

Niniejsze ogłoszenie w witrynie TED: <http://ted.europa.eu/udl?uri=TED:NOTICE:254777-2011:TEXT:PL:HTML>

**PL-Warszawa: Pakiety oprogramowania i systemy informatyczne  
2011/S 153-254777**

**OGŁOSZENIE O ZAMÓWIENIU**

**Usługi**

**SEKCJA I: INSTYTUCJA ZAMAWIAJĄCA**

**I.1) NAZWA, ADRESY I PUNKTY KONTAKTOWE**

Główny Urząd Statystyczny

al. Niepodległości 208

Kontaktowy: Główny Urząd Statystyczny, Biuro Administracyjno-Księgowe, al. Niepodległości 208, pok. 214

Do wiadomości: Jan Kozłowski

00-925 Warszawa

POLSKA

Tel. +48 226083446

E-mail: [j.kozlowski@stat.gov.pl](mailto:j.kozlowski@stat.gov.pl)

Faks +48 226083189

**Adresy internetowe**

Ogólny adres instytucji zamawiającej [www.stat.gov.pl](http://www.stat.gov.pl)

**Więcej informacji można uzyskać pod adresem:** jak podano wyżej dla punktu kontaktowego

**Specyfikacje i dokumenty dodatkowe (w tym dokumenty dotyczące dialogu konkurencyjnego oraz Dynamicznego Systemu Zakupów) można uzyskać pod adresem:** jak podano wyżej dla punktu kontaktowego

**Oferty lub wnioski o dopuszczenie do udziału w postępowaniu należy przysyłać na adres:** jak podano wyżej dla punktu kontaktowego

**I.2) RODZAJ INSTYTUCJI ZAMAWIAJĄCEJ I GŁÓWNY PRZEDMIOT LUB PRZEDMIOTY DZIAŁALNOŚCI**

Agencja/Urząd krajowy lub federalny

Ogólne usługi publiczne

Instytucja zamawiająca dokonuje zakupu w imieniu innych instytucji zamawiających Nie

**SEKCJA II: PRZEDMIOT ZAMÓWIENIA**

**II.1) OPIS**

**II.1.1) Nazwa nadana zamówieniu przez instytucję zamawiającą**

Wykonanie projektu technicznego, dostarczenie brakującej infrastruktury i licencji oraz budowa systemów: System Informacyjny Intranet, REGON, Broker Komunikacyjny, System Certyfikacji na potrzeby realizacji projektu SISP.

**II.1.2) Rodzaj zamówienia oraz lokalizacja robót budowlanych, miejsce realizacji dostaw lub świadczenia usług**

Usługi

Kategoria usług: nr 7

Główne miejsce świadczenia usług Polska.

Kod NUTS PL

**II.1.3) Ogłoszenie dotyczy**

Zamówienia publicznego

II.1.4) **Informacje na temat umowy ramowej**

II.1.5) **Krótki opis zamówienia lub zakupu(ów)**

I. Założenia ogólne

Celem zamówienia jest utworzenie spójnego środowiska dla realizacji zadań wykonywanych przez pracowników jednostek statystyki publicznej, zapewnienie pełnej integracji wdrażanych elementów przy zachowaniu ich architektonicznej separacji oraz minimalizowanie kosztów utrzymania systemu po okresie finansowania ze środków Unii Europejskiej.

Dodatkowo sposób realizacji projektu musi zapewnić przejęcie przez pracowników Zamawiającego kompetencji w zakresie administrowania i rozwijania poszczególnych elementów, w tym umożliwiać samodzielne dostosowywanie rozwiązań do zmieniających się warunków organizacyjnych i prawnych.

II. Wymagania i zakres zamówienia

Przedmiotem zamówienia jest zaprojektowanie, dostarczenie komponentów, dostarczenie brakującej infrastruktury (w tym skanerów, drukarek i czytników kodów) oraz licencji, wykonanie, zainstalowanie, uruchomienie i wdrożenie do użytkowania we wszystkich jednostkach statystyki publicznej systemu sprzętowo-programowego wraz ze szkoleniami i asystą techniczną, obejmującego następujące elementy:

1. System Informacyjny Intranet (SII) - realizujący zadania wewnętrznego portalu korporacyjnego statystyki publicznej wraz z systemem elektronicznego obiegu dokumentów obsługującego dokumenty przychodzące, wewnętrzne i wychodzące.

1) Portal korporacyjny musi zapewnić możliwość:

- a. prowadzenia wewnętrznego serwisu informacyjnego zapewniającego dostęp do firmowych informacji, aplikacji, dokumentów oraz poczty elektronicznej,
- b. pracy grupowej - wspólnej pracy nad dokumentami i wsparcia dla zespołów zadaniowych,
- c. projektowania i udostępniania aplikacji intranetowych,
- d. prowadzenia witryny osobistej pracownika – zagregowanej informacji o przydzielonych zadaniach,
- e. przekazu informacji w czasie rzeczywistym za pomocą komunikatora intranetowego,
- f. przeszukiwania zawartości całego portalu wraz z możliwością dostępu do źródeł zewnętrznych,
- g. publikowania, agregacji, analizy i raportowania danych.

2) System elektronicznego obiegu dokumentów musi zapewnić możliwość:

- a. wprowadzenia do systemu dokumentów wpływających w formie elektronicznej oraz papierowej (skanowania i wprowadzania do systemu ich cyfrowych obrazów),
- b. obsługi obiegu dokumentów elektronicznych wewnątrz organizacji oraz wysyłki dokumentów wychodzących, zarówno w formie papierowej jak i elektronicznej,
- c. zarządzania procesami pracy, w tym definiowania nowych procesów, dokonywania analizy, modelowania oraz dokonywania pomiarów procesów pracy,
- d. tworzenia nowych schematów dokumentów, spraw, raportów i elektronicznych formularzy,
- e. integracji z zewnętrznymi źródłami danych (bazy danych, usługi sieciowe) i systemami,
- f. prowadzenia elektronicznego archiwum (w tym dla dokumentów opatrzonych podpisem elektronicznym),
- g. spełnienia wymogów ustawowych, w tym w zakresie elektronicznej obsługi interesantów,

3) System SII dostarczy również funkcjonalności wspierające realizację zadań pracowników, w tym:

- a. umożliwiające zarządzanie zasobami,
- b. umożliwiające prowadzenie ewidencji czasu pracy (wykorzystywane także dla potrzeb procesów pracy),
- c. pozwalające na rejestrowanie zmian w strukturze organizacyjnej GUS oraz jednostek podległych i podporządkowanych Prezesowi GUS,
- d. indywidualny kalendarz pracownika,

e. książkę adresową pracowników.

2. System REGON – realizujący zadania krajowego rejestru urzędowego podmiotów gospodarki narodowej (REGON).

1) Celem wdrożenia jest:

- a. centralizacja systemu,
- b. modernizacja techniczna i strukturalna systemu rejestru,
- c. przygotowanie rejestru do obsługi trzech rodzajów źródeł zasilania: wniosków papierowych, wniosków elektronicznych oraz danych pozyskiwanych z innych rejestrów urzędowych i administracyjnych,
- d. zwiększenie dostępności rejestru dla osób trzecich oraz organów administracji publicznej,
- e. skrócenie czasu obsługi podmiotów,
- f. dostosowanie rejestru do nowych regulacji prawnych.

2) Zmodernizowany system rejestru REGON musi zapewnić możliwość:

- a. realizacji zadań ustawowych krajowego rejestru urzędowego podmiotów gospodarki narodowej (REGON),
- b. przechowywania bieżącego stanu rejestru oraz danych historycznych o podmiotach gospodarki narodowej, a w szczególności danych historycznych rejestru REGON wprowadzonych przed wdrożeniem zmodernizowanego systemu,
- c. wprowadzania, weryfikacji i edycji danych na podstawie wniosków papierowych, elektronicznych oraz danych pozyskiwanych z innych rejestrów urzędowych i administracyjnych (w szczególności: Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), Rejestru Szkół i Placówek Oświatowych (RSPO), Krajowej Ewidencji Podatników (KEP), Krajowego Rejestru Sądowego (KRS),
- d. generowania dokumentów elektronicznych (w szczególności zaświadczeń o numerze identyfikacyjnym REGON),
- e. udostępniania i wyszukiwania danych o podmiotach wpisanych do rejestru REGON na stronie internetowej Głównego Urzędu Statystycznego oraz platformie ePUAP,
- f. realizacji celów sprawozdawczych i raportowania,
- g. udostępniania danych rejestru na podstawie wniosków o udostępnienie danych.

3. Broker Komunikacyjny (BK)

System Broker Komunikacyjny musi zapewnić możliwość komunikacji pomiędzy niezależnymi od siebie systemami oraz stanowić platformę, która będzie udostępniała interfejsy dla usług sieciowych oraz umożliwiała przetwarzanie i monitorowanie informacji między integrowanymi systemami (ESB).

1) Celem wdrożenia jest wyeliminowanie:

- a. niespójnych informacji – integracja danych znajdujących się w wielu systemach,
- b. nieefektywnych procesów – optymalizacja procesów składających się z wielu operacji w kilku systemach,
- c. niekompatybilnych systemów – współpraca systemów, w tym takich, które nie zostały zaprojektowane z myślą o współpracy.

2) System musi zapewnić możliwość:

- a. efektywnej i prostej w zarządzaniu komunikacji między niezależnymi technologicznie systemami,
- b. pewnego i niezawodnego przesyłania komunikatów,
- c. przetwarzania i monitorowania informacji z integrowanych systemów,
- d. integracji na poziomie systemów informatycznych, procesów biznesowych i danych,
- e. stosowania standardowych, sprawdzonych komponentów architektury oraz jednolitych interfejsów dostępu do systemu,
- f. wykorzystania standardów interoperacyjności i zasad architektury korporacyjnej (EIF 2.0).

4. System Certyfikacji (SC)

System Certyfikacji będzie służył do prawidłowej realizacji przez jednostki statystyki publicznej zadań związanych z obsługą podpisu elektronicznego oraz usługą znakowania czasem. W skład zamówienia wchodzi następujące moduły funkcjonalne umożliwiające zintegrowanie z istniejącymi bądź powstającymi w jednostkach statystyki publicznej systemami, w tym systemem SII:

- a. serwer znakowania czasem (TSA),
- b. sprzętowy moduł kryptograficzny (HSM),
- c. komponent do weryfikacji podpisu elektronicznego,
- d. komponent do składania podpisu elektronicznego.

### III. Dodatkowe informacje

Użytkownikami systemu będą pracownicy Głównego Urzędu Statystycznego oraz wszystkich jednostek podległych i podporządkowanych Prezesowi GUS. Kluczową lokalizacją dla centralnie usytuowanego i zarządzanego systemu będzie siedziba Głównego Urzędu Statystycznego, będąca jednocześnie siedzibą Centrum Informatyki Statystycznej. W tym samym gmachu ulokowane są również inne instytucje statystyczne, które będą korzystać z systemu. Ponadto system pracować będzie również w siedzibach zakładów CIS w Radomiu i w Łodzi oraz w siedzibach 16 urzędów statystycznych i ich oddziałów (na dzień 16.6.2011 ich liczba wynosi 52) na terenie całego kraju. Maksymalna liczba użytkowników wewnętrznych wynosić będzie 7500, a maksymalna liczba użytkowników w jednej lokalizacji – 1500.

#### 1. Przedmiot zamówienia dla każdego z elementów obejmuje:

- 1) Sporządzenie analizy wymagań,
- 2) Wykonanie projektu technicznego,
- 3) Dostarczenie brakującej infrastruktury, w tym tzw. małej infrastruktury (skanery, drukarki i czytniki kodów),
- 4) Wykonanie wszystkich komponentów i modułów,
- 5) Przeprowadzenie testów,
- 6) Sporządzenie dokumentacji,
- 7) Realizację wymaganych przez Zamawiającego szkoleń,
- 8) Świadczenie usługi asysty technicznej.

#### 2. Zamawiający informuje, że w ramach realizowanych projektów informatycznych:

- 1) wykorzystywanym standardem opisu architektury korporacyjnej jest standard TOGAF
- 2) wykorzystywaną metodyką zarządzania projektami jest metodyka Prince2.
- 3) wykorzystywaną metodyką prowadzenia projektów aplikacyjnych jest metodyka SCRUM

3. Zamawiający posiada doświadczoną i odpowiednio wyszkoloną kadrę w zakresie ww. standardów i wymaga, aby przekazywana Zamawiającemu dokumentacja architektoniczna i projektowa była zgodna z ww. standardami.

Zamawiający przewiduje udzielenie zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 6 w wysokości 50 % zamówienia podstawowego.

#### Wymagania architektoniczne.

##### 1 Wymagania architektoniczne

##### 1.1 Zasady i standardy architektoniczne

##### 1.1.1 Zasada współdzielenia danych

Dane są zarządzane w sposób scentralizowany i współdzielone z punktu widzenia procesów biznesowych oraz lokalizacji poszczególnych komórek organizacji. Te same dane powinny być wprowadzane do systemu tylko raz. Wymagane jest opracowanie standaryzacyjnego modelu danych, elementów danych oraz metadanych definiujących środowisko współdzielenia danych wraz z odpowiednim repozytorium.

