SĄD NAJWYŻSZY
00-951 Warszawa, Pl. Krasińskich 2/4/6

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

(W TRYBIE PRZETARGU NIEOGRANICZONEGO)

dla

przystępujących do postępowania o udzielenie zamówienia publicznego

NA DOSTAWĘ SYSTEMU ZABEZPIECZANIA DOSTĘPU DO SIECI KOMPUTEROWEJ SĄDU NAJWYŻSZEGO

(wg art. 39 - 46 ustawy Prawo Zamówień Publicznych,
przy szacunkowej wartości zamówienia do 130.000 euro)

Zamawiający oczekuje, że przed przystąpieniem do opracowania oferty każdy z Wykonawców bardzo dokładnie zapozna się z niniejszą specyfikacją.

Warszawa, październik 2013 r.

Spis treści:

Załączniki do niniejszej specyfikacji:

1. Załącznik nr 1 – Wzór formularza oferty.
2. Załącznik A – Wzór oświadczenia o spełnieniu warunków, o których mowa w art. 22 ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych.
3. Załącznik B – Oświadczenie o przynależności do grupy kapitałowej
4. Załącznik D – Wzór oświadczenia dla Wykonawcy działającego w formie prawnej spółki z ograniczoną odpowiedzialnością.

1. Nazwa oraz adres zamawiającego

Zamawiającym jest Sąd Najwyższy, z siedzibą przy Pl. Krasińskich 2/4/6 w Warszawie.

2. Tryb udzielenia zamówienia

Postępowanie prowadzone jest w trybie przetargu nieograniczonego (art. 39 – 46 ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych), przy wartości przedmiotu zamówienia nie przekraczającej równowartości 130.000 euro.

3. Opis przedmiotu zamówienia

Kod zamówienia wg CPV 32424000-1

3.1. Przedmiotem zamówienia jest dostawa systemu zabezpieczania dostępu do sieci komputerowej Sądu Najwyższego obejmująca:

- system zarządzania bezpieczeństwem dostępu do sieci komputerowej,
- kontroler sieci bezprzewodowej,

wraz z wdrożeniem w środowisku Zamawiającego, przeszkoleniem administratorów i sprawowaniem powdrożeniowej opieki technicznej.

3.2. Wymagania ogólne:

3.2.1. oferowane produkty muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich – w umowie Zamawiający będzie wymagał dostarczenia wraz z produktami oświadczenia przedstawiciela producenta potwierdzającego ważność i zakres uprawnień licencyjnych,

3.2.2. jeżeli oprogramowanie wymaga stosowania dodatkowych licencji lub licencji czasowych w celu zapewnienia wymaganych funkcjonalności, to należy dostarczyć takie licencje na okres 36 miesięcy.

3.3. Wymagania dotyczące systemu zarządzania bezpieczeństwem dostępu do sieci komputerowej. Oferowany system musi:

3.3.1. umożliwiać uwierzytelnienie i kontrolę dostępu:

- kablowego w sieci LAN,
- bezprzewodowego w sieci WLAN,
- zdalnego VPN,

3.3.2. być kompatybilny z posiadanymi przez Zamawiającego przełącznikami z serii Cisco Catalyst 6500E (Supervisor Engine 720), Cisco Catalyst 3750X, Cisco Catalyst 3750E, Cisco Catalyst 2960S, Cisco Catalyst 2960G,

3.3.3. umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based),

3.3.4. umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników,

3.3.5. posiadać lokalną bazę użytkowników, którą można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV,

3.3.6. posiadać lokalną bazę stacji końcowych, którą można tworzyć per stacja końcowa na podstawie unikalnego adresu MAC,

3.3.7. wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC za pomocą mechanizmu MAB (MAC Authentication Bypass) lub równoważnego,
3.3.8. umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o złożone reguły,
3.3.9. wspierać implementację 802.1X z co najmniej następującymi suplikantami:
- wbudowanym klientem 802.1X dla Windows XP,
- wbudowanym klientem 802.1X dla Windows Vista,
- wbudowanym klientem 802.1X dla Windows 7,
- Apple Mac OS X Supplicant,
- Cisco AnyConnect 3.x,
- Juniper Odyssey 5.x,

3.3.10. wspierać protokoły uwierzytelnienia i standardy RADIUS, zgodnie z dokumentami:
- RFC 2138 — Remote Authentication Dial In User Service (RADIUS),
- RFC 2139 — RADIUS Accounting,
- RFC 2865 — Remote Authentication Dial In User Service (RADIUS),
- RFC 2866 — RADIUS Accounting,
- RFC 2867 — RADIUS Accounting for Tunnel Protocol Support,
- RFC 2868 — RADIUS Attributes for Tunnel Protocol Support,
- RFC 2869 — RADIUS Extensions,

oraz RADIUS Proxy dla zewnętrznego serwera RADIUS,
3.3.11. wspierać co najmniej następujące protokoły uwierzytelniania:
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi: EAP-MS-CHAPv2, EAP-GTC, EAP-TLS,

3.3.12. umożliwiać równoczesną obsługę co najmniej 800 urządzeń końcowych (endpoints) przewodowych i bezprzewodowych dla funkcjonalności uwierzytelnienia, autoryzacji i dostępu gościnnego, w tym co najmniej 100 urządzeń końcowych (endpoints) przewodowych i bezprzewodowych dla funkcjonalności wykrywania i profilowania urządzeń końcowych oraz oceny stanu urządzeń końcowych,
3.3.13. umożliwiać elastyczne dodawanie licencji na potrzeby wzrostu liczby obsługiwanych urządzeń końcowych,
3.3.14. umożliwiać inkrementalą skalowalność do co najmniej 5000 równocześnie obsługiwanych urządzeń końcowych (endpoints) poprzez dodawanie kolejnych serwerów/wirtualnych instancji do istniejącego wdrożenia,
3.3.15. umożliwiać profilowanie (profiling) stacji końcowej i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu,
3.3.16. umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:
- DHCP,
- HTTP,
- RADIUS,
- Network Scan (NMAP),
- DNS,
- SNMP,

