MOPS-DO/271/2/27/08

Ogłoszenie o zamówieniu publicznym

Miejski Ośrodek Pomocy Społecznej w Krakowie, ul. Józefińska 14, 30-529 Kraków, tel. (012) 616-54-27, fax (012) 616-54-28, e-mail: do@mops.krakow.pl

informuje o wszczęciu postępowania o udzielenie zamówienia publicznego na **dostawę oprogramowania komputerowego oraz oprogramowania do zarządzania siecią MOPS w Krakowie.**

I. Tryb zamówienia: przetarg nieograniczony
II. Rodzaj zamówienia: dostawy
III. Adres strony internetowej, na której jest zamieszczona specyfikacja istotnych warunków zamówienia: www.mops.krakow.pl, zakładka „Zamówienia publiczne"
IV. Określenie przedmiotu zamówienia:

CPV: 30241000-0

1. Przedmiotem zamówienia jest dostawa oprogramowania komputerowego, systemu do zarządzania siecią MOPS oraz serwis i aktualizacja w/w oprogramowania, zgodnie z opisem Zamawiającego podanym w załączniku nr 1 do specyfikacji.
2. Wytyczne dla II części zamówienia:
   1) Wykonawca dostarczy na zakupione oprogramowanie licencje bezterminową.
   2) Koszt całościowy za licencję oraz serwis, suport i aktualizację podzielony będzie na dwie równe raty. Pierwsza rata płatna w roku 2008 w terminie 14 dni od daty przyjęcia faktury przez Zamawiającego, wraz z protokołem przekazania. Druga rata płatna do końca 31 stycznia 2009. Zamawiający wymaga, aby Wykonawca dostarczył fakturę w terminie nie później, niż 16 stycznia 2009 r.
   3) Wykonawca zapewni bezpłatny serwis telefoniczny oraz za pomocą poczty internetowej.
   4) Dostarczone oprogramowanie zapewni obsługę minimum 400 komputerów w MOPS Kraków w 11 lokalizacjach:
      a) 1 lokalizacja z obsługą do 250 adresów IP
      b) 1 lokalizacja z obsługą do 100 adresów IP
      c) 4 lokalizacje z obsługą do 50 adresów IP
      d) 5 lokalizacji z obsługą do 25 adresów IP
   5) Czas na reakcję serwisu wynosi 24h.
   6) Godziny pracy serwisu muszą obejmować godziny pracy MOPS Kraków, tj. w poniedziałek w godzinach od 9:00 do 17:00 oraz od wtorku do piątku w godzinach od 7:30 do 15:30.
   7) Dostarczone oprogramowanie musi posiadać:
      a) Rozwiązanie typu "software appliance", tzn. system firewallowy zintegrowany z systemem operacyjnym.
      b) Przepustowość firewalla min 4 Gbps.
      c) Obsługę min. 700 000 sesji równoległych.
      d) zaporę sieciową z inspekcją stanu pakietów (stateful inspection firewall), serwer VPN, system zapobiegania włamaniom (Intrusion Prevention System), serwer

HTTP Proxy, serwer DNS, serwer DHCP, Mail Gateway, FTP Gateway, SSH Proxy, serwer polityk bezpieczeństwa.