Wymagane jest dostosowanie polityki dostępu do danych oraz wytycznych dla wytwórców nowego oprogramowania celem zagwarantowania dostępności danych dla budowanych systemów i aplikacji.

#### 1.1.2 Zasada określenia właściciela danych

Każdy element danych ma właściciela odpowiedzialnego za nadzór merytoryczny nad danymi.

#### 1.1.3 Zasada jednolitej definicji danych

Dane są zdefiniowane w spójny sposób, a ich definicje są jednolite, zrozumiałe i dostępne wszystkim użytkownikom.

#### 1.1.4 Zasada rejestracji przepływu danych

W ramach systemu powinien znajdować się mechanizm rejestrowania historii zdarzeń i komunikatów, umożliwiający zapamiętywanie wszystkich lub wybranych informacji audytowych w trwałym magazynie danych. Mechanizm ten powinien umożliwić monitorowanie i przegląd poszczególnych kroków w ramach określonych procesów wymiany informacji (procesów biznesowych).

#### 1.1.5 Zasada udostępniania usług aplikacji

Aplikacje i systemy powinny udostępniać swoje usługi zgodnie ze standardowym sposobem wywołania usług (Web Services) i dostępu do danych (do wyboru: JDBC 2.0 i nowsze, ODBC 3.5 i nowsze, XML 1.1, natywny dla konkretnej bazy danych).

#### 1.1.6 Zasada wykorzystania usług uniwersalnych

Podczas budowy Systemu wykorzystywane powinny być usługi uniwersalne opisane w punkcie 2, udostępniane przez systemy i aplikacje eksploatowane już przez Zamawiającego.

#### 1.1.7 Standardy technologiczne

Wymagane jest aby w zakresie wykorzystywanych standardów technologicznych system był zgodny z „Rozporządzeniem Rady Ministrów z dnia 11.10.2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych” oraz z „Projekt rozporządzenia Rady Ministrów z dnia ...2011 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych”. W obszarach nie zdefiniowanych w ww. dokumentach należy uwzględnić zalecenia organizacji W3C.

Główne założenie dotyczące zapewnienia interoperacyjności to wykorzystanie komunikacji z systemami wewnętrznymi i zewnętrznymi za pośrednictwem wywoływania usług w modelu SOA:

- 1) Opis usług realizowany będzie w postaci plików – standard WSDL (wersja 1.1);
- 2) Pliki zarejestrowane będą w rejestrze usług zgodnym ze standardem: UDDI (w wersji przynajmniej najmniej 3.0);
- 3) Komunikacja pomiędzy usługami będzie zgodna z protokołem SOAP (w wersji 1.2); W ramach opisu usług, do opisu struktury komunikatów wykorzystany będzie standard XSD (w wersji 1.1).

Struktura plików wymiany danych będzie zgodna ze specyfikacją XML (wersji 1.0).

Standardy kodowania, w tym znaków narodowych zawierają się w specyfikacji XML (mogą być dowolne pod warunkiem zgodności z XML). Usługi zbudowane w oparciu o Web Services powinny zostać zaimplementowane zgodnie ze standardem OASIS WS-S (Web Services Security).

System powinien umożliwić szyfrowanie i podpisywanie komunikatów XML:

- 1) Podpis elektroniczny w formacie XML będzie zgodny ze standardem XMLsig,
- 2) Szyfrowanie dokumentów w formacie XML będzie zgodne ze standardem XMLenc.

System powinien wspierać wyszukiwanie informacji w zewnętrznych systemach zgodnie ze standardem OpenSearch v. 1.1.

Komunikacja powiadamiania i przekazywania poczty elektronicznej powinna być zgodna ze standardem SMTP. Modelowanie procesów biznesowych w systemie powinno być realizowane zgodnie z językiem modelowania UML 2.0.

System powinien wspierać szyfrowanie komunikacji w Internecie zgodnie z protokołem SSL ver. 3.0/TLS ver. 1.1.

#### 1.1.8 Standardy bezpieczeństwa

Bezpieczeństwo informacji rozumiane jest - zgodnie z normą PN-ISO/IEC 27001:2007 - jako zachowanie poufności, integralności i dostępności informacji. Dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Mechanizmy bezpieczeństwa, zastosowane do ochrony informacji, spełniać powinny przynajmniej wymagania określone w Załączniku A do normy PN-ISO/IEC 27001:2007.

Mechanizmy i procedury zapewnienia ciągłości działania systemu, w tym Plany Ciągłości Działania Systemu i Plany Odtwarzania po katastrofie, spełniać powinny przynajmniej wymagania zawarte w normach BS 25999-1 i BS 25999-2, oraz ISO/PAS 22399:2007.

Mechanizmy i procedury zarządzania jakością usług powinny spełniać wymagania i zalecenia zawarte w normach PN-ISO/IEC 20000-1:2007 oraz PN-ISO/IEC 20000-2:2007.

Analiza ryzyka zasobów informacyjnych, powinna być przeprowadzona zgodnie z wytycznymi zawartymi w normie PN-ISO/IEC 27005.

Plany i procedury z zakresu prowadzenia audytów bezpieczeństwa bazować powinny na obowiązujących normach bezpieczeństwa oraz metodykach i zaleceniach z zakresu audytu bezpieczeństwa, w tym:

- 1) PN-ISO/IEC 27001:2007,
- 2) BS 25999-1,
- 3) BS 25999-2,
- 4) PN-ISO/IEC 20000-1:2007,
- 5) PN-ISO/IEC 20000-2:2007.

#### 1.1.9 Standardy danych

Dane powinny być przechowywane w systemach relacyjnych baz danych, do których zapewniony jest dostęp zgodny ze standardem SQL 2006 – ISO/IEC 9075-14:2006.

Użyte systemy relacyjnych baz danych powinny zapewniać aplikacjom dostęp do danych za pośrednictwem interfejsu aplikacyjnego zgodnego ze standardami, do wyboru: JDBC 2.0 i nowsze, ODBC 3.5 i nowsze.

#### 1.2 Jakość

Celem procesu zarządzania jakością w środowisku Projektu jest zapewnienie, poprzez wytworzone mechanizmy kontrolne, że wszystkie wytworzone produkty i artefakty projektowe będą posiadały poziom jakości zgodny z oczekiwaniami Zamawiającego.

Istotnym założeniem przyjmowanym dla realizacji Projektu jest wymóg zgodności prac realizowanych przez Wykonawcę ze standardami jakości serii ISO 9001, ISO 2000, ISO 9000-3 oraz normami i standardami w zakresie bezpieczeństwa informacji (np.: ISO 27001, BS 25999, ISO/PAS 22399).

Na potrzeby realizacji Projektu przyjęto, że System Zarządzania Jakością zostanie zbudowany w oparciu o wytyczne metodyki Prince2, która w swoich założeniach jest zgodna z normami zarządzania jakością serii ISO 9001. Dodatkowo w obszarze zarządzania jakością oprogramowania wymagane jest spełnienie wymagań zawartych w normie ISO 9000-3. W obszarze zarządzania jakością usług IT wymagane jest spełnienie wymagań określonych w normie ISO 20000. W obszarze zarządzania bezpieczeństwem informacji wymagane jest spełnienie wymagań zawartych w normach ISO 27001, BS 25999 i ISO/PAS 22399. Wymaga się, aby wszelkie prace prowadzone po stronie Wykonawcy były zgodne z wytycznymi tych norm oraz metodyki Prince2. Zgodnie z definicją zawartą w normie ISO9000-3 System Zarządzania Jakością rozumiany jest jako zintegrowany proces trwający przez cały cykl tworzenia Systemu, od fazy rozmów z klientem do utrzymywania. Odpowiedzialność za wdrożenie i utrzymanie Systemu Zarządzania Jakością zgodnego z wymaganiami Zamawiającego spoczywa na Wykonawcy.

Procesy produkcyjne muszą zostać zdefiniowane i zaplanowane. Obejmuje to przeprowadzanie procesu produkcji w kontrolowanych warunkach, zgodnie z udokumentowanymi instrukcjami. Procesy specjalne, tzn.

takie, których efekty nie mogą zostać w pełni zweryfikowane po zakończeniu procesu, muszą mieć określone wskaźniki oceniające stan procesu i być ciągle monitorowane i kontrolowane.

Przyczyny powstawania produktów niezgodnych z wymaganiami muszą zostać zidentyfikowane i zlikwidowane przez działania korygujące. Oprócz tego, potencjalne przyczyny powstawania produktów niezgodnych z wymaganiami muszą zostać zneutralizowane na drodze działań zapobiegawczych. Oba rodzaje działań pociągają za sobą wprowadzenie zmian do procedur.

Wymagane jest planowanie i wykonywanie przeglądów, testów i audytów. Rezultaty przeglądów, testów i audytów muszą być dokumentowane i przekazywane do kierownictwa projektu. Naturalną konsekwencją przeglądów, testów i audytów jest wykonywanie działań korygujących mających na celu skorygowanie wykrytych nieprawidłowości.

Zapisy dotyczące jakości muszą być gromadzone, utrzymywane oraz dysponowane według zasad ustalonych z Zamawiającym.

### 1.3 Organizacja bezpieczeństwa

#### 1.3.1 System Zarządzania Bezpieczeństwem informacji

Wykonawca opracuje i wdroży dla projektowanych systemów, SZBI (System Zarządzania Bezpieczeństwem Informacji), wykorzystując wskazania zawarte w normie ISO serii 27001. W ramach opracowania SZBI następujące działania powinny zostać zrealizowane i udokumentowane:

- 1) Przeprowadzona powinna zostać klasyfikacja aktywów informacyjnych przetwarzanych w ramach systemu;
- 2) Przeprowadzona powinna zostać analiza ryzyka zasobów informacyjnych.;
- 3) Opracowana powinna zostać Polityka Bezpieczeństwa systemu zawierająca przynajmniej następujące zagadnienia:

- a) Deklaracja stosowania,
  - b) Zakres Polityki Bezpieczeństwa systemu,
  - c) Ogólne zasady bezpieczeństwa,
  - d) Zgodność z prawem i polskimi normami,
  - e) Odpowiedzialność za realizację,
  - f) Zakres rozpowszechniania,
  - g) Audyty bezpieczeństwa,
  - h) Tryb wprowadzania zmian;
- 4) Opracowane powinny zostać Zasady Bezpieczeństwa Systemu, z uwzględnieniem wyników analizy ryzyka,
  - 5) Zasady Bezpieczeństwa powinny być zgodne z obecnie funkcjonującym u Zamawiającego regulacjami dotyczącymi bezpieczeństwa informacji w zakresie gromadzenia, przetwarzania i udostępniania informacji, w tym w szczególności z Polityką Bezpieczeństwa Systemów Teleinformatycznych;
  - 6) Opracowane Zasady Bezpieczeństwa obejmować powinny przynajmniej następujące zagadnienia:
    - a) Organizacja bezpieczeństwa informacji,
    - b) Zarządzanie aktywami,
    - c) Bezpieczeństwo zasobów ludzkich,
    - d) Bezpieczeństwo fizyczne i środowiskowe,
    - e) Zarządzanie systemami i sieciami,
    - f) Kontrola dostępu,
    - g) Zarządzanie ciągłością działania,
    - h) Pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
    - i) Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
    - j) Zgodność z wymaganiami prawnymi i własnymi standardami;
  - 7) Opracowane powinny zostać procesy zarządzania ryzykiem;

- 8) Opracowane powinny zostać procesy zarządzania incydentami bezpieczeństwa;
- 9) Opracowane powinny zostać procesy zarządzania dostępem;
- 10) Opracowana powinna zostać polityka retencji danych;
- 11) Opracowane powinny zostać zasady bezpiecznego korzystania z systemu.