3.3.17. umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176 po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji,
3.3.18. umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy,

3.3.19. posiadać dostarczony przez producenta zestaw profili urządzeń, w tym dla:
- urządzeń z systemem Android,
- urządzeń Apple (MacBook, iPad, iPhone, iPod),
- urządzeń BlackBerry,
- stacji roboczych z systemami operacyjnymi (MS Windows 7, MS Windows Vista, MS Windows XP, FreeBSD, Linux, OS-X, OpenBSD, Sun),

3.3.20. umożliwiać głęboką analizę stacji końcowej MS Windows pod kątem plików w tym:
- istnienia pliku na stacji końcowej,
- wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż),
- daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż),

3.3.21. umożliwiać głęboką analizę stacji końcowej z systemem MS Windows pod kątem wpisów w rejestrze, w tym kluczy rejestru z kluczem root: HKLM, HKCC, HKCU, HKU, HKCR z zadanym podkluczem pod kątem:
- istnienia lub nieistnienia klucza,
- wartości klucza rejestru,
- istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version,

3.3.22. umożliwiać głęboką analizę stacji końcowej z systemem MS Windows pod kątem uruchomionych aplikacji (Application Condition), w tym nazwy uruchomionego lub nie uruchomionego procesu,

3.3.23. umożliwiać głęboką analizę stacji końcowej z systemem MS Windows pod kątem uruchomionych usług systemowych (Service Condition), w tym nazwy uruchomionego lub nie uruchomionego procesu,

3.3.24. umożliwiać głęboką analizę stacji końcowej z systemem MS Windows, Mac OS-X pod kątem zainstalowanych programów antywirusowych (AV), w tym:
- stwierdzenia czy system AV jest obecny na stacji,
- stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od daty ostatniego pliku definicji i od aktualnego czasu systemowego,

3.3.25. umożliwiać głęboką analizę stacji końcowej z systemem MS Windows, Mac OS-X pod kątem zainstalowanych aplikacji antispyware (AS), w tym:
- stwierdzenia czy system AS jest obecny na stacji,
- stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni od daty ostatniego pliku definicji i od aktualnego czasu systemowego,

3.3.26. umożliwiać tworzenie słownika prostych i złożonych warunków dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT,

3.3.27. umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym co najmniej dla:
- stacji z MS Windows 7, Vista, XP wyposażonych w przeglądarki Microsoft Internet Explorer, Mozilla Firefox, Google Chrome,
- stacji z Apple Mac OS X wyposażonych w przeglądarki Mozilla Firefox, Safari, Google Chrome,

3.3.28. umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsorów), przy czym uwierzytelnienie sponsora musi się odbywać sekwencyjnie w oparciu o:
- wewnętrzną bazę użytkowników,
- zewnętrzne repozytorium użytkowników,

3.3.29. umożliwiać konfigurację uprawnień sponsora, w tym uprawnień do:
- logowania się do systemu,
- tworzenia pojedynczego konta gościnnego,
- tworzenia wielu kont gościnnych,

- tworzenia kont losowych,
- importowania kont gościnnych z pliku CSV,
- wysyłania wiadomości e-mail po utworzeniu konta gościnnego,
- wyświetlenia hasła konta gościnnego,
- wydrukowania danych konta gościnnego,
- wyświetlenia danych stworzonych kont gościnnych,
- zawieszenia (suspend) i reinicjacji kont gościnnych,

3.3.30. umożliwiać konfigurację wyglądu portalu sponsora i gościa, w tym:
- zmianę logo strony logowania,
- zmianę obrazu tła strony logowania,
- zmianę logo bannera,
- zmianę obrazu tła bannera,
- zmianę koloru tła strony logowania,
- zmianę koloru tła strony bannera,
- zmianę koloru tła strony z treścią,
- zresetowanie ustawień do konfiguracji fabrycznej producenta,

3.3.31. umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portów http i https,

3.3.32. umożliwiać automatyczne kasowanie wygasłych kont gościnnych:
- na żądanie,
- okresowo co zadaną liczbę dni i o określonej godzinie,

3.3.33. posiadać wzorce językowe lub umożliwiać ich dodanie dla stron sponsora i gościa, w tym w językach:
- polskim,
- angielskim,

3.3.34. umożliwiać konfigurację dla użytkowników gościnnych:
- wyświetlenia im informacji o polityce akceptowalnego użycia sieci,
- zezwolenia gościom na zmianę hasła,
- wymogu zmiany hasła gościa przed wygaszeniem,
- wymogu ściągnięcia i instalacji klienta głębokiej analizy stacji (posture) przez gościa,
- samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora,
- samorejestracji urządzenia końcowego dla dostępu gościnnego,

3.3.35. umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego,

3.3.36. umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne,

3.3.37. umożliwiać konfigurację czasu ważności hasła w zadanym przedziale w dniach,

3.3.38. umożliwiać kreację profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego,

3.3.39. umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych:
- znaków alfabetu, które mogą występować w haśle,
- minimalnej ilości znaków alfabetu w haśle,
- znaków numerycznych, które mogą występować w haśle,
- minimalnej ilości znaków numerycznych w haśle,
- znaków specjalnych, które mogą występować w haśle,
- minimalnej ilości znaków specjalnych w haśle,

