. postępowania prowadzonego w trybie przetargu nieograniczonego na realizację zamówienia pn.: Zakup oprogramowania umożliwiającego zarządzanie certyfikatami w Mobilnych Terminalach Noszonych**, sprawa nr 230/BŁiI/13/MSz.**

Działając na podstawie art. 38 ust. 2 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2013 r., poz. 907 – ustawa Pzp) przekazuję wyjaśnienia treści SIWZ.

Pytanie nr 1

Dotyczy: Załącznik nr 1 do SIWZ, sekcja „Przedmiot zamówienia/umowy obejmuje", pkt. 1, str. 12. Prosimy o zdefiniowanie zakresu w jakim zamawiane oprogramowanie ma współpracować z wykorzystywanym w Policji oprogramowaniem na urządzeniach.

Odpowiedź

Dostarczone oprogramowanie musi współpracować z wykorzystywanym w Policji oprogramowaniem na urządzeniach oraz być kompatybilne zarówno ze sprzętem jak i zainstalowanym oprogramowaniem, przy wykorzystaniu posiadanej przez Zamawiającego biblioteki do obsługi kart kryptograficznych oraz przy spełnieniu wymagań w zakresie oprogramowania wskazanych w SIWZ.

Pytanie nr 2

Dotyczy: Załącznik nr 1 do SIWZ, rozdział I „Wymagania w zakresie oprogramowania", str. 12.

a) Czy zamawiane oprogramowanie ma uczestniczyć w procesie logowania do urządzenia? Jeśli tak, to w jakim zakresie?

Odpowiedź: Zamawiane oprogramowanie nie ma uczestniczyć w procesie logowania do urządzenia.

b) Które oprogramowanie spośród oprogramowania wykorzystywanego w Policji na urządzeniach może podejmować próby nawiązania sesji SSL za pomocą certyfikatu użytkownika?

Odpowiedź: Mobilny Klient SWD oraz wbudowana przeglądarka internetowa.

c) Czy Zamawiający wymaga, aby zamawiana aplikacja przechwytywała każdą próbę nawiązania sesji SSL (także dla ewentualnych aplikacji zainstalowanych w przyszłości) za pomocą certyfikatu użytkownika i prezentowała listę zarejestrowanych certyfikatów do wyboru?

Odpowiedź: Zamawiający wymaga, aby zamawiana aplikacja przechwytywała każdą próbę nawiązania

sesji SSL (także dla ewentualnych aplikacji zainstalowanych w przyszłości) za pomocą certyfikatu użytkownika Listę certyfikatów z magazynu Windows podczas uwierzytelniania prezentuje przeglądarka/mobilny klient SWD.

d) Czy Zamawiający wymaga, aby zamawiana aplikacja modyfikowała usługi systemu operacyjnego urządzenia tak, aby próby nawiązania sesji SSL za pomocą certyfikatu użytkownika na poziomie były przekierowywane do zamawianego oprogramowania?

Odpowiedź: Zamawiający wyjaśnia, że system operacyjny pośredniczy w komunikacji pomiędzy aplikacją a CSP (podczas ładowania CSP weryfikowany jest cyfrowy podpis, uzyskany wcześniej podczas certyfikacji).

e) Czy uwierzytelnianie przy dostępie do policyjnych systemów informatycznych realizowanym za pomocą wbudowanej przeglądarki realizowane jest za pomocą certyfikatów użytkownika?

Odpowiedź: Tak, uwierzytelnianie przy dostępie do policyjnych systemów informatycznych realizowanym za pomocą wbudowanej przeglądarki realizowane jest za pomocą certyfikatów użytkownika.

f) Czy prezentowanie listy zarejestrowanych certyfikatów z dostępnych tokenów podczas uwierzytelniania jest funkcją, która ma być realizowana przez zamawiane oprogramowanie, czy też będzie realizowana przez jakiś inny komponent? Jaki?

Odpowiedź: Nie, prezentowanie listy zarejestrowanych certyfikatów z dostępnych tokenów podczas uwierzytelniania jest funkcją realizowaną przez przeglądarkę/mobilnego klienta SWD.

Pytanie nr 3

Dotyczy: Załącznik nr 1 do SIWZ, sekcja „Wymagania funkcjonalne", str. 12.

a) Czy zamawiana aplikacja ma startować jeszcze przed zalogowaniem do urządzenia?