#### 1.3.2 Plany Ciągłości Działania (BCP) i Plany Odtwarzania po katastrofie (DRP)

W ramach świadczenia usługi wdrożeniowej Wykonawca opracuje i wdroży dla projektowanych systemów, plany BCP i DRP, obejmujące przynajmniej:

##### 1) Plany Ciągłości Działania:

- a) analiza wpływu zdarzeń na organizację (ang. - Business Impact Analysis - BIA),
- b) opracowanie strategii przetrwania,
- c) opracowanie Planu Ciągłości Działania,
- d) opracowanie programu szkoleń i budowania świadomości pracowników,
- e) opracowanie planu aktualizacji, testowania i audytowania planu ciągłości działania,
- f) opracowanie planu komunikacji kryzysowej,

##### 2) Plany Odtwarzania po katastrofie:

- a) opis struktury zespołów Disaster Recovery,
- b) opracowanie schematu i procedur odtwarzania po katastrofach,
- c) opracowanie scenariuszy działania w przypadku katastrofy,
- d) opracowanie procedur sporządzania kopii zapasowych,
- e) opracowanie procedur odtworzenia zasobów, które uległy awarii/katastrofie,

#### 1.3.3 Audyt bezpieczeństwa

W ramach świadczenia usługi wdrożeniowej, dla projektowanych systemów, Wykonawca opracuje plany audytu bezpieczeństwa, które będą mogły być wykorzystane do przeprowadzania wewnętrznych i zewnętrznych audytów bezpieczeństwa. Plany audytu bezpieczeństwa obejmować powinny w szczególności:

- 1) Audyt architektury modułów rozwiązania;
- 2) Audyt logiki biznesowej modułów rozwiązania;
- 3) Audyt infrastruktury techniczno-systemowej;
- 4) Audyt kodu źródłowego aplikacji składających się na moduły rozwiązania;
- 5) Audyt uprawnień, uwierzytelniania i autoryzacji i użytkowników.
- 6) Audyt zgodności z regulacjami (normy, standardy, polityki)
- 7) Testy penetracyjne aplikacji

#### 1.4 Architektura systemu bazująca na SOA

System powinien zostać zbudowany zgodnie z pryncypiami architektury SOA, w szczególności:

- 1) System musi być zbudowany w oparciu o architekturę zbudowaną z luźno ze sobą powiązanych usług, które można wielokrotnie wykorzystywać i są niezależnie od siebie zaimplementowane,
- 2) System musi umożliwić korzystanie z usług za pomocą zdefiniowanych interfejsów niezależnie od platformy systemowej,
- 3) System musi umożliwić użytkownikowi korzystanie z usług niezależnie od lokalizacji,
- 4) System musi dostarczyć mechanizm kontroli dostępu do usług,
- 5) System musi umożliwić projektowanie usług i zależności pomiędzy nimi,
- 6) System musi umożliwić projektowanie i generowanie interfejsów usług oraz ich implementację,
- 7) System musi umożliwić projektowanie i implementację komunikatów służących do wymiany informacji pomiędzy usługami,
- 8) System musi umożliwiać osadzanie i rekonfigurację nowych usług bez zakłócenia działania innych aplikacji i realizacji operacji biznesowych,

- 9) System musi zapewnić rejestr usług, który umożliwi publikację i odnajdywanie potrzebnych usług,
- 10) System musi udostępnić mechanizm monitorowania dostępności usług, zintegrowany z scentralizowanym systemem monitorowania posiadanym przez Zamawiającego.
- 11) Komunikacja pomiędzy poszczególnymi komponentami oprogramowania powinna odbywać się z wykorzystaniem szyny usług spełniającej następujące wymagania:
- 12) Szyna usług musi realizować translację komunikacji,
- 13) Szyna usług musi umożliwić integrację rejestrów danych zaimplementowanych w różnych technologiach,
- 14) Szyna usług musi realizować przekierowania komunikacji w zależności od kontekstu i treści komunikatu,
- 15) Szyna usług musi posiadać mechanizmy równoważenia obciążenia komunikacji pomiędzy węzłami,
- 16) Szyna usług musi umożliwić integrację aplikacji i usług zaimplementowanych w różnych technologiach,
- 17) Szyna usług musi zapewnić zachowanie integralności, niezaprzeczalności i poufności komunikacji,
- 18) Szyna usług musi zapewniać mechanizmy filtracji i weryfikacji poprawności komunikatów.

#### 1.4.1.1 Otwartość i możliwości rozbudowy

System musi posiadać strukturę modułową, realizującą poszczególne grupy funkcjonalności za pomocą autonomicznych komponentów. Poszczególne komponenty muszą integrować się za pomocą zestandaryzowanych interfejsów. Powyższe właściwości muszą w konsekwencji zapewniać możliwość rozbudowy funkcjonalnej systemu poprzez instalowanie nowych komponentów w środowisku aplikacyjnym, nie wymagając przy tym poważnych modyfikacji istniejącego oprogramowania.

#### 1.5 System monitorowania usług IT

Na potrzeby projektowanych systemów, bazując na obowiązujących normach, a w szczególności ISO/IEC 2000 i ISO/IEC27001, Wykonawca dostarczy rozwiązanie wspierające monitorowanie usług IT. W szczególności rozwiązanie wspierać musi co najmniej następujące obszary:

- 1) Zarządzanie zdarzeniami i logami,
- 2) Monitorowanie dostępności,
- 3) Monitorowanie wydajności i pojemności,
- 4) Monitorowanie podatności.

Do budowy rozwiązania wspierającego monitorowanie usługami IT Wykonawca wykorzystać powinien systemy i oprogramowanie posiadane i eksploatowane obecnie przez zamawiającego udostępniające usługi uniwersalne opisane w punkcie 2. Wykonawca dostarczy licencje i infrastrukturę techniczno-systemową niezbędną do rozbudowy systemów posiadanych i eksploatowanych przez zamawiającego w celu spełnienia wymagań Zamawiającego.

#### 1.5.1 Zarządzanie zdarzeniami i logami

System monitorowania musi spełniać następujące funkcjonalności w zakresie zarządzania zdarzeniami i logami:

- 1) Gromadzenie i utrzymywanie informacji historycznych dotyczących pojemności, wydajności i dostępności;
- 2) Gromadzenie historycznych raportów skanowania podatności i integralności;
- 3) Gromadzenie zdarzeń generowanych przez różne źródła w formatach SNMP oraz syslog;
- 4) Umożliwienie wykonywania analizy danych historycznych pod kątem planowania w zakresie wydajności, pojemności, dostępności, podatności i integralności;
- 5) Umożliwienie elastycznego definiowania raportów na podstawie zgromadzonych danych, niezależnie od ich typu i źródła;
- 6) Umożliwienie graficznego przedstawienia informacji o stanie monitorowanych elementów infrastruktury i aplikacji;
- 7) Umożliwienie korelacji zdarzeń pochodzących z różnych źródeł (m.in. systemu monitorowania, logów systemów operacyjnych, urządzeń sieciowych) w celu wykrycia źródła potencjalnych problemów oraz zidentyfikowania incydentów. Korelacja zdarzeń powinna polegać zarówno na określaniu relacji między

zdarzeniami tej samej klasy (np. pochodzącymi z tego samego źródła lub tej samej klasy źródeł) jak i określaniu relacji między zdarzeniami różnych klas. Wynikiem procesu korelowania zdarzeń powinno być wygenerowanie odpowiedniego nowego zdarzenia, zwanego incydem, do obsłużenia przez operatora, maszyną korelacyjną wyższego poziomu lub inny system informatyczny. Korelowane zdarzenia mogą dotyczyć tych samych lub różnych zasobów;

- 8) Umożliwienie elastycznego definiowania i określania reguł korelacji z poziomu interfejsu administracyjnego.
- 9) Umożliwienie powiadamiania o przekroczeniu dopuszczalnych progów w zakresie dostępności, pojemności i wydajności;
- 10) Udostępnianie dla administratorów systemu graficznego interfejsu w przeglądarce;
- 11) Skalowalność zarówno w zakresie rozbudowy elementów monitorowanych jak i w zakresie nowej funkcjonalności monitorowania;
- 12) Zapewnienie jednego, wiarygodnego źródła czasu dla wszystkich urządzeń, systemów i aplikacji pracujących w ramach portalu.

#### 1.5.2 Monitorowanie dostępności

System monitorowania musi spełniać następujące wymagania funkcjonalne w zakresie monitorowania dostępności:

- 1) Monitorowanie stanu pracy serwerów oraz innych urządzeń (np. urządzenia sieciowe, macierze, biblioteki taśmowe) wchodzących w skład infrastruktury technicznej;
- 2) Monitorowanie stanu pracy systemów operacyjnych, oprogramowania narzędziowego oraz aplikacji użytkowych;
- 3) Monitorowanie dostępności kanałów komunikacyjnych LAN i WAN;
- 4) Monitorowanie dostępności warstwy front-end w sieci Internet;
- 5) Analiza dostępności systemów pracujących w układach klastrowych;
- 6) Monitorowanie istnienia wybranych plików;
- 7) Monitorowanie czasu odpowiedzi urządzeń sieciowych;
- 8) Monitorowanie informacji o błędach pochodzących z urządzeń oraz oprogramowania.

#### 1.5.3 Monitorowanie wydajności i pojemności

System monitorowania musi spełniać następujące wymagania funkcjonalne w zakresie monitorowania wydajności i pojemności:

- 1) Monitorowanie stopnia wykorzystania zasobów serwerów (procesory, pamięć operacyjna, interfejsy sieciowe itp.);
- 2) Monitorowanie oprogramowania narzędziowego (np. baz danych, serwery aplikacyjne) pod kątem wykorzystania zasobów im przydzielonych;
- 3) Monitorowanie obciążenia kanałów komunikacyjnych LAN i WAN;
- 4) Monitorowanie ilości zalogowanych do systemu użytkowników zewnętrznych;

#### 1.5.4 Monitorowanie podatności

System monitorowania musi spełniać następujące wymagania funkcjonalne w zakresie monitorowania podatności:

- 1) Skanowanie systemów operacyjnych serwerów, serwerów WWW i urządzeń sieciowych w poszukiwaniu typowych błędów konfiguracji zabezpieczeń;
- 2) Skanowanie systemów operacyjnych serwerów, serwerów WWW i urządzeń sieciowych pod kątem wystąpienia luk umożliwiających nieautoryzowany dostęp;
- 3) Skanowanie systemów pod kątem aktualności zainstalowanych uzupełnień;
- 4) Wykrywanie usług uruchomionych na serwerach, w tym wykrywanie usług zbędnych i niebezpiecznych;
- 5) Wykrywanie kont lokalnych niezgodnych z aktualną polityką bezpieczeństwa (np. posiadających puste hasła);

- 6) Skanowanie systemów zapór (firewall) w celu weryfikacji szczelności i efektywności ich działania;
- 7) Weryfikacja zgodności aktualnych zabezpieczeń z bieżącymi zaleceniami i politykami bezpieczeństwa.

#### 1.6 Mechanizmy kontroli i zarządzania dostępem

System powinien spełniać następujące wymagania z zakresu kontroli i zarządzania dostępem:

- 1) System powinien dostarczać mechanizmy kontroli dostępu administratorów umożliwiające dostęp do systemu wyłącznie po jednoznacznym zidentyfikowaniu przeprowadzonym w ramach procesu uwierzytelnienia;
- 2) System powinien zapewniać odpowiednie mechanizmy uwierzytelniania użytkowników nie anonimowych;
- 3) System powinien zapewniać odpowiednie zabezpieczenia przed nieautoryzowanym dostępem na poziomie wszystkich komponentów serwera (system operacyjny, motory baz danych, serwery aplikacyjne, serwery WWW i inne, jeśli zostaną zastosowane);
- 4) System powinien przechowywać i przysyłać hasła użytkowników wyłącznie w postaci zabezpieczonej;
- 5) System powinien zapewniać mechanizmy kontroli uprawnień oparte na rolach, umożliwiające kontrolę poziomu dostępu każdego użytkownika zarówno w zakresie dostępu do danych przetwarzanych, jak i korzystania z jego funkcjonalności. System uprawnień musi umożliwić ograniczenie dostępu wyłącznie do takich danych oraz takiego zakresu funkcji, jaki jest niezbędny użytkownikowi;
- 6) System powinien posiadać mechanizmy umożliwiające rozliczalność działań użytkowników systemowych i nie anonimowych;
- 7) System powinien posiadać mechanizmy umożliwiające rozliczalność działań administracyjnych związanych z nadawaniem i odbieraniem uprawnień.
- 8) System powinien umożliwiać podział użytkowników na grupy z możliwością przynależenia do kilku grup równocześnie;
- 9) System powinien umożliwiać zarządzanie użytkownikami oraz grupami w zakresie ustalania uprawnień;
- 10) System powinien umożliwiać blokowanie dostępu określonym grupom użytkowników do zdefiniowanych zasobów systemu;
- 11) Hasło użytkownika utrwalone w systemie nie może być zapisane otwartym tekstem. System powinien przechowywać postać hasła po przetworzeniu algorytmu bezpiecznej do zastosować kryptograficznych jednokierunkowej funkcji mieszającej (np. SHA-1);

#### 1.7 Mechanizmy kryptograficzne

System powinien spełniać następujące wymagania z zakresu mechanizmów kryptograficznych:

- 1) W przypadku szyfrowania rozwiązanie powinno implementować mechanizmy kryptograficzne oparte na powszechnie uznanych standardach. Moc wykorzystanych algorytmów kryptograficznych nie powinna być mniejsza od mocy zapewnianej przez takie algorytmy jak System.Security.Cryptography.TripleDESCryptoServiceProvider System.Security.Cryptography.Aes (AES-128) System.Security.Cryptography.RSA (RSA-1024), System.Security.Cryptography.SHA1
- 2) Rozwiązanie powinno zapewniać zabezpieczenie transmisji danych wrażliwych pomiędzy urządzeniem końcowym a serwerami aplikacyjnymi. Poziom zabezpieczenia transmisji nie powinien być mniejszy od poziomu zapewnianego przez protokoły SSL ver. 3.0/TLS ver. 1.1 z kluczem o długości 128 bitów;
- 3) Rozwiązanie powinno umożliwiać wykorzystanie usług kryptografii asymetrycznej (PKI), w szczególności:
  - a) oznaczania dokumentów wiarygodnym czasem przez zaufany urząd znakowania czasem będący na liście kwalifikowanych podmiotów świadczących usługi certyfikacyjne oraz wewnętrzny serwer znakowania czasem budowany w ramach zadania SC,
  - b) elektronicznego podpisywania dokumentów za pomocą zarówno certyfikatów kwalifikowanych, jak i niekwalifikowanych,
  - c) weryfikacji podpisu elektronicznego.