3.3.40. umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego:
- tworzenie nazwy użytkownika z adresu e-mail,
- minimalnej długości nazwy użytkownika,

- znaków alfabetu, które mogą występować w nazwie użytkownika,
- minimalnej ilości znaków alfabetu w nazwie użytkownika,
- znaków numerycznych, które mogą występować w nazwie użytkownika,
- minimalnej ilości znaków numerycznych w nazwie użytkownika,
- znaków specjalnych, które mogą występować w nazwie użytkownika,
- minimalnej ilości znaków specjalnych w nazwie użytkownika,

3.3.41. zapewniać wysoką dostępność wszystkich elementów funkcjonalnych, tzn. uszkodzenie systemu w jednej instancji nie może powodować niedostępności jakiejkolwiek funkcjonalności systemu dla użytkowników,

3.3.42. umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych i w ten sposób umożliwiać skalowanie rozwiązania,

3.3.43. wspierać integrację z Microsoft Windows Active Directory, w tym co najmniej Active Directory 2008 32/64-bit,

3.3.44. wspierać protokół Lightweight Directory Access Protocol (LDAP),

3.3.45. umożliwiać zarządzanie za pomocą interfejsu graficznego przez przeglądarkę internetową, w tym co najmniej: Google Chrome, Microsoft Internet Explorer, Mozilla Firefox,

3.3.46. umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym, serwerze TFTP/FTP/SFTP, udziale NFS, dysku CDROM/DVD,

3.3.47. umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).

3.3.48. umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled),

3.3.49. umożliwiać uwierzytelnianie administratorów z wykorzystaniem wewnętrznej bazy użytkowników,

3.3.50. umożliwiać wymuszenie reguł złożoności haseł dla administratorów,

3.3.51. umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora,

3.3.52. umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP,

3.3.53. umożliwiać generowanie co najmniej następujących raportów:
- raportów dla protokołów AAA: trendów uwierzytelnienia 802.1X, accountingu RADIUS, uwierzytelniania RADIUS,
- raportów dozwolonych protokołów,
- raportów dla stacji końcowych, w tym: uwierzytelnień typu MAC Authentication, Top N uwierzytelnień per adres MAC stacji, Top N uwierzytelnień per maszyna, Top N uwierzytelnień per RADIUS Calling Station ID,
- raportów dla błędów, w tym: sumarycznych przyczyn nieudanych uwierzytelnień, Top N uwierzytelnień per rodzaj błędu,
- raportów dla urządzeń sieciowych: sumarycznych uwierzytelnień dla urządzeń sieciowych, Top N uwierzytelnień per urządzenie sieciowe,
- raportów użytkowników: sumarycznych uwierzytelnień użytkowników, Top N uwierzytelnień per użytkownik, stanu provisioningu agenta Posture na stacjach końcowych, sesji użytkowników gościnnych, aktywności użytkowników gościnnych, uwierzytelnień per unikalny użytkownik,
- raportów sesji RADIUS: aktywnych sesji RADIUS, historii sesji RADIUS,

- raportów dla głębokiej analizy stacji końcowej (Posture): trendów głębokiej analizy (Posture) per skonfigurowana polityka Posture, szczegółowych wyników posture assessment per użytkownik,

3.3.54. umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
- wiadomości e-mail,
- syslog,

3.3.55. posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
- badanie łączności IP za pomocą ping, nslookup, traceroute,
- wyszukiwanie zdarzeń RADIUS z uwzględnieniem: nazwy użytkownika, adresu MAC, Audit Session ID, adresu IP NAS, numeru portu NAS, statusu uwierzytelnienia (udana lub nieudana), powodu (jeżeli uwierzytelnienie nieudane), zakresu czasowego co do dnia, godziny i minuty,
- rozwiązywanie problemów głębokiej analizy stanu stacji końcowej (Posture Assessment),
- wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu,

3.3.56. być kompatybilny z opisanym w pkt. 3.5 kontrolerem sieci bezprzewodowych,

3.3.57. być wdrożony w środowisku posiadanym przez Zamawiającego, tj. VMware vSphere 5, w postaci 2 szt. maszyn wirtualnych (virtual appliance).

3.4. Dopuszcza się zrealizowanie wymagań opisanych w pkt 3.3 w postaci zintegrowanej w jednej aplikacji lub w postaci zespołu aplikacji. W przypadku zespołu aplikacji należy zintegrować poszczególne elementy ze sobą, tak by umożliwiały tworzenie spójnych polityk bezpieczeństwa, zarządzanych centralnie, szczegółowo opisać architekturę rozwiązania i udokumentować w jaki sposób realizowane są poszczególne funkcje i jakie informacje i w jaki sposób są wymieniane przez poszczególne aplikacje. Wszystkie użyte komponenty muszą stanowić rozwiązania komercyjne z gwarantowanym wsparciem technicznym producenta. Należy dołączyć oświadczenia producentów o wzajemnej kompatybilności aplikacji oraz o wsparciu proponowanej architektury.