e) Ochronę przed atakami typu Dos/Dos: IP spoofing, SYN flooding, flood ping i innymi, oraz przed skanowaniem portów i adresów.
f) Możliwość pracy w trybie bridging (transparentnym).
g) Obsługę NAT, PAT, proxy arp i sieci wirtualnych (VLAN).
h) Obsługę protokołów VoIP – H.323, SIP, SCCP.
i) Obsługę protokołów OSPF, RIP.
j) Możliwość pełnego zdalnego zarządzania firewallem, serwerem VPN oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej pod systemem
MS Windows.
k) Możliwość podzielenia reguł firewalla na logiczne grupy, pomiędzy którymi występują kaskadowe połączenia.
l) Możliwość definiowania tzw. reguł dynamicznych na firewallu, automatycznie wyłączających się po ustalonym czasie.
m) Wbudowany analizator pakietów (sniffer).
n) Wbudowany tester reguł pozwalający na sprawdzenie poprawności i wyników działania tworzonych reguł przed ich aktywacją na firewallu.
o) Automatyczne przywracanie ostatniej działającej konfiguracji sieci po 90 sekundach od momentu utracenia połączenia administracyjnego.
p) Dostępną funkcjonalność IPS.
q) Wbudowany filtr antyspamowy (SMTP/POP3).
r) Możliwość integracji ze skanerem antywirusowym pozwalającym na skanowanie ruchu przechodzącego przez bramkę po protokołach SMTP, POP3, HTTP i FTP.
s) Możliwość integracji z klasyfikatorem stron WWW.
t) Możliwość integracji z filtrem aplikacji P2P, Skype i komunikatorów internetowych, w tym Gadu-Gadu.
u) Możliwość integracji z modułem, który pozwala na kontrolę ruchu szyfrowanego HTTPS oraz danych przesyłanych w strumieniu XML. Moduł ma dostarczać również wizualizację połączeń HTTP/HTTPS.
v) Możliwość generowania statystyk w czasie rzeczywistym - opóźnienie nie większe niż 10 sekund.
w) Możliwość zarządzania systemem przez większa liczbę administratorów o określonych uprawnieniach.
x) Możliwość ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym).
y) Funkcję aktywnego powiadomienia o zdarzeniach (przez SMTP i SNMP).
z) Możliwość budowy kanałów VPN w strukturze gwiaździstej z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami – minimalna liczba kanałów VPN zapewniających pełną komunikację pomiędzy wszystkimi lokalizacjami nie powinna być większa niż liczba lokalizacji.
aa) Obsługę multitransport VPN – tworzenie do 24 kanałów VPN pomiędzy tymi samymi lokalizacjami korzystających z różnych łączy, z opcją Master-Slave.
bb) Możliwość nawiązywania połączeń VPN przechodzących przez serwer proxy HTTPS.
cc) Dostępne centrum autoryzacji na lokalnym serwerze VPN.
dd) Możliwość uwierzytelniania użytkowników za pomocą certyfikatów cyfrowych i/lub logowania.

ee) Możliwość podłączenia zdalnych klientów poprzez kanały VPN client-server za pośrednictwem klienta VPN wyposażonego w personal firewall, którego ustawienia są kontrolowane przez administratora firewalla korporacyjnego.

ff) Możliwość kontroli dostępu do sieci firmowej końcówek klienckich (NAC) zarówno
w granicach sieci firmowej, jak i poza nią.

gg) Możliwość scentralizowanego zarządzania politykami bezpieczeństwa i ich dystrybucją do końcówek klienckich.

hh) Możliwość integracji z usługami katalogowymi Active Directory, LDAP, obsługiwana przez usługi firewall, serwer VPN, proxy HTTP, proxy FTP, proxy SSH oraz uwierzytelnianie administratorów.

ii) Możliwość przydzielania ustawień tunelu VPN client-to-site na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP.

jj) Aplikację – klienta VPN dla platform Windows, Linux.

kk) Możliwość zdefiniowania na platformach Windows skrótu do połączenia VPN z ukrytymi wszystkimi opcjami konfiguracyjnymi.

ll) Obsługę uwierzytelniania administratorów przy pomocy hasła (lokalnego lub synchronizowanego z usługą katalogową), klucza zapisanego na tokenie lub karcie kryptograficznej albo równocześnie przy pomocy i hasła, i klucza.

mm) Obsługę uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI oraz obsługa list CRL udostępnionych na serwerze LDAP.

nn) Integrację z modułem systemu centralnego zarządzania pozwalająca na:
- zarządzanie wieloma firewallami (serwerami usług) z jednej konsoli administracyjnej (konfigurowanie i monitorowanie parametrów systemu, firewalla, serwera VPN),
- możliwość definiowania dowolnej liczby administratorów o różnych uprawnieniach funkcjonalnych i dostępie do różnych grup serwerów,
- możliwość tworzenia szablonów ustawień i równoczesnej zmiany tych samych ustawień na dowolnej liczbie zarządzanych serwerów,
- zarządzanie zdalnymi lokalizacjami przez dodatkowy niezależny tunel VPN,
- centralny dziennik zdarzeń,
- graficzny edytor kanałów VPN - możliwość zestawiania kanałów VPN pomiędzy serwerami na zasadzie „przeciągnij i upuść",
- budowę hierarchicznej struktury zarządzania bezpieczeństwem,
- budowę Cluster Firewall – możliwość zarządzania zestawem reguł na firewallu (przypisywanie i blokowanie dostępu do wybranych zestawów reguł),
- generowanie statystyk centralnych,
- tworzenie obiektów globalnych,
- obsługę infrastruktury klucza publicznego (PKI),
- zastosowanie opcjonalnego systemu przeprowadzania audytu dokonanych zmian w konfiguracji serwerów z możliwością zapisywania (backupu) i przywracania ustawień historycznych (tzw. revision control system),
- zastosowanie opcjonalnego modułu tworzenia graficznych raportów historycznych, okresowych i na żądanie.