4) Dla każdego serwera świadczącego usługi zabezpieczone protokołem HTTPS Wykonawca musi dostarczyć certyfikaty SSL (w standardzie X.509 v3) wydane przez krajowy lub międzynarodowy zaufany urząd certyfikacji (np.: Unizeto, KIR, PWPW, Mobicert, SAFE Technologies, VeriSign, Thawte).

#### 1.8 Mechanizmy rozliczalności

System powinien spełniać następujące wymagania z zakresu rozliczalności:

System powinien zapewniać mechanizmy logowania operacji: prób logowania i wylogowania użytkownika, modyfikacji danych, wykonanych akcji w systemie wraz z rejestracją czasu operacji, identyfikatora użytkownika oraz wyniku operacji;

System powinien zapewniać mechanizmy przechowywania logów systemowych w sposób chroniący je przed modyfikacją i nieuprawnionym usunięciem.

2 Usługi uniwersalne dostarczane przez systemy i aplikacje eksploatowane przez Zamawiającego

W ramach projektu SISP COIS-2/2010/SISP zbudowane zostały następujące Systemy udostępniające usługi uniwersalne:

1) Uwierzytelnianie, autoryzacja i zarządzanie tożsamością

a) System usług katalogowych

b) System PKI

c) System zarządzania tożsamością użytkowników i rolami

2) Monitorowanie, zarządzanie i raportowanie

a) System monitorowania i wizualizacji

b) System zarządzania siecią

3) System ServiceDesk

Systemy te tworzą zintegrowane środowisko informatyczne udostępniające podstawowe usługi niezbędne do pracy szeregu wdrażanych i planowanych w GUS systemów informatycznych i aplikacji.

#### 2.1 System usług katalogowych

System usług katalogowych oparty jest na technologii Microsoft Active Directory w wersji 2008. Stanowi on jeden z kluczowych elementów infrastruktury informatycznej Statystyki Publicznej. Pełni on rolę zintegrowanej platformy wspierającej pracę użytkowników, stacji roboczych, serwerów i aplikacji, zarządzania środowiskiem pracy użytkowników oraz konfiguracji ustawień bezpieczeństwa.

System realizuje następujące usługi:

1) Centralny katalog informacji o użytkownikach i komputerach.

2) Centralny katalog informacji o zasobach (w tym: sieciowe zasoby plikowe oraz drukarki).

3) Uwierzytelnienie użytkowników i stacji roboczych w obrębie sieci korporacyjnej.

4) Autoryzacja użytkowników przy dostępie do aplikacji i zasobów.

5) Zarządzanie konfiguracją komponentów oprogramowania na stacjach roboczych w tym konfiguracja ustawień bezpieczeństwa (platforma Windows).

6) Scentralizowane zarządzanie konfiguracją bezpieczeństwa dla serwerów (platforma Windows).

7) Zestaw usług sieciowych niezbędnych do funkcjonowania całego systemu sieciowego:

a) DNS – usługa hierarchicznego rozwiązywania nazw sieciowych.

b) DHCP – usługa automatycznego przydzielania sieciowych adresów IP.

c) LDAP – protokół dostępu do systemu usług katalogowych.

d) Kerberos - protokół uwierzytelniania i autoryzacji.

#### 2.2 System PKI

Infrastruktura Klucza Publicznego (ang. Public Key Infrastructure - PKI) zbudowana została na bazie usług certyfikacyjnych systemu MS Windows Server 2008. Infrastruktura Klucza Publicznego tworzona na potrzeby

Statystyki Publicznej przeznaczona jest do wspomagania funkcji związanych z uwierzytelnianiem i autoryzacją do zasobów teleinformatycznych. Zarówno uwierzytelnianie, jak i autoryzacja dotyczyć mogą:

- 1) użytkowników systemów teleinformatycznych,
- 2) serwerów,
- 3) usług systemowych i aplikacyjnych.

System realizuje następujące usługi:

- 1) wydawanie certyfikatów cyfrowych w formacie zgodnym ze standardem X.509 v3,
- 2) unieważnianie wydanych certyfikatów cyfrowych,
- 3) publikowanie certyfikatów cyfrowych w repozytorium (ldap, serwer webowy),
- 4) definiowanie szablonów certyfikatów określających przeznaczenie certyfikatów, a w szczególności certyfikatów wykorzystywanych w następujących operacjach:
  - a) logowanie do systemu MS Windows,
  - b) szyfrowanie komponentów systemu plików MS Windows z wykorzystaniem mechanizmu EFS
  - c) szyfrowanie i podpis poczty elektronicznej,
- 5) archiwizacja wybranych kluczy prywatnych,
- 6) bezpieczne zarządzanie urzędami certyfikacji w wykorzystaniu zasady segregacji obowiązków,
- 7) publikowanie list certyfikatów unieważnionych (ang. Certificate Revocation List) w repozytorium (ldap, serwer webowy),
- 8) weryfikacji ważności certyfikatów w oparciu o listy CRL,
- 9) weryfikacja ważności certyfikatów w oparciu o mechanizm OCSP (ang. Online Certificate Status Protocol)

### 2.3 System zarządzania tożsamością użytkowników i rolami

Zadaniem systemu jest usprawnienie procesu zarządzania tożsamościami elektronicznymi użytkownikami.

W ramach systemu uruchomiony jest katalog korporacyjny, który pełni funkcję źródła informacji o rolach biznesowych użytkowników Projektu i przypisanych im uprawnieniach. Katalog korporacyjny nie uczestniczy w procesie uwierzytelniania i autoryzacji użytkowników. Informacjami o tożsamościach elektronicznych, przypisanych im rolach biznesowych i związanych z nimi uprawnieniach zasilany jest katalog operacyjny LDAP wchodzący w skład systemu usług katalogowych Active Directory.

Do budowy systemu zarządzania tożsamością użytkowników i rolami wykorzystane zostało rozwiązane Quest One firmy Quest Software, składające się z Quest Active Roles Server, Quest ActiveRoles Quick Connect for Base Systems oraz Quest ActiveRoles Self Service Manager.

W skład systemu IDM wchodzi następujące moduły:

- 1) Główny moduł systemu IDM
- 2) Moduł bezpieczeństwa
- 3) Moduł Self-Service
- 4) Moduł zarządzania rolami i regułami biznesowymi
- 5) Moduł zarządzania katalogiem korporacyjnym i jego zasobami
- 6) Moduł zarządzania zatwierdzaniem zmian i przepływem informacji
- 7) Moduł propagacji uprawnień

System realizuje następujące usługi:

Główny moduł systemu IDM udostępnia następujące usługi:

- 1) Centralizuje administrację uprawnieniami użytkowników,
- 2) Kontroluje dostęp do aplikacji na zasadzie przynależności użytkownika do określonych grup domenowych,
- 3) W katalogu korporacyjnym przechowuje informacje o rolach biznesowych, odpowiadających im uprawnieniom i tożsamościach elektronicznych, oraz związanych z nimi relacjach,

- 4) Zasila katalog operacyjny LDAP (usługa katalogowa Microsoft Active Directory) informacjami o tożsamościach elektronicznych, przypisanych im rolach biznesowych i związanych z nimi uprawnieniach,
- 5) Zapewnia spójność danych pomiędzy Katalogiem Korporacyjnym a Katalogiem Operacyjnym,
- 6) Umożliwia czasowe przydzielanie użytkowników do grup,
- 7) Umożliwia pełne raportowania o zmianach oraz aktywności użytkowników,
- 8) Umożliwia automatyczne uzupełnianie danych (np. opis, adres e-mail, login name) po wprowadzeniu podstawowych atrybutów np. imię i nazwisko,
- 9) Dostarcza widoki biznesowe pokazujące tylko te obiekty środowiska, którymi zarządza lub za które odpowiada użytkownik/administrator,
- 10) Zawiera interfejs webowy dla administratorów,
- 11) Zawiera interfejs webowy dla pracowników Service Desk,
- 12) Umożliwia modyfikację interfejsów Web dla użytkowników końcowych, w tym stworzenie różnych wersji językowych,
- 13) Zapewnia mechanizmy blokowania i archiwizacji kont użytkowników,
- 14) Umożliwia definiowanie dodatkowych atrybutów dla użytkowników bez konieczności rozszerzania schematu usług katalogowych LDAP,
- 15) Wykorzystuje do zarządzania mechanizmy Power Shell oraz SPML.

Moduł Self Service udostępnia następujące usługi:

- 1) Oferuje centralne miejsce do zgłaszania wniosków użytkowników o przydzielenie dostępu,
- 2) Umożliwia użytkownikom zarządzanie swoim kontem oraz danymi osobistymi (np. edycję atrybutów) poprzez interfejs webowy,
- 3) Umożliwia użytkownikom wnioskowanie o zmiany w dostępie,
- 4) Zapewnia spersonalizowane interfejsy webowe dla personelu Service Desk oraz właścicieli danych,
- 5) Oferuje mechanizm kontroli uprawnień użytkowników dla zarządzanych zasobów,
- 6) Umożliwia wyznaczonym osobom kontrolować dostępy pracowników i jednocześnie zarządzać ich prawami dostępu danych lub aplikacji,
- 7) Umożliwia resetowanie hasła użytkownika przez jego samego bez potrzeby zgłaszania takich sytuacji do działu Service Desk.

Moduł zarządzania katalogiem operacyjnym udostępnia następujące usługi:

- 1) Zapewnia zarządzanie środowiskiem usług katalogowych LDAP oraz zasobami serwerów Windows z poziomu jednego interfejsu,
- 2) Umożliwia dynamiczne zarządzanie przynależnością użytkowników do grup w domenie Active Directory, na podstawie informacji o nadanych im rolach biznesowych.
- 3) Zapewnia bezpieczny oraz zautomatyzowany proces zarządzania użytkownikami w środowisku usług katalogowych LDAP z usługą systemu Kerberos (tworzenie, modyfikowanie obiektów, blokowanie) a także umożliwia rozszerzenie tego procesu do innych aplikacji/systemów,
- 4) Zawiera mechanizmy do zarządzania środowiskiem usług katalogowych LDAP z poziomu przeglądarki WWW, bez konieczności instalowania przez użytkowników/administratorów dodatkowego oprogramowania na swoich stacjach roboczych,

Moduł zarządzania rolami i regułami biznesowymi udostępnia następujące usługi:

- 1) Rozdziela role użytkowników w środowisku usług katalogowych LDAP przydzielając im odpowiednie zestawy uprawnień i dostępu do aplikacji/systemów w środowisku,
- 2) Zapewnia mechanizmy sprawdzające poprawność danych wprowadzanych do usług katalogowych LDAP oraz zgodność ze standardem lub wypracowanym szablonem,

3) Umożliwia bardzo szczegółowe przydzielanie uprawnień dla użytkowników usług katalogowych LDAP oraz systemów takich jak Exchange, DNS, DHCP, Windows,

4) Umożliwia definiowanie uprawnień/ról dla grup i użytkowników,

Moduł bezpieczeństwa udostępnia następujące usługi:

1) Zapewnia centralne audytowanie zmian administracyjnych.