3.5. Wymagania dotyczące kontrolera sieci bezprzewodowej:

3.5.1. umożliwiający centralną kontrolę punktów dostępu bezprzewodowego:
- zarządzanie politykami bezpieczeństwa,
- zarządzanie pasmem radiowym,
- zarządzanie mobilnością,
- zarządzanie jakością transmisji,

zgodnie z protokołem CAPWAP (RFC 5415) lub równoważnym,

3.5.2. obsługa co najmniej 5 punktów dostępowych, z możliwością rozszerzenia do min. 200,

3.5.3. w postaci maszyny wirtualnej działającej w środowisku zwirtualizowanym pod obsługą VMware ESX/ESXi 5.x,

3.5.4. zarządzanie pasmem radiowym punktów dostępowych:
- automatyczna adaptacja do zmian w czasie rzeczywistym,
- optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia),
- dynamiczne przydzielanie kanałów radiowych,
- wykrywanie, eliminacja i unikanie interferencji,
- równoważenie obciążenia punktów dostępowych,

- tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych,
- automatyczna dystrybucja klientów pomiędzy punkty dostępowe,
- mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych,

3.5.5. mapowanie SSID do segmentów VLAN w sieci przewodowej:
- 1:1,
- 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty),
- możliwość lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID) lub tunelowania ruchu klientów do kontrolera,

3.5.6. obsługa mechanizmów bezpieczeństwa:
- 802.11i, WPA2, WPA, WEP,
- 802.1x z EAP (PEAP, EAP-TLS, EAP-FAST),
- obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, LDAP, wbudowana lokalna baza użytkowników (min. 2.000 wpisów),
- możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID,
- możliwość profilowania użytkowników: przydział sieci VLAN, przydział list kontroli dostępu (ACL),
- uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 (wykrywanie podszywania się punktów dostępowych użytkowników pod adresy infrastruktury),
- uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509,
- obsługa list kontroli dostępu (ACL),
- wykrywanie i dezaktywacja obcych punktów dostępowych,
- wbudowany system IDS wykrywający typowe ataki na sieci bezprzewodowe (fake AP, netstumbler, deathentication flood, itp.),
- współpraca z systemami IDS/IPS,
- ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego CAPWAP,

3.5.7. obsługa mobilności (roaming-u) użytkowników w ramach i pomiędzy kontrolerami,

3.5.8. obsługa mechanizmów QoS:
- 802.1p,
- WMM, TSpec,
- ograniczanie pasma per użytkownik,
- Call Admission Control – ze statyczną definicją pasma i dynamiczną w oparciu o analizę profili ruchu,
- U-APSD,

3.5.9. obsługa dostępu gościnnego:
- przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony),
- możliwość kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta,

3.5.10. współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizowania w budynku, obsługa tagów telemetrycznych,

3.5.11. mechanizmy pozwalające na dezaktywację modułów radiowych w określonych godzinach w celu redukcji poboru energii przez system,

3.5.12. zarządzanie przez HTTPS, SNMPv3, SSH,

3.5.13. kompatybilność z posiadanymi przez Zamawiającego punktami dostępowymi Cisco Aironet 1042N,
3.5.14. kompatybilność z opisanym w pkt. 3.3 systemem zarządzania bezpieczeństwem dostępu do sieci.

3.6. Wymagania dotyczące prac wdrożeniowych w środowisku Zamawiającego:
3.6.1. utworzenie projektu wdrożenia na podstawie przedstawionych na etapie wdrożenia wymagań Zamawiającego, w tym stworzenie polityki dostępu urządzeń końcowych (stacje robocze, drukarki sieciowe, laptopy, urządzenia mobilne itp.) do sieci Zamawiającego,
3.6.2. instalacja w środowisku wirtualnym i konfiguracja zgodnie z projektem wdrożenia dostarczonych produktów (kontrolera sieci bezprzewodowej oraz systemu zarządzania bezpieczeństwem dostępu do sieci złożonego z dwóch redundantnych maszyn wirtualnych),
3.6.3. integracja systemu zarządzania bezpieczeństwem dostępu do sieci z bazą Active Directory posiadaną przez Zamawiającego,
3.6.4. konfiguracja urządzeń sieciowych posiadanych przez Zamawiającego do współpracy z systemem zarządzania bezpieczeństwem dostępu do sieci oraz kontrolerem sieci bezprzewodowej,
3.6.5. konfiguracja urządzeń końcowych Zamawiającego w zakresie przewidzianym w projekcie wdrożeniowym,
3.6.6. konfiguracja dostępu gościnnego w zakresie przewidzianym w projekcie wdrożeniowym,
3.6.7. w I etapie uruchomienie rozwiązania w trybie monitoringu (bez blokowania dostępu) w celu zdiagnozowania i weryfikacji poprawności polityki dostępu do sieci oraz konfiguracji rozwiązania,
3.6.8. w II etapie docelowe uruchomienie rozwiązania w trybie kontroli dostępu do sieci.

3.7. Wymagania dotyczące szkoleń:
3.7.1. zakres taki jak w autoryzowanych szkoleniach producenta z zakresu podstawowego administrowania systemem,
3.7.2. dla 2 osób,
3.7.3. co najmniej 2 dni szkoleniowe.

3.8. Wymagania dotyczące powdrożeniowej opieki technicznej:
3.8.1. okres 12 miesięcy od wdrożenia,
3.8.2. w zakresie rekonfigurowania i rozwiązywania bieżących problemów,
3.8.3. do 10 zgłoszeń miesięcznie.