Odpowiedź: Nie, zamawiana aplikacja nie ma startować jeszcze przed zalogowaniem do urządzenia.

b) Na jakim etapie pracy z urządzeniem (podczas jakich czynności/procesów) aplikacja ma proponować użytkownikowi odblokowanie tokena w przypadku wykrycia blokady?

Odpowiedź: Podczas próby dostępu do policyjnych systemów informatycznych, w momencie wykrycia zablokowania tokenu.

c) Czy Zamawiający dopuszcza, aby konfiguracja czasu, o którym mowa w pkt. 8 był zrealizowana za pomocą pliku tekstowego? Jeśli nie, to jakie są w tym zakresie wymagania?

Odpowiedź: Zamawiający miał na myśli konfigurację pozostałego czasu do upłynięcia terminu ważności certyfikatu. Wartość może być konfigurowana za pomocą pliku tekstowego.

Pytanie nr 4

Dotyczy: Załącznik nr 1 do SIWZ, sekcja „Wymagania funkcjonalne", str. 12.

a) Jak należy rozumieć wymaganie pełnej kompatybilności w działaniu dostarczonego Przedmiotu umowy z zainstalowanym oprogramowaniem na urządzeniach Zamawiającego?

Odpowiedź: Zamawiający oczekuje pełnej kompatybilności w działaniu dostarczonego oprogramowania z zainstalowanym oprogramowaniem na urządzeniach Zamawiającego oraz kompatybilności z posiadanymi urządzeniami i kartami kryptograficznymi.

b) Czy wspomnianą kompatybilność należy rozumieć jako niezakłócanie poprawnego działania oprogramowaniem zainstalowanego na urządzeniach Zamawiającego?

Odpowiedź: Tak, wspomnianą kompatybilność należy rozumieć jako niezakłócanie poprawnego działania oprogramowaniem zainstalowanego na urządzeniach Zamawiającego.

c) Czy wspomnianą kompatybilność należy rozumieć jako umożliwienie wyboru certyfikatu z listy tym aplikacjom spośród aplikacji zainstalowanych na urządzeniach Zamawiającego, które wymagają uwierzytelniania za pomocą certyfikatów użytkownika?

Odpowiedź: Wspomnianą kompatybilność należy rozumieć również jako umożliwienie skorzystania z certyfikatu tym aplikacjom spośród aplikacji zainstalowanych na urządzeniach zamawiającego, które wymagają uwierzytelniania za pomocą certyfikatów użytkownika

Pytanie nr 5

Dotyczy: Załącznik nr 1 do SIWZ, rozdział IV „Urządzenia Zamawiającego", str. 14

a) Czy zamawiane oprogramowanie ma zabezpieczać dostęp do urządzenia czy też zabezpieczanie dostępu do urządzenia będzie realizowane przez inny komponent nieobjęty niniejszym Zamówieniem?

Odpowiedź: Dostęp do urządzenia będzie realizowany przez inny komponent nieobjęty niniejszym Zamówieniem.

b) Które spośród aplikacji zainstalowanych na urządzeniach Zamawiającego wykorzystują „apletu uwierzytelniającego Comarch microSD crypto"?

Odpowiedź: Zamawiane oprogramowanie umożliwiające zarządzanie certyfikatami w Mobilnych Terminalach Noszonych ma wykorzystywać aplet uwierzytelniający Comarch microSD crypto.

c) Czy „aplet uwierzytelniający Comarch microSD crypto" potrafi zaprezentować listę zarejestrowanych w systemie certyfikatów?

Odpowiedź: Zamawiane oprogramowanie ma zaprezentować użytkownikowi listę wirtualnych tokenów.

Na podstawie art. 27 ust. 2 ustawy Prawo zamówień publicznych (Dz. U. z 2013 r. poz. 907– ustawa Pzp) oraz zapisów Rozdziału VIII, pkt. 3 SIWZ proszę o potwierdzenie otrzymania wiadomości.

NACZELNIK
WYDZIAŁU ZAMÓWIEŃ PUBLI
BIURA FINANSÓW
KOMENDY GŁÓWNEJ PO
Tomasz PIOTRKOWIC