2) Zapewnia komunikację szyfrowaną pomiędzy interfejsem użytkownika, a serwerem zarządzającym,

3) Zapewnia raportowanie historii zmian informacji o tożsamościach użytkowników

4) Oddziela natywne uprawnienie użytkowników w środowisku usług katalogowych LDAP od uprawnień

przydzielonych w systemie zarządzania tożsamością, dzięki czemu zabezpiecza możliwość wykonania zmian natywnie (za pomocą narzędzi systemowych) na usługach katalogowych LDAP,

5) Oferuje kontrolę dostępu na poziomie uprawnień do systemu,

6) Chroni dane usług katalogowych LDAP przed niepowołanym dostępem,

7) Chroni przed możliwością wprowadzania niespójnych informacji lub niezgodnych z polityką firmy do usług katalogowych LDAP

Moduł propagacji uprawnień udostępnia następujące usługi:

1) Upraszcza wprowadzanie danych poprzez integrację z zewnętrznymi źródłami danych takimi jak systemy ERP/HR, bazami danych Oracle, SQL Server i innymi środowiskami,

2) Wspiera realizację procesów propagacji uprawnień (automatyczne tworzenie konta i roli w środowisku usług katalogowych LDAP, nadawanie im uprawnień, wypełnianie atrybutów, tworzenie skrzynki pocztowej, tworzenie folderów domowych, aliasów poczty oraz dowolnych akcji wykonanych za pomocą skryptów), re-provisioningu (automatycznego odbierania uprawnień, przededefiniowania atrybutów oraz przydzielaniu nowych uprawnień, zmiana roli pracownika) oraz deprovisioningu (blokowanie konta, resetowanie hasła, przenoszenie do innej jednostki organizacyjnej, kasowanie atrybutów),

3) Posiada opcję umożliwiającą zarządzanie dostępem do MS SharePoint,

4) Oferuje możliwość integracji poprzez następujące protokoły (SQL connection, ODBC, LDAP, CSV, SunOne, SharePoint, ADAM/AD LDS, Novell, Oracle connection)

5) Wspiera synchronizację haseł

Moduł zarządzania zatwierdzaniem zmian i przepływem udostępnia następujące usługi:

1) Umożliwia kontrolę i zarządzanie mechanizmem akceptacji zmian usług katalogowych LDAP oraz innych systemów połączonych rozwiązaniem do zarządzania tożsamością

2) Umożliwia tworzenie szczegółowego mechanizmu akceptacji/odrzućcia zmian

#### 2.4 System monitorowania i wizualizacji

W skład systemu monitorowania i wizualizacji wchodzi następujące moduły:

1) Moduł zarządzania konfiguracją stacji roboczych

2) Moduł zarządzania konfiguracją serwerów

3) Moduł monitorowania serwerów i aplikacji dla platformy Windows

4) Moduł monitorowania podatności

5) Moduł zarządzania licencjami

6) Moduł zarządzania zdarzeniami i logami

7) Moduł raportowania i wizualizacji

##### 2.4.1 Moduł zarządzania konfiguracją stacji roboczych

Moduł zarządzania konfiguracją stacji roboczych zbudowany został w oparciu o rozwiązanie MS SCCM 2007.

Realizuje on następujące usługi:

1) inwentaryzacja sprzętu oraz oprogramowania,

2) automatyczna dystrybucja oraz instalacja oprogramowania,

- 3) automatyczna dystrybucja oraz instalacja poprawek i aktualizacji dla oprogramowania (realizowane przez WSUS),
- 4) usługi zdalnego zarządzania (zdalna konsola, zdalne narzędzia administracyjne i diagnostyczne uruchamiane z konsoli pracowania wsparcia),
- 5) mechanizmy software metering dla potrzeb pomiaru wykorzystania aplikacji,
- 6) komponent OSD (Operating System Deployment).

Usługi zarządzające dotyczą następujących platform systemowych:

- 1) Windows XP Professional.
- 2) Windows Vista Bussines/ Ultimate/Enterprise.
- 3) Windows 7 Professional/Ultimate.

#### 2.4.2 Moduł zarządzania konfiguracją serwerów

Moduł zarządzania konfiguracją serwerów zbudowany został w oparciu o rozwiązania MS SCCM 2007.

Realizuje on następujące usługi:

- 1) inwentaryzacja sprzętu oraz oprogramowania,
- 2) automatyczna dystrybucja oraz instalacja oprogramowania,
- 3) automatyczna dystrybucja oraz instalacja poprawek i aktualizacji dla oprogramowania (realizowane przez WSUS),
- 4) usługi zdalnego zarządzania (zdalna konsola, zdalne narzędzia administracyjne i diagnostyczne uruchamiane z konsoli pracowania wsparcia),
- 5) komponent OSD (Operating System Deployment).

Usługi zarządzające dotyczą następujących platform systemowych:

- 1) Windows 2000 Server,
- 2) Windows Server 2003 (również wersje x64),
- 3) Windows Server 2008 (również core i x64),
- 4) Windows Server 2008 R2.

#### 2.4.3 Moduł monitorowania serwerów i aplikacji dla platformy Windows

Moduł monitorowania konfiguracją serwerów i aplikacji dla platformy Windows zbudowany został w oparciu o rozwiązanie MS SCOM 2007. Realizuje on następujące usługi:

- 1) gromadzenie i archiwizacja danych o zdarzeniach,
- 2) detekcja i identyfikacja incydentów,
- 3) alerty administratorów systemów i użytkowników - określenie oczekiwanych działań użytkowników w przypadku pojawienia się i zaobserwowania nietypowych lub podejrzanych działań,
- 4) określenie poszczególnych poziomów alertów,
- 5) raportowanie.
- 6) Wykrywanie przekroczenia ustalonych progów wydajności sprzętu i oprogramowania oraz dostępności aplikacji usług i procesów.
- 7) Powiadamianie administratorów o przekroczeniu dopuszczalnych progów wykorzystania monitorowanych zasobów.
- 8) Monitorowanie systemów operacyjnych:
  - a) Windows 2000 Server,
  - b) Windows Server 2003 (również wersje x64),
  - c) Windows Server 2008 (również core i x64),
  - d) Windows Server 2008 R2.
- 9) Weryfikacja poprawności pracy agentów monitorowania.

- 10) Gromadzenie i utrzymywanie informacji historycznych dotyczących monitorowanych elementów infrastruktury.
- 11) Powiadomianie administratorów o niedostępności monitorowanych serwerów i urządzeń.
- 12) Wykonywanie zdalnych akcji (komenda na systemie, uruchomienie skryptu, etc) na systemie monitorowanym z poziomu konsoli centralnego systemu zarządzania.
- 13) Możliwość definiowania automatycznego uruchamiania takich akcji w przypadku wybranych zdarzeń.
- 14) Udostępnianie konsoli alarmów oraz stanu monitorowanych usług poprzez konsolę przeglądarki internetowej.
- 15) Dostęp do systemu monitorowania poprzez konta dla upoważnionych użytkowników i chronić je hasłem.
- 16) Monitorowanie poziomu wykorzystania zasobów sprzętowych serwerów:
  - a) procesory,
  - b) pamięć operacyjna,
  - c) przestrzeń dyskowa,
  - d) interfejsy sieciowe.

#### 2.4.4 Moduł monitorowania podatności

Moduł monitorowania podatności zbudowany został w oparciu o rozwiązanie Nessus firmy Tenable Network Security. Realizuje on następujące usługi:

1) Monitorowanie podatności obejmujące następujące platformy systemowe:

- a) systemy z rodziny MS Windows,
- b) systemy Linux.

2) Monitorowanie podatności obejmujące następujące platformy aplikacyjne:

- a) IIS,
- b) MS SQL Server,
- c) MS Terminal Server,

#### 2.4.5 Moduł zarządzania licencjami

Moduł zarządzania licencjami zbudowany został w oparciu o rozwiązanie Matrix42 Service Store firmy Matrix42. Realizuje on następujące usługi:

- 1) inwentaryzacja puli nabytych licencji,
- 2) inwentaryzacja fingerprintów oprogramowania (sygnatur oprogramowania pobranych podczas procesu skanowania) z poszczególnych, objętych monitoringiem serwerów i stacji roboczych,
- 3) monitorowanie balansu licencyjnego pomiędzy nabytymi licencjami a aktualnie zainstalowanym i wykorzystywanym oprogramowaniem,
- 4) utrzymanie katalogu ponad 600 tys. licencji od ponad 5 tys. dostawców oprogramowania dzięki wbudowanemu serwisowi Matrix42 License Intelligence Service (LIS),
- 5) automatyczne raportowanie niedoborów lub nadwyżek licencyjnych dla poszczególnych typów oprogramowania,

#### 2.4.6 Moduł zarządzania zdarzeniami i logami

Moduł zarządzania zdarzeniami i logami zbudowany został w oparciu o rozwiązanie RSA enVision firmy RSA. Realizuje on następujące usługi:

- 1) gromadzenie i archiwizacja wszystkich informacji o zdarzeniach,
- 2) agregacja zgromadzonych danych,
- 3) kategoryzacja danych,
- 4) korelacja danych,
- 5) detekcja i identyfikacja incydentów w oparciu o zdefiniowaną taksonomię incydentów

6) powiadamianie administratorów i operatorów o przypadkach pojawienia się i zaobserwowania nietypowych lub podejrzanych działań,

7) raportowania o zaistniałych incydentach,

8) automatyczne reagowanie na wybrane incydenty (natychmiastowa odpowiedź, zbieranie informacji, uszeregowanie, wdrożenie czynników korygujących itp.),

#### 2.4.7 Moduł raportowania i wizualizacji

Realizuje on następujące usługi:

1) udostępnianie za pośrednictwem interfejsu graficznego informacji o skonsolidowanym stanie serwerów,

2) powiadamianie administratorów i operatorów o przypadkach pojawienia się i zaobserwowania nietypowych lub podejrzanych działań występujących w środowisku teleinformatycznym,

3) udostępnianie, za pośrednictwem interfejsu graficznego, informacji o aktualnych problemach wymagających reakcji administratorów i operatorów,

4) raportowania o zaistniałych incydentach,

#### 2.5 System zarządzania siecią

System zarządzania siecią zbudowany został w oparciu o rozwiązanie NNM firmy HP. Realizuje on następujące usługi:

1) wykrywanie urządzeń w sieci,

2) zbieranie podstawowych danych wydajnościowych urządzeń sieciowych,

3) wyszukiwanie podłączonych urządzeń końcowych do danych węzłów sieciowych,

4) analiza ruchu trapów SNMP w sieci,

5) kolekcje danych SNMP określonego typu (OID),

6) wykonanie zautomatyzowanej diagnostyki urządzeń sieciowych,

7) wprowadzanie zmian w konfiguracji urządzeń sieciowych,

8) wykrywanie nieplanowanych zmian dokonanych w konfiguracji urządzeń,

9) weryfikację poprawności dokonywanych zmian w konfiguracji,

10) identyfikację wersji oprogramowania i konfiguracji urządzeń,

11) wycofywanie wprowadzonych zmian,

12) analizy statystyczne zebranych danych z konkretnych urządzeń obejmujące różne przedziały czasu,

13) przygotowywanie raportów na podstawie analiz statystycznych,

14) przygotowywanie raportów zbiorczych.

#### 2.6 System ServiceDesk

System ServiceDesk zbudowany został w oparciu o rozwiązanie ServiceCenter firmy HP.

Podstawową funkcjonalnością systemu jest zarządzanie procesami wsparcia w oparciu o metodykę ITIL.

System zapewnia obsługę Użytkowników końcowych w zakresie przewidzianym do wdrożenia, obejmującym następujące procesy:

1) Funkcja Serwis Desk

2) Zarządzanie Incydemem

3) Zarządzanie Konfiguracją

4) Zarządzanie Wiedzą

Dodatkowo system posiada możliwość obsługi następujących procesów zgodnie z najnowszą wersją ITIL (v.3) [ale nie implementowanych w ramach tego wdrożenia].

1) Zarządzanie Problemem

2) Zarządzanie Zmianą

3) Zarządzanie Poziomem Usług

4) Zarządzanie Katalogiem Usług

- 5) Zarządzanie Portfelem Usług
  - 2.6.1 Moduł podstawowy
    - 1) Powiadomienia o zdarzeniach
    - 2) Obsługa prac harmonogramowanych
    - 3) Budowa dostosowanych do wymagań szczegółowych Klienta formatek
    - 4) Budowa dostosowanych do wymagań szczegółowych Klienta procesów workflow
    - 5) Generator raportów ekranowych (wraz z predefiniowanymi zestawieniami)
    - 6) Funkcjonalność Single Sign-On
    - 7) Audyt zmian w rekordach danych
    - 8) Klient GUI/WWW
    - 9) Zabezpieczenie haseł i dostępu do systemu oraz danych
  - 2.6.2 Funkcja Service Desk
    - 1) Udostępnienie interfejsu WWW (wraz z dostępem do Bazy Wiedzy)
    - 2) Przyjmowanie zgłoszeń poprzez e-mail
    - 3) Rejestracja i obsługa zgłoszeń
    - 4) Zarządzanie cyklem życia zgłoszeń
    - 5) Zamykanie zgłoszeń
  - 2.6.3 Zarządzanie incydentami
    - 1) Rejestracja incydentów
    - 2) Zarządzanie cyklem życia incydentów
    - 3) Zamykanie incydentów
    - 4) Zarządzanie Grupami Wsparcia
    - 5) Obsługa alertów
  - 2.6.4 Zarządzanie konfiguracją
    - 1) Rejestracja elementów CI
    - 2) Zarządzanie cyklem życia elementów CI
    - 3) Przegląd/aktualizacja danych o elementach CI
    - 4) Likwidacja elementów CI
    - 5) Zarządzanie bazą CMDB
  - 2.6.5 Zarządzanie Wiedzą
    - 1) Pozyskiwanie Wiedzy (zgłoszenia, incydenty)
    - 2) Zatwierdzanie kandydatów do Bazy Wiedzy
    - 3) Wyszukiwanie w Bazie Wiedzy (użytkownik, Serwis Desk)
    - 4) Zarządzanie Bazą Wiedzy
- II.1.6) **Wspólny Słownik Zamówień (CPV)**  
48000000, 48311100, 30216110, 72212000, 72268000, 72253200, 72212211
- II.1.7) **Zamówienie jest objęte Porozumieniem w sprawie zamówień rządowych (GPA)**  
Tak
- II.1.8) **Podział na części**  
Nie
- II.1.9) **Dopuszcza się składanie ofert wariantowych**  
Nie
- II.2) **WIELKOŚĆ LUB ZAKRES ZAMÓWIENIA**
  - II.2.1) **Całkowita wielkość lub zakres**

Bez VAT 7 481 475,00 PLN

II.2.2) **Opcje**

Nie

II.3) **CZAS TRWANIA ZAMÓWIENIA LUB TERMIN REALIZACJI**

Okres w miesiącach: 18 (od udzielenia zamówienia):

**SEKCJA III: INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM**

III.1) **WARUNKI DOTYCZĄCE ZAMÓWIENIA**

III.1.1) **Wymagane wadia i gwarancje**

Wadium w kwocie: 100 000,00 PLN (słownie: sto tysięcy złotych) należy wnieść przed upływem terminu składania ofert.