3.9. Warunki serwisu i gwarancji.
3.9.1. Oferowane produkty muszą być objęte 36-miesięcznym wsparciem serwisowym opartym na usługach serwisowych producenta, niezależnych od statusu partnerskiego Wykonawcy. Okres wsparcia serwisowego będzie liczony od daty podpisania bez zastrzeżeń protokołu odbioru końcowego przedmiotu zamówienia.
3.9.2. Oferowane wsparcie serwisowe musi zapewnić Zamawiającemu przez cały okres trwania:
- serwis świadczony w reżimie 24 godziny 7 dni w tygodniu 365 dni w roku,
- możliwość wysłania zgłoszeń serwisowych (np. dotyczących błędów w oprogramowaniu) bezpośrednio producentowi (a nie tylko Wykonawcy zamówienia),

- bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon, e-mail oraz WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją oprogramowania,
- możliwość pobierania bezpośrednio od producenta poprawek oraz nowych wydań oprogramowania zgodnie z zapotrzebowaniem Zamawiającego, jednakże w ramach ogólnie dostępnej oferty producenta, a także w ramach wykupionego zestawu funkcjonalności oprogramowania, wraz z wolnym od dodatkowych opłat prawem (tj. licencją) do korzystania z pobranego oprogramowania na zasadach określonych w warunkach licencyjnych dla użytkownika końcowego.

3.9.3. Zamawiający będzie wymagał dostarczenia wraz z produktami oświadczenia przedstawiciela producenta potwierdzającego objęcie oprogramowania pakietem serwisowym, spełniającym wymagania opisane w pkt 3.9.2.

3.9.4. Umowa będzie przewidywała udzielenie przez Wykonawcę gwarancji prawidłowego działania funkcjonalności wdrożonego systemu określonych w projekcie wdrożenia w okresie 12 miesięcy. Okres gwarancji będzie liczony od daty podpisania bez zastrzeżeń protokołu odbioru końcowego przedmiotu zamówienia. Przywrócenie prawidłowego działania funkcjonalności systemu będzie musiało nastąpić w ciągu 4 godzin od zgłoszenia, a za każdą godzinę opóźnienia Zamawiający będzie mógł naliczyć karę umowną w wysokości 500 zł.

4. Opis części zamówienia

Zamawiający nie dopuszcza podziału zamówienia.
Zamawiający nie dopuszcza składania ofert wariantowych. Zamówienie musi być zrealizowane zgodnie z wymaganiami określonymi w niniejszej specyfikacji.
Zamawiający nie wyraża zgody na powierzenie przez Wykonawcę wykonania części lub całości przedmiotu zamówienia podwykonawcom.

5. Termin wykonania zamówienia

Dostawa przedmiotu zamówienia do siedziby Zamawiającego wraz z wykonaniem prac wdrożeniowych i szkoleń powinna nastąpić w ciągu 30 dni od daty podpisania umowy.

6. Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków

6.1. W postępowaniu mogą wziąć udział wszyscy Wykonawcy, spełniający warunki określone w art. 22 ust. 1 i nie wykluczeni na podstawie art. 24 ust.1 i 2 Ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych.

6.2. Wykonawcą może być podmiot gospodarczy utworzony przez osobę fizyczną, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej oraz podmioty powyższe występujące wspólnie.

6.3. Ocena spełniania warunków wymaganych od Wykonawców prowadzona będzie na podstawie analizy wymaganych dokumentów i oświadczeń metodą „zero – jedynkową". Oznacza to, iż wystarczającym powodem do wykluczenia Wykonawcy z postępowania będzie niespełnienie któregokolwiek z warunków wymienionych w pkt 6.1. SIWZ lub brak w ofercie (a następnie brak uzupełnienia, na wezwanie Zamawiającego, zgodnie z art. 26, ust. 3 Ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych)

któregokolwiek z wymaganych dokumentów lub oświadczeń, o których mowa w pkt 7 SIWZ.

7. Wykaz oświadczeń lub dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu

Dokumenty i oświadczenia, o których mowa w tym punkcie, powinny być sporządzone w języku polskim i złożone w oryginale lub jako kserokopie poświadczone za zgodność z oryginałem, przy zachowaniu obowiązujących Wykonawcę zasad reprezentacji. Zamawiający wykluczy z postępowania Wykonawcę, jeżeli stwierdzi, że dostarczone przez niego informacje, mające wpływ na wynik prowadzonego postępowania są nieprawdziwe (art. 24 ust. 2 pkt. 3 Ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych).

7.1. Aktualny odpis z właściwego rejestru, jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
7.2. Oświadczenie o spełnianiu (lub nie) wymogów art. 22 Ustawy Prawo Zamówień Publicznych w postaci określonej w Załączniku A.
7.3. Listę podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 Prawa Zamówień Publicznych (w rozumieniu Ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. Nr 50, poz. 331, z późn. zm.), albo informację o tym, że Wykonawca nie należy do grupy kapitałowej.
7.4. Dokument fakultatywny - oświadczenie Wykonawcy działającego w formie prawnej spółki z ograniczoną odpowiedzialnością wynikające z art. 230 Kodeksu Spółek Handlowych w postaci określonej w Załączniku D.
7.5. Dokument fakultatywny - umowę regulującą współpracę podmiotów występujących wspólnie (np. konsorcjum lub spółka cywilna).
7.6. Dokument fakultatywny - w przypadku gdyby oferta została podpisana przez inną osobę niż wskazują na to dokumenty dopuszczające do obrotu prawnego do oferty należy dołączyć pełnomocnictwo do występowania w imieniu Wykonawcy.
7.7. Dokument fakultatywny - wskazanie części zamówienia, którą Wykonawca zamierza powierzyć podwykonawcom (o ile takie zamierzenie jest planowane przez wykonawcę).

8. Informacja o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń i dokumentów

8.1. Każdy Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia. Pytania Wykonawców muszą mieć formę pisemną. Kwestie odpowiedzi Zamawiającego reguluje art. 38 Ustawy PZP.