oo) Możliwość obsługi klastra High Availability z możliwością pracy w trybach Active-Passive i Active-Active.

pp) Możliwość obsługi min. 10 interfejsów fizycznych.
qq) Obsługę łączy gigabitowych oraz możliwość łączenia dwóch kart sieciowych w jedną logiczną kartę sieciową w celu zwiększenia przepustowości.
rr) Obsługę kilku łączy internetowych równocześnie, w tym multipath routing.
ss) Automatyczne przekierowanie ruchu na łącze zapasowe w przypadku awarii łącza głównego.
tt) Możliwość podziału łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników z osobna lub dla grup użytkowników oraz możliwość ustawiania priorytetów (traffic shaping).
uu) Możliwość zarządzania pasmem w ramach tunelu VPN i na każdym tunelu VPN z osobna.
vv) Możliwość kompresji danych przesyłanych w tunelach VPN site-2-site między firewallami i w tunelach VPN client-2-site.
ww) Funkcję automatycznej zmiany trasowania ruchu VPN w przypadku awarii tunelu VPN.

8) Czas pełnej instalacji lub odtworzenia systemu zapory sieciowej po awarii sprzętu musi wynosi do 10 minut.
9) Rozwiązanie musi posiadać możliwość obsługi platform sprzętowych opartych o architekturę Intel x86.
10) Wykonawca powinien zapewnić Zamawiającemu jedno bezpłatne szkolenie (co najmniej 3-dniowe) prowadzone w języku polskim przez certyfikowanego przez producenta szkoleniowca.
11) Wykonawca powinien zapewnić możliwość szkoleń dodatkowych, zlecanych na podstawie odrębnie prowadzonego postępowania o udzielenie zamówienia publicznego.
12) Wykonawca dostarczy wraz z oprogramowaniem certyfikat zgodności oprogramowania ze standardem IPSec (VPNC Basic & AES Interop Certified) oraz ze standardem certyfikat ISO 15408/Common Criteria na poziomie EAL 4+.

3. Warunki dodatkowe:
1) Wykonawca dostarczy przedmiot zamówienia własnym transportem, na własny koszt, w sposób zapewniający jego całość i nienaruszalność, w terminie ustalonym umową. Miejsce dostawy: magazyn centralny MOPS w Krakowie przy ul. Józefińskiej 14, w godzinach pracy Zamawiającego, tj.: w poniedziałki 9.00-17.00 oraz od wtorku do piątku 7.30-15.30.
2) Faktura oraz protokół przekazania mają zawierać szczegółowe zestawienie oprogramowania
3) Zamawiający nie odbierze towaru w przypadku gdy Wykonawca przy dostawie nie dostarczy poprawnie wystawionych: faktury oraz protokołu przekazania.
4) W przypadku stwierdzenia przez Zamawiającego w ciągu 7 dni od dostawy wad w dostarczonym towarze Wykonawca ma obowiązek wymienić wadliwy towar do 7 dni od daty otrzymania zgłoszenia.
5) Wszelkie kary umowne mogą być potrącane z wynagrodzenia należnego Wykonawcy.
6) Wykonawca jest związany ofertą przez 30 dni licząc od upływu terminu składania ofert.
7) Cena oferty określona stosownie do wymagań specyfikacji zawiera wszystkie koszty realizacji zamówienia.
8) Zamawiający wymaga, aby Wykonawca zawarł umowę na warunkach określonych we wzorach umów stanowiących załączniki nr 2 i 3 do specyfikacji, w terminie określonym przez Zamawiającego w wezwaniu do jej podpisania.

V. Czy Zamawiający dopuszcza złożenie oferty częściowej: tak (3 części zamówienia)

VI. Czy Zamawiający dopuszcza złożenie oferty wariantowej: nie

VII. Termin wykonania zamówienia:

1. I część zamówienia - do 21 dni kalendarzowych od daty podpisania umowy,
2. II część zamówienia – serwis: 2 lata od dnia podpisania umowy, dostawa oprogramowania: 14 dni kalendarzowych od dnia podpisania umowy.
3. III część zamówienia – do 2 dni kalendarzowych od dnia podpisania umowy

VIII. Warunki udziału w postępowaniu i sposób dokonywania oceny spełniania tych warunków:

Warunki, które muszą spełniać wykonawcy biorący udział w postępowaniu określone są w art. 22 ust 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2007 r. nr 223, poz. 1655).