Zabezpieczenie należytego wykonania umowy wynosić będzie 10 % zaoficerowanej w ofercie ceny całkowitej brutto.

III.1.2) **Główne warunki finansowania i płatności i/lub odniesienie do odpowiednich przepisów je regulujących**

Termin płatności: 14 dni od daty złożenia faktury z protokołem odbioru.

Zamawiający dopuszcza płatności częściowe.

Za datę dokonania płatności uznaje się datę złożenia zlecenia przelewu w banku Zamawiającego.

Umowa realizowana w ramach Programu Operacyjnego Innowacyjna Gospodarka, współfinansowanego ze środków Europejskiego Funduszy Rozwoju Regionalnego 2007–2013.

III.1.3) **Forma prawna, jaką musi przyjąć grupa wykonawców, której zostanie udzielone zamówienie**

Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W tym przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.

III.1.4) **Inne szczególne warunki, którym podlega realizacja zamówienia**

Nie

III.2) **WARUNKI UDZIAŁU**

III.2.1) **Sytuacja podmiotowa wykonawców, w tym wymogi dotyczące wpisu do rejestru zawodowego lub handlowego**

Informacje i formalności konieczne do dokonania oceny spełniania wymogów: A. W zakresie potwierdzenia niepodlegania wykluczeniu na podstawie art. 24 ust. 1 ustawy, należy przedłożyć:

1. oświadczenie o braku podstaw do wykluczenia

2. 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, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert, a w stosunku do osób fizycznych oświadczenie w zakresie art. 24 ust. 1 pkt 2 ustawy

3. aktualne zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzające, że wykonawca nie zalega z opłacaniem podatków lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert

4. aktualne zaświadczenie właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające, że wykonawca nie zalega z opłacaniem składek na ubezpieczenie zdrowotne i społeczne, lub potwierdzenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu -

wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert

5. aktualną informację z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4-8 ustawy, wystawioną nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert

6. aktualną informację z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 ustawy, wystawioną nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert

Wykonawca powołujący się przy wykazywaniu spełnienia warunków udziału w postępowaniu na potencjał innych podmiotów, które będą brały udział w realizacji części zamówienia, przedkłada także dokumenty dotyczące tego podmiotu w zakresie wymaganym dla wykonawcy, określonym w pkt III.2.1)A.

B. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, przedkłada:

B.1. dokument wystawiony w kraju, w którym ma siedzibę lub miejsce zamieszkania potwierdzający, że:

1) nie otwarto jego likwidacji ani nie ogłoszono upadłości - wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert,

2) nie zalega z uiszczaniem podatków, opłat, składek na ubezpieczenie społeczne i zdrowotne albo że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert,

3) nie orzeczono wobec niego zakazu ubiegania się o zamówienie - wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert,

B.2. zaświadczenie właściwego organu sądowego albo administracyjnego miejsca zamieszkania dotyczące niekaralności osób, o których mowa w art. 24 ust.1 pkt 5-8 ustawy, w zakresie określonym w art. 24 ust.1 pkt 5-8 ustawy, wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert – albo oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio miejsca zamieszkania osoby lub kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, jeżeli w miejscu zamieszkania osoby lub kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się takiego zaświadczenia.

### III.2.2) **Zdolność ekonomiczna i finansowa**

Informacje i formalności konieczne do dokonania oceny spełniania wymogów: Dla udokumentowania spełnienia warunku w zakresie zdolności ekonomicznej i finansowej należy przedłożyć dokumenty (oryginały lub kopie poświadczone przez Wykonawcę za zgodność z oryginałem):

a) informację banku lub spółdzielczej kasy oszczędnościowo-kredytowej, w których wykonawca posiada rachunek, potwierdzającą wysokość posiadanych środków finansowych lub zdolność kredytową wykonawcy, wystawioną nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia,

b) opłaconą polisę, a w przypadku jej braku inny dokument potwierdzający, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia.

Wykonawca powołujący się przy wykazywaniu spełnienia warunków udziału w postępowaniu na zdolność finansową innych podmiotów, przedkłada informację banku lub spółdzielczej kasy oszczędnościowo-

kredytowej, dotyczącej podmiotu, z którego zdolności finansowej korzysta na podstawie art. 26 ust. 2b ustawy, potwierdzającą wysokość posiadanych środków finansowych lub zdolność kredytową wykonawcy, wystawioną nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia.

Minimalny poziom ewentualnie wymaganych standardów Wykonawca musi wykazać:

a) posiadanie środków finansowych na rachunku bankowym lub zdolności kredytowej w wysokości nie mniejszej niż 1 000 000,00 PLN.

b) posiadanie opłaconego ubezpieczenia od odpowiedzialności cywilnej w zakresie prowadzonej działalności obejmującej przedmiot zamówienia na wartość nie mniejszą niż 1 000 000,00 PLN;

W przypadku Wykonawców wspólnie ubiegających się o Zamówienie warunki mogą być spełnione łącznie. Zamawiający dokona oceny spełnienia warunków udziału w postępowaniu na zasadzie spełnia/nie spełnia.

### III.2.3) **Zdolność techniczna**

Informacje i formalności konieczne do dokonania oceny spełniania wymogów:

W celu potwierdzenia spełnienia warunków udziału w postępowaniu wykonawcy muszą złożyć wraz z wnioskiem o dopuszczenie do udziału w postępowaniu:

a) wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, usług w zakresie niezbędnym do wykazania spełniania warunku wiedzy i doświadczenia w okresie ostatnich trzech lat przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców, oraz załączenie dokumentu potwierdzającego, że te usługi zostały wykonane lub są wykonywane należycie,

b) wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości, wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnych dla wykonania zamówienia, a także zakresu wykonywanych przez nie czynności, oraz informację o podstawie do dysponowania tymi osobami.

Minimalny poziom ewentualnie wymaganych standardów

W przetargu mogą wziąć udział Wykonawcy, którzy posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia, co oznacza, że:

A. W okresie ostatnich trzech lat przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie:

I. wykonali co najmniej trzy zrealizowane zamówienia systemów informatycznych klasy Portal Intranetowy, o wartości przekraczającej 100 000 PLN brutto za każdą wykonaną usługę, wdrożonych u różnych podmiotów, o charakterze podobnym do przedmiotu zamówienia, tzn. obejmujących zaprojektowanie, implementację i wdrożenie portalu intranetowego o modułowej strukturze, realizującego co najmniej funkcjonalność obsługi urlopów wraz z obsługą zastępstw i obsługi delegacji wraz z rozliczaniem pracowniczych podróży służbowych w organizacji o strukturze rozproszonej, ogólnopolskiej posiadającej co najmniej 5 oddziałów oraz co najmniej 300 użytkowników, w tym:

1. Co najmniej dwa zamówienia opisane w punkcie I dodatkowo obejmowały zaprojektowanie, implementację i wdrożenie rozwiązania intranetowego opartego o platformę Microsoft SharePoint Server wraz z implementacją niestandardowych modułów biznesowych z wykorzystaniem narzędzi programistycznych Microsoft Visual Studio;

2. Co najmniej jedno z zamówień opisanych w punkcie I musi dodatkowo spełniać wszystkie poniższe wymagania:

1) Dotyczy wdrożenia systemu, w którym liczba użytkowników pracujących w lokalizacjach rozproszonych geograficznie jest większa niż 1000;

2) Dotyczy wdrożenia, w którym system został uruchomiony w architekturze wieloserwerowej z wykorzystaniem mechanizmów klastrowania, load balancingu oraz mechanizmów failover;

3) Dotyczy wdrożenia, w ramach którego została wykonana integracja z każdym z wymienionych poniżej systemów zewnętrznych, które funkcjonują u Zamawiającego tj.:

a) Integracja z usługami Active Directory w zakresie autoryzacji i autentykacji użytkowników;

b) Integracja z systemem poczty korporacyjnej;

3. Co najmniej jedno z zamówień opisanych w punkcie I musi dodatkowo spełniać wszystkie poniższe wymagania:

1) Dotyczy wdrożenia systemu w architekturze rozproszonej, w organizacji, która posiada co najmniej 10 oddziałów terenowych;

2) Dotyczy wdrożenia systemu, który na poziomie administracyjnym posiada możliwość dostosowania funkcjonalności do potrzeb poszczególnych oddziałów oraz zapewnia możliwość delegowania funkcji zarządzania zawartością i funkcjami portalu dla przedstawicieli różnych oddziałów;

3) Dotyczy wdrożenia systemu dostosowanego w warstwie graficznej do wytycznych identyfikacji wizualnej firmy;

4) Dotyczy wdrożenia, w ramach którego została wykonana integracja z każdym z wymienionych poniżej systemów zewnętrznych, które funkcjonują u Zamawiającego tj.:

a) Integracja z usługami Active Directory w zakresie autoryzacji i autentykacji użytkowników;

b) Integracja z systemem poczty korporacyjnej; oraz

II. Jedno zamówienie zrealizowane w administracji publicznej polegające na wdrożeniu elektronicznego systemu zarządzania dokumentami (EZD) w rozumieniu rozporządzenia Prezesa Rady Ministrów z dnia 18.1.2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14 poz. 67). Wdrożony system musi posiadać możliwość podpisywania dokumentów podpisem elektronicznym oraz weryfikacji podpisu w rozumieniu ustawy z dnia 18.9.2001 r. o podpisie elektronicznym (Dz. U. Nr 130 poz. 1450, z późn. zm), a także zapewniać integrację z platformą ePUAP. oraz

III. Trzy zrealizowane zamówienia systemów informatycznych klasy Elektroniczny Obieg Dokumentów (wraz z instalacją i wdrożeniem) o wartości przekraczającej 500 000 PLN brutto za każdą wykonaną usługę, wdrożonych w architekturze zapewniającej wysoką dostępność oraz obsługujących korespondencję przychodzącą, wewnętrzną i wychodzącą realizowaną zgodnie z instrukcją kancelaryjną opartą o wykaz akt, w tym:

1. Co najmniej dwa z zamówień opisanych w punkcie III muszą dodatkowo spełniać wszystkie poniższe wymagania:

1) Dotyczy wdrożenia systemu zrealizowanego w sieci WAN lub Internet dla co najmniej 500 użytkowników w rozproszonych lokalizacjach;

2) Dotyczy wdrożenia systemu zrealizowanego dla co najmniej 10 lokalizacji;

3) Dotyczy wdrożenia systemu zapewniającego możliwość składania i weryfikowania podpisu elektronicznego;

4) Dotyczy wdrożenia systemu obsługującego min. 5 dedykowanych procesów obiegu dokumentów Zamawiającego;

5) Dotyczy wdrożenia systemu zrealizowanego z wykorzystaniem technologii (łącznie):

a) Microsoft Windows 2003 Server bądź nowszy;

b) Microsoft SQL Server 2005 bądź nowszy;

c) Microsoft SharePoint 2007 lub nowszy;

d) Microsoft .NET Framework;

e) Microsoft Active Directory;

f) Microsoft Exchange 2007 lub nowszy.