Zapytania należy kierować na adres :

Sąd Najwyższy
Pl. Krasińskich 2/4/6
00-951 Warszawa

z dopiskiem:

ZAPYTANIE DOTYCZĄCE SIWZ
NA DOSTAWĘ SYSTEMU ZABEZPIECZANIA DOSTĘPU
DO SIECI KOMPUTEROWEJ SĄDU NAJWYŻSZEGO

Zapytania skierowane faksem na numer (22) 530-90-30 powinny być ponadto niezwłocznie przekazane listem poleconym.

8.2. Zamawiający nie przewiduje zwołania spotkania informacyjnego dla Wykonawców.

9. Osoby uprawnione do porozumiewania się z wykonawcami

Osobą upoważnioną do kontaktu z Wykonawcami jest:

Maciej Pajączkowski - Dyrektor Biura Informatyki - tel. (22) 530 84 09

10. Wymagania dotyczące wadium

Zamawiający wymaga wniesienia wadium w wysokości 3 000 zł, na konto:

08 1010 1010 0401 8113 9130 0000

albo w formie gwarancji lub poręczeń zgodnie z art. 45 ust. 6 Ustawy Prawo Zamówień Publicznych.

Wadium wnoszone w pieniądzu powinno być wpłacone na konto Zamawiającego, a potwierdzenie wpłaty dołączone do oferty.

Środki pieniężne winny znaleźć się na rachunku bankowym Zamawiającego przed upływem terminu składania ofert. W przypadku wniesienia wadium w pieniądzu za moment wniesienia uznaje się moment uznania na rachunku Zamawiającego. Wadium wniesione w pieniądzu Zamawiający przechowuje na rachunku bankowym.

11. Termin związania ofertą

Wykonawcy pozostają związani złożoną przez siebie ofertą przez okres 30 dni od upływu terminu składania ofert, tj. do 10 listopada 2013 roku. Ten termin związania ofertą należy wpisać w formularz oferty.

12. Opis sposobu przygotowania ofert

12.1. Zamawiający oczekuje, że przed przystąpieniem do opracowania oferty każdy z Wykonawców bardzo dokładnie zapozna się z niniejszą Specyfikacją Istotnych Warunków Zamówienia.

12.2. Zamawiający oczekuje odniesienia się przez Wykonawców do wszystkich wymogów zawartych w Specyfikacji Istotnych Warunków Zamówienia, jak również zobowiązuje się do doprecyzowania lub uzupełnienia powyższych wymogów, w przypadku, gdy zdaniem Wykonawcy, działającego z najwyższą starannością i fachowością, takie doprecyzowanie lub uzupełnienie jest wskazane lub konieczne.

12.3.Oferta musi składać się z:

12.3.1. **Formularz Ofertowy** – powstały przez wypełnienie Załącznika nr 1 do SIWZ,

12.3.2. **Oświadczenie o spełnianiu wymogów art. 22 ust. 1 i art. 24 ust. 1 i 2** Ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych – podpisany przez Wykonawcę - powstały przez wypełnienie Załącznika A do SIWZ.

12.3.3. **Aktualny odpis z właściwego rejestru,** jeżeli odrębne przepisy wymagają wpisu do rejestru, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1

pkt 2 Ustawy Prawo Zamówień Publicznych, wystawiony **nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.**

12.3.4. **Listy podmiotów należących do tej samej grupy kapitałowej,** o której mowa w art. 24 ust. 2 pkt 5 Prawa Zamówień Publicznych (w rozumieniu Ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. Nr 50, poz. 331, z późn. zm.), albo informacji o tym, że Wykonawca nie należy do grupy kapitałowej.

12.3.5. **Umowa regulująca współpracę podmiotów występujących wspólnie** (np. konsorcjum lub spółka cywilna) – fakultatywnie.

12.3.6. **Oświadczenie Wykonawcy działającego w formie prawnej spółki z ograniczoną odpowiedzialnością** wynikające z art. 230 Kodeksu Spółek Handlowych – fakultatywnie.

12.3.7. **Pełnomocnictwo do reprezentacji** – w przypadku, gdy oferta jest podpisana przez inne osoby niż wskazują na to dokumenty dopuszczające do obrotu prawnego– fakultatywnie.

12.3.8. **Specyfikacja oferowanych produktów.**

12.3.9. **Oświadczenia producentów** o wzajemnej kompatybilności aplikacji oraz o wsparciu proponowanej architektury – fakultatywnie, zgodnie z pkt. 3.4 SIWZ.

12.3.10. **Dokumentów potwierdzających:**

- Kopia potwierdzenia wpłaty wadium na konto Zamawiającego lub oryginały gwarancji lub poręczeń zgodne z art. 45 ust. 6 Ustawy Prawo Zamówień Publicznych (w rozumieniu Ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. Nr 50, poz. 331, z późn. zm.).

12.4.Postać oferty

Oferta powinna być sporządzona w języku polskim (załączniki: certyfikaty, zaświadczenia itp. mogą być sporządzone w języku ich wydania i dostarczone wraz z tłumaczeniem na język polski), na maszynie do pisania, wydrukowana z komputera lub inną trwałą i czytelną techniką. Każdy z Wykonawców może złożyć tylko jedną ofertę, pod rygorem wykluczenia z postępowania. Wszystkie kartki oferty (na których znajduje się tekst) powinny **być trwale spięte, ponumerowane oraz parafowane lub podpisane** przez osobę (osoby) uprawnione do występowania i reprezentacji w imieniu wykonawcy. Parafowanie, trwałe spięcie i numeracja stron pełnią funkcję porządkową, nie obarczoną rygorem odrzucenia oferty.

12.5.Opakowanie i oznakowanie ofert

Oferta powinna być opakowana w trwale zamkniętą i nieprzejrzystą kopertę.