Zamawiający żąda przedstawienia następujących dokumentów:

1. Aktualny odpis z właściwego rejestru albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej, określające pełna nazwę, status prawny i dokładny adres firmy, potwierdzające, że Wykonawca jest uprawniony do występowania w obrocie prawnym.

   Zaświadczenie winno jednoznacznie wskazywać osobę/y upoważnioną/e do dokonywania czynności prawnych w imieniu Wykonawcy (należyta reprezentacja). Wykonawca posiadający siedzibę poza granicami Rzeczypospolitej Polskiej zamiast w/w dokumentu winien złożyć dokument wystawiony w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzający, że nie otwarto jego likwidacji ani nie ogłoszono upadłości. Jeżeli w kraju pochodzenia osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się w/w dokumentu, zastępuje się go dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio kraju pochodzenia osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania.

   Zaświadczenie winno jednoznacznie wskazywać osobę/y upoważnioną/e do dokonywania czynności prawnych w imieniu Wykonawcy (należyta reprezentacja).

   W przypadku:

   1) podmiotów posiadających osobowość prawną jak i spółek prawa handlowego nie posiadających osobowości prawnej – wyciąg z rejestru sądowego,
   2) osób fizycznych wykonujących działalność gospodarczą – zaświadczenie o wpisie do ewidencji działalności gospodarczej,
   3) spółki z ograniczoną odpowiedzialnością, gdy zaciągnięcie zobowiązania z tytułu realizacji zamówienia przewyższa dwukrotnie wysokość kapitału zakładowego Wykonawca zobowiązany jest przedłożyć uchwałę wspólników upoważniającą do zaciągania zobowiązań, a w przypadku gdy umowa spółki stanowi inaczej, umowę spółki wraz ze wskazanym w niej dokumentem upoważniającym do zaciągania ww zobowiązań o ile dokument taki w umowie spółki jest wymagany (art. 230 kodeksu spółek handlowych),
   4) wspólnego ubiegania się wykonawców o udzielenie zamówienia – pełnomocnictwo do reprezentowania wykonawców w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy.

2. Pełnomocnictwo osoby/osób podpisującej/podpisujących ofertę do podejmowania zobowiązań w imieniu firmy składającej ofertę, gdy nie wynika to z w/w dokumentów. W przypadku udzielenia pełnomocnictwa, wymagana jest forma i rodzaj pełnomocnictwa właściwy do poszczególnych czynności.

UWAGA:

Wymienione dokumenty muszą być aktualne na dzień składania ofert.

W przypadku dokumentów wymienionych w ust 1 za aktualne uważa się dokumenty wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

Wykonawca jest zobowiązany przedłożyć dokumenty zgodne ze stanem faktycznym.

Wniosek o zmianę wpisu w dokumencie kierowany do stosownego urzędu nie stanowi dokumentu w rozumieniu Rozporządzenia Prezesa Rady Ministrów z dnia 19 maja 2006 r. w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy oraz form w jakich te dokumenty mogą być składane.

Wykonawca zobowiązany jest złożyć oryginały lub kserokopie dokumentów poświadczonych za zgodność z oryginałem przez Wykonawcę.

IX. Wadium: nie dotyczy

X. Kryteria oceny ofert i ich znaczenie:

cena = 100 %

$$\text{Ocena łączna} = \frac{\text{cena najniższa spośród ważnych ofert}}{\text{cena podana przez danego wykonawcę}} \times 100\ \%$$

XI. Miejsce składania ofert: Dziennik Podawczy Miejskiego Ośrodka Pomocy Społecznej w Krakowie, ul. Józefińska 14,

XII. Termin składania ofert: 16.07.2008 r. godz. 8:30

XIII. Termin związania ofertą: 30 dni od dnia złożenia oferty

XIV. Czy Zamawiający zamierza zawrzeć umowę ramową: nie

XV. Czy Zamawiający zamierza ustanowić dynamiczny system zakupów: nie

XVI. Osoby upoważnione do kontaktu z wykonawcami: Wojciech Porębski, Paweł Cichopek; fax (012) 616-54-28

XVII. Data zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych: 8.07.2008

MIEJSKI OŚRODEK POMOCY SPOŁECZNEJ
Kraków, ul. Józefińska 14
wpł.dn. 08. LIP. 2008
L. dz. .....
Otrzymują .....

DYREKTOR
mgr Józefa Grodecka

Starszy Inspektor
mgr Wojciech Porębski