2. Co najmniej jedno z zamówień opisanych w punkcie III musi dotyczyć wdrożenia systemu, którego elementem była spełniająca wszystkie wymogi prawne Elektroniczna Skrzynka Podawcza zintegrowana z wdrożonym Elektronicznym Obiegiem Dokumentów. oraz

IV. Jedno zamówienie zrealizowane w administracji publicznej polegające na budowie i wdrożeniu systemu umożliwiającego w sieci Internet wypełnienie, podpisanie z użyciem kwalifikowanego podpisu elektronicznego i złożenie formularzy elektronicznych, przy czym zamówienie musi spełniać wszystkie poniższe wymagania:

1. Dotyczy wdrożenia systemu wykorzystującego słowniki adresowe krajowego rejestru podziału terytorialnego kraju (TERYT);

2. Dotyczy wdrożenia systemu udostępniającego usługi Web Service dla potrzeb integracji z innymi systemami, z mechanizmami WS Security;

3. Dotyczy wdrożenia systemu umożliwiającego przechowywanie dokumentów opatrzonego kwalifikowanym podpisem elektronicznym wraz z zachowaniem ich wartości dowodowej (pielęgnacja podpisu);

4. Dotyczy wdrożenia systemu zawierającego w sobie wszystkie wymagane prawnie mechanizmy Elektronicznej Skrzynki Podawczej;

5. Dotyczy wdrożenia systemu umożliwiającego wygenerowanie dokumentu w formie elektronicznej; oraz

V. Dwa zrealizowane zamówienia na bazodanowy system informatyczny, o wartości przekraczającej 500 000 PLN brutto za każdą wykonaną usługę, przy czym zamówienia muszą spełniać wszystkie poniższe wymagania:

1. Zamówienia polegały na budowie systemów bazodanowych masowego gromadzenia i przetwarzania danych z wieloma punktami wprowadzania danych na terenie Polski w zakresie funkcjonalnym, w przypadku każdego z systemów dla minimum 100 nazwanych użytkowników wewnętrznych pracujących jednocześnie;

2. Zamówienia polegały na zaprojektowaniu i budowie systemów internetowych pozwalających na dostęp do danych zawartych w systemach bazodanowych, w przypadku każdego z systemów dla minimum 100 anonimowych użytkowników zewnętrznych pracujących jednocześnie;

3. Zamówienia polegały na integracji każdego z systemów bazodanowych z systemami elektronicznego obiegu dokumentów w celu obsługi i przetwarzania dla potrzeb systemów bazodanowych dokumentów elektronicznych w formacie xml. oraz

VI. Dwa zrealizowane zamówienia na systemy informatyczne klasy Broker Integracyjny (szyna ESB), o wartości przekraczającej 500 000 PLN brutto za każdą wykonaną usługę o charakterze podobnym do przedmiotu zamówienia, tzn. zrealizowane w sieci WAN lub Internet obsługujące transakcje od co najmniej 500 użytkowników (osób, organizacji, agencji etc.), w minimum 10 lokalizacjach każdy, w architekturze zapewniającej wysoką dostępność, z wykorzystaniem technologii (łącznie):

a) Microsoft Windows 2003 Server bądź nowszy;

b) BizTalk Server 2006 lub nowszy;

c) Microsoft SQL Server 2005 bądź nowszy;

d) Microsoft .NET Framework;

e) Windows Communication Foundation;

1. Wdrożenie co najmniej jednego z systemów opisanych w punkcie VI odbywało się z wykorzystaniem Team Foundation Server lub równoważnego, jako narzędzia do zarządzania cyklem życia aplikacji i automatycznych testów i automatycznego budowania aplikacji;

2. W co najmniej jednym systemie opisanym w punkcie VI liczba testów automatycznych wynosiła powyżej 90 %;

3. Co najmniej jeden system opisany w punkcie VI umożliwiał przyjęcie powyżej 15 000 000 dokumentów (komunikatów) w ciągu roku. oraz

VII. Co najmniej jedno zamówienie polegające na budowie systemu informatycznego zapewniającego bezpieczeństwo elektronicznej wymianie dokumentów w oparciu o infrastrukturę PKI, obsługującego rejestr publiczny o wartości przekraczającej 250 000 PLN brutto za wykonaną usługę. oraz

VIII. Co najmniej jedno zamówienie polegające na budowie systemu informatycznego, którego elementem było wykonanie projektu technicznego łącznie z wykonaniem polityki bezpieczeństwa i wykonaniem infrastruktury PKI, w tym dostarczenie narzędzi do weryfikacji certyfikatów PKI zgodnych ze standardem X.509 v3 i podpisów elektronicznych XaDES o wartości przekraczającej 250 000 PLN brutto za wykonaną usługę.

B. Dysponują następującymi osobami zdolnymi do wykonania zamówienia i spełniającymi niżej wymienione warunki, przy czym dopuszcza się pełnienie jednocześnie dwóch różnych ról przez jedną osobę:

I. Kierownik Projektu – osoba, która posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
- 2) kwalifikacje z zakresu zarządzania projektami potwierdzone posiadaniem jednego ze wskazanych certyfikatów: „PRINCE2 Practitioner” lub IPMAmin. Level „C” lub Project Management Professional (PMP) (patrz przypis 2),
- 3) minimum 10 letnie doświadczenie zawodowe, w tym co najmniej 5 lat doświadczenia w pełnieniu funkcji Kierownika projektów informatycznych,
- 4) udział w roli Kierownika projektu w co najmniej 2 projektach o wartości minimum 1 000 000 PLN brutto za każdą wykonaną usługę,
- 5) poświadczenie bezpieczeństwa osobowego upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą co najmniej „poufne”,
- 6) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną,

II. Zespół Architektów Systemów i Bezpieczeństwa – co najmniej 2 osoby, z których:

1. każda posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
- 2) udział, w okresie ostatnich 5 lat, w roli architekta w obszarze informatycznej infrastruktury technicznej lub oprogramowania, w minimum 2 projektach o wartości zamówienia na kwotę co najmniej 1 000 000 PLN brutto każdy,
- 3) kwalifikacje z zakresu zarządzania projektami potwierdzone posiadaniem jednego ze wskazanych certyfikatów: „PRINCE2 Practitioner” lub IPMAmin. Level „C” lub Project Management Professional (PMP) (patrz przypis 2),
- 4) znajomość zasad architektury korporacyjnej potwierdzoną co najmniej certyfikatem TOGAF 8 Certified lub TOGAF 9 na poziomie „Foundation”, lub IT Architect Open Group, wydanym przez instytucję akredytowaną przez The Open Group, lub certyfikatem IBM Certified Infrastructure Systems Architect (patrz przypis 2),
- 5) kwalifikacje eksperckie z zakresu bezpieczeństwa informacji potwierdzone posiadaniem certyfikatu CISA: Certified Information System Auditor (<http://www.isaca.org>) lub certyfikatu CISSP: Certified Information System Security Professional (<http://www.isc2.org>) (patrz przypis 2),
- 6) uprawnienia audytora systemu zarządzania usługami IT według normy ISO20000 wydane przez akredytowaną instytucję, lub certyfikat ITIL Foundation in IT Service Management wydany przez APMG lub instytucję przez niego akredytowaną (patrz przypis 2),
- 7) poświadczenie bezpieczeństwa osobowego upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą co najmniej „poufne”,
- 8) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną,

2. dla Zespołu wymagane są następujące kwalifikacje i certyfikaty techniczne:

- 1) certyfikat dokumentujący znajomość przynajmniej jednego systemu operacyjnego na poziomie administracyjnym, wydany przez producenta oprogramowania systemu operacyjnego lub akredytowaną przez niego instytucję (patrz przypis 1),
- 2) certyfikat dokumentujący znajomość przynajmniej jednego systemu zarządzania bazą danych na poziomie administracyjnym, wydany przez producenta oprogramowania systemu zarządzania bazą danych lub akredytowaną przez niego instytucję (patrz przypis 1),
- 3) certyfikat dokumentujący znajomość przynajmniej jednego systemu zarządzania infrastrukturą IT na poziomie administracyjnym, wydany przez producenta oprogramowania systemu zarządzania infrastrukturą IT lub akredytowaną przez niego instytucję (patrz przypis 1),
- 4) kwalifikacje eksperckie z zakresu prowadzenie testów penetracyjnych potwierdzone posiadaniem certyfikatu CEH: Certified Ethical Hacker (<http://www.eccouncil.org>) lub certyfikatu GIAC Certified Penetration Tester (<http://www.giac.org>) (patrz przypis 2),
- 5) uprawnienia audytora systemu zarządzania bezpieczeństwem informacji według normy bezpieczeństwa ISO27001 lub ISO17799 lub BS7799, wydane przez akredytowaną instytucję (patrz przypis 2),
- 6) uprawnienia audytora systemu zarządzania ciągłością działania według normy BS25999 wydane przez akredytowaną instytucję, lub certyfikat Associate Business Continuity Professional (ABCP), wydany przez DRII lub instytucję przez niego akredytowaną (patrz przypis 2).

III. Zespół Analityków Systemów Integracyjnych – co najmniej 2 osoby, przy czym:

1. każda z tych osób posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
- 2) udział, w okresie ostatnich 5 lat, w roli analityka lub projektanta w co najmniej 2 projektach o wartości zamówienia na kwotę co najmniej 1 000 000 PLN brutto każdy, w obszarze informatycznej infrastruktury technicznej i oprogramowania,
- 3) certyfikat dokumentujący znajomość architektury systemów SOA; certyfikat powinien być wydany przez producenta oprogramowania służącego do integracji systemów IT zgodnego z SOA,
- 4) poświadczenie bezpieczeństwa osobowego upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą co najmniej „poufne”,
- 5) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną

2. dla Zespołu wymagane są następujące kwalifikacje i certyfikaty techniczne:

- 1) kwalifikacje w dziedzinie zarządzania projektami potwierdzone certyfikatem: PRINCE2 co najmniej na poziomie „Foundation”, wydanym przez APMG lub instytucję przez niego akredytowaną, lub certyfikatem co najmniej na poziomie Certified Associate In Project Management (CAPM), wydanym przez PMI lub instytucję przez niego akredytowaną (patrz przypis 2),
- 2) kwalifikacje eksperckie z zakresu bezpieczeństwa informacji potwierdzone posiadaniem, certyfikatu CISA: Certified Information System Auditor (<http://www.isaca.org>) lub certyfikatu CISSP: Certified Information System Security Professional (<http://www.isc2.org>) (patrz przypis 2),
- 3) certyfikat dokumentujący znajomość przynajmniej jednego systemu operacyjnego na poziomie administracyjnym, wydany przez producenta oprogramowania systemu operacyjnego lub akredytowaną przez niego instytucję (patrz przypis 1),
- 4) certyfikat dokumentujący znajomość przynajmniej jednego systemu zarządzania bazą danych na poziomie administracyjnym, wydany przez producenta oprogramowania systemu zarządzania bazą danych lub akredytowaną przez niego instytucję (patrz przypis 1).

IV. Zespół Analityków Aplikacyjnych – co najmniej 4 osoby, przy czym:

1. każda z tych osób posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
  - 2) minimum 2-letnie doświadczenie zawodowe w zakresie analizy biznesowej i systemowej;
  - 3) udział w ciągu ostatnich 2 lat, co najmniej w 2 projektach, gdzie zajmowała się modelowaniem procesów biznesowych z zastosowaniem języka UML 2.0,
  - 4) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną.
2. dla Zespołu wymagane są następujące kwalifikacje i certyfikaty techniczne:
- 1) przynajmniej 2 osoby brały udział w ciągu ostatnich 3 lat w minimum dwóch projektach informatycznych dotyczących wdrożenia systemu klasy workflow,
  - 2) przynajmniej 2 osoby mają doświadczenie w roli analityka wiodącego (lub równoważnej roli) w realizacji minimum jednego projektu informatycznego,
  - 3) przynajmniej 2 osoby mają co najmniej 2-letnie doświadczenie w projektowaniu systemów wykorzystujących Internet, dokument elektroniczny i podpis elektroniczny,
  - 4) przynajmniej 2 osoby mają co najmniej 2-letnie doświadczenie w analizie i projektowaniu systemów bazodanowych, komunikacji przez usługi sieciowe oraz w integracji systemów, w tym systemów bazodanowych z systemami elektronicznego obiegu dokumentów.
- V. Zespół Ekspertów ds. wdrożenia i utrzymania – co najmniej 2 osoby, z których każda posiada:
- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
  - 2) doświadczenie w zakresie wdrażania systemów informatycznych (w ciągu 3 ostatnich lat odpowiadał za przeprowadzenie zakończonego sukcesem wdrożenia w którym liczba użytkowników końcowych przekracza 1000 osób),
  - 3) doświadczenie w zakresie projektowania i wdrażania systemów zapewnienia ciągłości funkcjonowania (synchronizowanie i przełączanie ośrodków przetwarzania, systemy backupu, systemy do odtwarzania po awarii, rozwiązania o wysokiej niezawodności i dostępności),
  - 4) doświadczenie w projektowaniu utrzymania dla systemów informatycznych, projektowaniu procesów utrzymaniowych, ról i odpowiedzialności,
  - 5) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną.
- VI. Lider zespołu programistów: osoba, która posiada:
- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
  - 2) znajomość metodyki prowadzenia projektów SCRUM potwierdzoną posiadaniem certyfikatu Certified SCRUM Master (patrz przypis 2),
  - 3) co najmniej 5-letnie doświadczenie w zakresie budowy i wdrażania dedykowanych systemów informatycznych z wykorzystaniem Microsoft Visual Studio,
  - 4) udział w minimum trzech projektach programistycznych, z wykorzystaniem technologii Microsoft Team Foundation Server w tym przynajmniej jeden, jako lider zespołu programistów,
  - 5) udział w minimum jednym projekcie o wartości usług 1 000 000 PLN obejmującym swym zasięgiem ponad 1000 użytkowników w minimum 10 lokalizacjach, którego przedmiotem było zaprojektowanie, stworzenie i wdrożenie dedykowanego projektu opartego o technologie Windows .Net i WCF,
  - 6) certyfikat techniczny dokumentujący znajomość technologii Microsoft Office SharePoint Server 2007 lub nowszy na poziomie administracyjnym, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),
  - 7) certyfikat techniczny dokumentujący znajomość technologii Microsoft Windows SharePoint Services 3.0 na poziomie administracyjnym, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),

8) certyfikat techniczny dokumentujący znajomość technologii .NET Framework, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),

9) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną.