Koperta powinna być **zaadresowana na adres Zamawiającego** oraz oznakowana jak niżej, a ponadto **opatrzona nazwą i dokładnym adresem** Wykonawcy.

OFERTA NA DOSTAWĘ SYSTEMU ZABEZPIECZANIA DOSTĘPU DO SIECI KOMPUTEROWEJ SĄDU NAJWYŻSZEGO
NIE OTWIERAĆ PRZED GODZINĄ 12:30 W DNIU 10 PAŹDZIERNIKA 2013 R.

Opakowanie ofert pełni funkcję porządkową, nie obarczoną rygorem odrzucenia oferty, jednakże w przypadku innego opakowania i oznaczenia Wykonawca składający ofertę ponosi ryzyko z tego faktu wynikające.

13. Miejsce oraz termin składania i otwarcia ofert

13.1. Oferty należy składać w siedzibie Zamawiającego przy Pl. Krasińskich 2/4/6 w Warszawie, pokój nr 1 N 07 (godziny urzędowania: poniedziałek – piątek od 9:00 do 15:00).

13.2. Termin składania ofert upływa dnia 10 października 2013 r. o godzinie 12.00. W przypadku drogi pocztowej oferta musi znaleźć się w siedzibie Zamawiającego w podanym wyżej terminie. Oferty, które nadejdą po terminie nie będą rozpatrywane.

13.3. Otwarcie ofert jest jawne. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

13.4. Po otwarciu każdej z ofert, w części jawnej zostaną podane i zapisane w protokole podstawowe ich dane wg wymagań art. 86 ust. 4 Ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych.

13.5. Szczegółowe sprawdzenie ważności ofert (spełnienie warunków wymaganych od wykonawców), a następnie ocena merytorycznej treści ofert dokonane będą w części niejawnej, w sposób zgodny z uregulowaniami Ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych.

13.6. Na temat treści złożonych ofert nie będą prowadzone żadne negocjacje, Zamawiający zastrzega sobie jednak prawo wezwania Wykonawcy, celem udzielenia przez niego wyjaśnień dotyczących treści złożonej oferty, jeśli będzie to potrzebne do jej oceny.

13.7. Warunki sprawdzenia pełnej zgodności oferowanych produktów z wymogami specyfikacji.

W przypadku jakichkolwiek wątpliwości Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności oferowanych produktów z wymogami specyfikacji.

W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby Zamawiającego w terminie 10 dni od daty otrzymania wezwania, egzemplarz wskazanego przedmiotu oferty. W odniesieniu do oprogramowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty.

Nie przedłożenie oferowanych produktów do sprawdzenia w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia.

Po wykonaniu sprawdzenia, dostarczone egzemplarze będą zwrócone Wykonawcy.

14. Opis sposobu obliczenia ceny

Cenę ofertową należy wyliczyć zgodnie z zasadami podanymi w formularzu oferty.

15. Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między zmawiającym a wykonawcą

Rozliczenia prowadzone między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN). Zamawiający nie dopuszcza możliwości rozliczenia zamówienia w walutach obcych.

16. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów oraz sposobu oceny ofert

16.1. Jedynym kryterium wyboru oferty najkorzystniejszej jest cena ofertowa (100%).
16.2. W sprawie ceny podanej w ofercie nie będą prowadzone żadne negocjacje.
16.3. Zamawiający udzieli zamówienia Wykonawcy, który otrzymał największą ilość punktów, wyliczoną wg. wzoru:

$$P = c^{of}_{min} / c^{of}_{i} * 100 \text{ pkt}$$

c^{of}_{min} – najniższa cena ze wszystkich złożonych ofert,
c^{of}_{i} – cena rozpatrywanej oferty.

16.4. Jeżeli nie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że zostały złożone oferty o takiej samej cenie, zastosowanie znajdzie art. 91 ust. 5 i 6 Ustawy Prawo Zamówień Publicznych.

17. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy

17.1. O wyborze najkorzystniejszej oferty Zamawiający zawiadomi niezwłocznie wszystkich Wykonawców, którzy ubiegali się o udzielenie zamówienia, zgodnie z art. 92 Ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych.
17.2. Wykonawca, którego oferta została wybrana zostanie w powyższym powiadomieniu wezwany do podpisania umowy. Zamawiający określi również dzień podpisania umowy.

18. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy

Od wybranego Wykonawcy wymagać się będzie podpisania umowy zawierającej w swojej treści postanowienia wymienione w pkt. 3 niniejszej specyfikacji istotnych warunków zamówienia.

Przed podpisaniem umowy nie będzie wymagane wniesienie zabezpieczenia należytego wykonania umowy.

Należność za wykonanie zamówienia zostanie uregulowana przelewem, w terminie 21 dni od daty otrzymania prawidłowo wystawionej faktury, wystawionej po protokolarnym odbiorze przedmiotu zamówienia.

19. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia

Środki ochrony prawnej określone w dziale VI Ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych przysługują Wykonawcom, a także innym osobom, jeżeli mają lub miały interes w uzyskaniu zamówienia oraz poniosły lub mogły ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów powyżej przywołanej ustawy.

Dyrektor Biura Informatyki
w Sądzie Najwyższym
Maciej Pajszakowski

GŁÓWNY SPECJALISTA
d/s. Zamówień Publicznych
w Sądzie Najwyższym
dr inż. Jerzy Dylewski

Załącznik nr 1

.....
pieczątka firmowa wykonawcy

OFERTA

NA DOSTAWĘ SYSTEMU ZABEZPIECZANIA DOSTĘPU DO SIECI KOMPUTEROWEJ SĄDU NAJWYŻSZEGO

1. **Zamawiający**

   Zamawiającym jest Sąd Najwyższy, 00-951 Warszawa, Pl. Krasińskich 2/4/6.

2. **Wykonawca**

   Nazwa wykonawcy .....

   .....

   Siedziba wykonawcy .....

   .....

3. Na podstawie specyfikacji istotnych warunków zamówienia oferujemy zawarcie umowy, w której zobowiążemy się do realizacji dostawy będącej przedmiotem niniejszego zamówienia w terminie określonym w pkt 5 SIWZ.

Nazwa i skrócony opis systemu zarządzania bezpieczeństwem dostępu do sieci komputerowej z pkt. 3 SIWZ:
Nazwa: .....
Producent: .....

Nazwa i skrócony opis kontrolera sieci bezprzewodowej z pkt. 3 SIWZ:
Nazwa: .....
Producent: .....

i inne zgodnie z pkt. 3 SIWZ

Cena oferowanego rozwiązania wynosi (netto) ..... zł
(słownie zł : .....)

Cena oferowanego rozwiązania wynosi (brutto) ..... zł
(słownie zł : .....)

4. Informujemy, że zapoznaliśmy się z treścią specyfikacji istotnych warunków zamówienia. Do dokumentów postępowania nie wnosimy zastrzeżeń.

5. Oświadczamy, że uważamy się za związanych niniejszą ofertą do dnia 10 listopada 2013 r.

6. Załącznikami do naszej oferty są:

- Aktualny odpis z właściwego rejestru jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
- Załącznik A – Oświadczenie o spełnieniu warunków, o których mowa w art. 22 i 24 ustawy Prawo Zamówień Publicznych.
- Załącznik B – Oświadczenie o przynależności do grupy kapitałowej. Lista podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 Prawa Zamówień Publicznych (w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. Nr 50, poz. 331, z późn. zm.), albo informacji o tym, że Wykonawca nie należy do grupy kapitałowej.
- Załącznik C – (oraz fakultatywnie dokumenty i oświadczenia wymienione w pkt. 7 SIWZ).
- Załącznik D – oświadczenie dla spółek z ograniczoną odpowiedzialnością (fakultatywnie).
- Załącznik E – Specyfikacja techniczna oferowanych produktów.
- Załącznik F – Oświadczenia producentów o wzajemnej kompatybilności aplikacji oraz o wsparciu proponowanej architektury zgodnie z pkt. 3.4 SIWZ (fakultatywnie).

Data: ....

podpis osoby upoważnionej

Załącznik A

Pieczątka firmowa Wykonawcy

OŚWIADCZENIE

z art. 22 ust. 1 i art. 24 ust. 1 i 2 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (tekst jednolity Dz. U. 2007 r. Nr 223, poz. 1655 ze zm.)

Przystępując do udziału w postępowaniu o zamówienie publiczne **na dostawę systemu zabezpieczania dostępu do sieci komputerowej Sądu Najwyższego** w imieniu swoim i reprezentowanej przeze mnie (nas) firmy oświadczam, że:

1) Posiadamy uprawnienia do wykonywania działalności określonej przedmiotem zamówienia (art. 22 ust. 1 pkt 1),
2) Posiadamy niezbędną wiedzę i doświadczenie (art. 22 ust 1 pkt 2),
3) Dysponujemy odpowiednim potencjałem technicznym i osobami zdolnymi do wykonania zamówienia (art. 22 ust 1 pkt 3),
4) Znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie przedmiotowego zamówienia (art. 22 ust. 1 pkt 4),
5) Nie podlegamy wykluczeniu na podstawie art. 24 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych.

....., dnia ..... .2013 r.

.....
podpis(-y) osoby(osób) uprawnionej(-ych)
do reprezentowania wykonawcy

Pieczątka firmowa Wykonawcy

Załącznik B

OŚWIADCZENIE

Składając ofertę w postępowaniu o udzielnie zamówienia publicznego, którego przedmiotem jest:

DOSTAWA SYSTEMU ZABEZPIECZANIA DOSTĘPU DO SIECI KOMPUTEROWEJ SĄDU NAJWYŻSZEGO

prowadzonym przez Sąd Najwyższy oświadczamy, że

- nie należymy do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy Prawo zamówień publicznych*,
- należymy do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy Prawo zamówień publicznych*. W przypadku przynależności Wykonawcy do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy Prawo zamówień publicznych, Wykonawca składa wraz z ofertą listę podmiotów należących do grupy kapitałowej.

....., dnia ..... .2013 r.

.....
podpis(y) osoby(osób) uprawnionej
do reprezentowania wykonawcy

* niepotrzebne skreślić.

Załącznik D

Pieczątka firmowa Wykonawcy

OŚWIADCZENIE

Niniejszym oświadczamy, że zgodnie z treścią art. 230 Kodeksu spółek handlowych – Zarząd Spółki z ograniczoną odpowiedzialnością .....

.....

z siedzibą .....

wpisanej do .....

jest upoważniony do rozporządzania prawem lub zaciągnięcia zobowiązania do świadczenia o wartości do kwoty ..... zł. (słownie .....

..... złotych) bez uchwały wspólników.

Wszystkie zamówienia i umowy o wartości do powyżej wymienionej kwoty, jakie zostały przez Zarząd Spółki złożone i zawarte, pozostają w mocy prawnej zgodnie z treścią powołanego wyżej przepisu Kodeksu spółek handlowych.

....., dnia ..... .2013 r.

.....
podpis(y) osoby(osób) uprawnionej
do reprezentowania wykonawcy