VII. Zespół Specjalistów ds. zapewnienia jakości – co najmniej 2 osoby przy czym:

1. każda osoba posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
- 2) kwalifikacje eksperckie z zakresu bezpieczeństwa informacji potwierdzone posiadaniem certyfikatu CISA: Certified Information System Auditor (<http://www.isaca.org>) lub certyfikatu CISSP: Certified Information System Security Professional (<http://www.isc2.org>) (patrz przypis 2),
- 3) kwalifikacje eksperckie w zakresie identyfikacji ryzyk i zarządzania nimi poprzez opracowywanie, wdrażanie i utrzymywanie mechanizmów kontrolnych w systemach informatycznych potwierdzone posiadaniem certyfikatu Certified in Risk and Information Systems Control (ISACA CRISC <http://www.isc2.org>) (patrz przypis 2),
- 4) co najmniej 5-letnie doświadczenie w zakresie projektowania i wdrożeń systemów informatycznych w tym w ciągu ostatnich trzech lat brała udział w przynajmniej trzech projektach o wartości przekraczającej 500 000 PLN brutto za każdą wykonaną usługę,
- 5) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną.

2. dla Zespołu wymagane są następujące kwalifikacje i certyfikaty techniczne:

- 1) znajomość technologii Microsoft udokumentowana posiadaniem jednego z następujących certyfikatów technicznych: Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Systems Administrator (MCSA), Microsoft Certified Technology Specialist (MCTS) (patrz przypis 1),
- 2) uprawnienia audytora systemu zarządzania usługami IT według normy ISO20000 wydane przez akredytowaną instytucję, lub certyfikat ITIL Foundation in IT Service Management wydany przez APMG lub instytucję przez niego akredytowaną (patrz przypis 2),
- 3) kwalifikacje eksperckie z zakresu prowadzenie testów penetracyjnych potwierdzone posiadaniem certyfikatu CEH: Certified Ethical Hacker (<http://www.eccouncil.org>) lub certyfikatu GIAC Certified Penetration Tester (<http://www.giac.org>) (patrz przypis 2),
- 4) uprawnienia audytora systemu zarządzania bezpieczeństwem informacji według normy bezpieczeństwa ISO27001 lub ISO17799 lub BS7799, wydane przez akredytowaną instytucję (patrz przypis 2),
- 5) uprawnienia audytora systemu zarządzania ciągłością działania według normy BS25999 wydane przez akredytowaną instytucję, lub certyfikat Associate Business Continuity Professional (ABCP), wydany przez DRII lub instytucję przez niego akredytowaną (patrz przypis 2),

VIII. Zespół Ekspertów ds. wytwarzania oprogramowania – co najmniej 6 osób, przy czym:

1. każda osoba posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
- 2) udział w projekcie o wartości brutto dostarczonych usług przekraczającej 500 000 PLN,
- 3) certyfikat Microsoft Certified Professional Developer (patrz przypis 1),
- 4) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną.

2. dla Zespołu wymagane są następujące kwalifikacje i certyfikaty techniczne:

- 1) przynajmniej 2 osoby posiadają znajomość technologii Microsoft udokumentowaną posiadaniem jednego z następujących certyfikatów technicznych: Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Systems Administrator (MCSA), Microsoft Certified Technology Specialist (MCTS) (patrz przypis 1),

- 2) przynajmniej 2 osoby posiadają certyfikat techniczny dokumentujący znajomość technologii Microsoft Office SharePoint Server 2007 lub nowszy na poziomie administracyjnym, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),
- 3) przynajmniej 2 osoby posiadają certyfikat techniczny dokumentujący znajomość technologii Microsoft Windows SharePoint Services 3.0 na poziomie administracyjnym, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),
- 4) przynajmniej 2 osoby posiadają certyfikat techniczny dokumentujący znajomość systemu Microsoft SQL Server 2005 lub nowszy na poziomie administracyjnym, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),
- 5) przynajmniej 2 osoby posiadają certyfikat techniczny dokumentujący znajomość systemu BizTalk Server 2006 lub nowszy na poziomie administracyjnym, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),
- 6) przynajmniej 2 osoby posiadają znajomość metodyki prowadzenia projektów SCRUM potwierdzona posiadaniem certyfikatu Certified SCRUM Master (patrz przypis 2).

IX. Projektant Integracji Systemów Dedykowanych – osoba, która posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
- 2) kwalifikacje w zakresie integracji oprogramowania, w co najmniej dwóch różnych technologiach integracyjnych;
- 3) co najmniej 5-letnie doświadczenie w zakresie budowy i wdrożenia dedykowanych systemów informatycznych,
- 4) udział w minimum trzech projektach informatycznych, których przedmiotem było zaprojektowanie, budowa i wdrożenie dedykowanego systemu o wartości dostarczonych usług minimum 500 000 PLN brutto każdy,
- 5) udział w minimum jednym projekcie o wartości dostarczonych usług 1 000 000 PLN dotyczącym integracji systemów rozproszonych, którego przedmiotem było zaprojektowanie, stworzenie i wdrożenie dedykowanego projektu opartego o technologie Windows .Net i WCF,
- 6) doświadczenie w realizacji co najmniej 1 projektu dot. Platformy Integracji z wykorzystaniem środowiska Microsoft BizTalk Server 2006 lub nowszym oraz Microsoft Visual Studio ALM 2010 w zakresie zarządzania cyklem życia aplikacji i wykonywania testów wydajnościowych i funkcjonalnych w Visual Studio 2010, pracę z Microsoft Test Manager, Microsoft Visual Studio 2010 Test Agents, w instytucji zatrudniającej co najmniej 1000 osób.
- 7) certyfikat Microsoft Certified Professional Developer (patrz przypis 1),
- 8) certyfikat techniczny dokumentujący znajomość technologii .NET Framework 2.0, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),
- 9) certyfikat techniczny dokumentujący znajomość systemu BizTalk Server 2006 lub nowszy na poziomie administracyjnym, wydany przez producenta oprogramowania lub akredytowaną przez niego instytucję (patrz przypis 1),
- 10) znajomość metodyki prowadzenia projektów SCRUM potwierdzona posiadaniem certyfikatu Certified SCRUM Master (patrz przypis 2)
- 11) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną.

X. Zespół Instruktorów – co najmniej 2 osoby, z których każda posiada:

- 1) wyższe wykształcenie techniczne lub z zakresu nauk ścisłych,
- 2) co najmniej 3 letnie doświadczenie w prowadzeniu szkoleń informatycznych w tym zagadnień PKI, co może udokumentować przeprowadzeniem, co najmniej 3 szkoleń przez każdego z instruktorów.

3) biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną.

Przypis 1 - Zamawiający dopuszcza wykazanie posiadania innych certyfikatów niż wymagane pod warunkiem, że potwierdzają one posiadanie co najmniej tej samej wiedzy co wymagane przez Zamawiającego i są wydane przez instytucję akredytowaną przez producenta danego oprogramowania/sprzętu.

Przypis 2 - Zamawiający dopuszcza wykazanie posiadania innych certyfikatów niż wymagane. W takim przypadku Wykonawca jest zobowiązany do wykazania, że:

1. certyfikat potwierdza posiadanie co najmniej tej samej wiedzy i doświadczenia co certyfikat wskazany przez Zamawiającego;
2. proces certyfikacyjny dla certyfikatu innego niż wskazany przez Zamawiającego został przeprowadzony przez jednostkę wskazaną przez Zamawiającego w wymaganiach lub inną jednostkę akredytowaną, zgodnie z normą PN-EN ISO/IEC 17024:2004 „Ocena zgodności. Ogólne wymagania dotyczące jednostek certyfikujących osoby” oraz Dokumentem interpretacyjnym IAF (International Accreditation Forum, Inc., IAF) „Wytyczne IAF do stosowania ISO/IEC 17024:2004 (idt. z PN-EN ISO/IEC 17024:2003)”, Wydanie 1 (IAF GD 24:2004).

Uwaga:

W przypadku, gdy Wykonawcą jest podmiot, który powstał w wyniku połączenia, Zamawiający uzna spełnienie określonych warunków, jeżeli zostanie wykazane wykonanie zamówień w wymaganym czasie, przez co najmniej jeden z połączonych podmiotów.

W przypadku składania oferty przez podmioty występujące wspólnie, wyżej wymieniony warunek musi spełniać, co najmniej 1 podmiot albo podmioty mogą spełniać go łącznie.

Wykonawca, który realizował zamówienia obejmujące zakres szerszy niż przedmiot zamówienia określony w wymaganiach, winien podać tylko wartość części zamówienia odpowiadającej przedmiotowi zamówienia.

W przypadku Wykonawców, którzy realizowali usługi/zamówienia za wynagrodzeniem wyrażonym w innych walutach niż złoty polski, Zamawiający przeliczy wartość tych usług/zamówień po średnim kursie NBP z dnia ukazania się ogłoszenia o zamówieniu.

#### III.2.4) **Zamówienia zastrzeżone**

Nie

#### III.3) **SPECYFICZNE WARUNKI DOTYCZĄCE ZAMÓWIEŃ NA USŁUGI**

##### III.3.1) **Świadczenie usługi zastrzeżone jest dla określonego zawodu**

Nie

##### III.3.2) **Osoby prawne powinny wskazać nazwiska oraz kwalifikacje zawodowe osób odpowiedzialnych za wykonanie usługi**

Nie

#### **SEKCJA IV: PROCEDURA**

##### IV.1) **RODZAJ PROCEDURY**

###### IV.1.1) **Rodzaj procedury**

Ograniczona

###### IV.1.2) **Ograniczenie liczby wykonawców, którzy zostaną zaproszeni do składania ofert lub do udziału**

Przewidywana liczba wykonawców 5

Obiektywne kryteria wyboru ograniczonej liczby kandydatów: Kryteria oceny pierwszego etapu: Jeżeli liczba Wykonawców, którzy spełniają warunki udziału w postępowaniu będzie mniejsza bądź równa 5, do złożenia ofert zostaną zaproszeni wszyscy Wykonawcy spełniający te warunki. Jeżeli liczba Wykonawców, którzy spełniają warunki udziału w postępowaniu będzie większa niż 5, zamawiający zaprosi do składania ofert 5 Wykonawców, którzy otrzymali najwyższe oceny spełniania warunku udziału w postępowaniu w zakresie

doświadczenia zawodowego. Ocena spełniania warunku udziału w postępowaniu będzie dokonywana na podstawie następującego kryterium: Ocena spełniania warunku zostanie dokonana na podstawie "Wykazu zrealizowanych zamówień" w następujący sposób: Wykonawca, który wykaże w "Wykazie zrealizowanych zamówień" większą niż minimalna wymagana do wzięcia udziału w przetargu liczbę zrealizowanych zamówień spełniających określone warunki uzyska punkty, na podstawie których ustalona zostanie kolejność Wykonawców. Punkty będą przyznawane za większą niż minimalna wymagana do wzięcia udziału w przetargu liczbę zrealizowanych zamówień, czyli liczone do punktacji będą te zamówienia, które nie zostały wzięte pod uwagę przy kwalifikowaniu Wykonawcy jako spełniającego wymagania do wzięcia udziału w przetargu. Punkty zostaną przyznane za każde wykazane ponad minimum zamówienie, o którym mowa w ogłoszeniu w punkcie III.2.3) Zdolność techniczna w punktach: A.I.1., tj. za każde ponad minimum dwa zrealizowane zamówienia systemów informatycznych klasy Portal Intranetowy, o wartości przekraczającej 100 000 PLN brutto za każdą wykonaną usługę, wdrożone u różnych podmiotów, o charakterze podobnym do przedmiotu zamówienia, tzn. obejmujących zaprojektowanie, implementację i wdrożenie portalu intranetowego o modułowej strukturze, realizującego co najmniej funkcjonalność obsługi urlopów wraz z obsługą zastępstw i obsługi delegacji wraz z rozliczaniem pracowniczych podróży służbowych w organizacji o strukturze rozproszonej, ogólnopolskiej posiadającej co najmniej 5 oddziałów oraz co najmniej 300 użytkowników i dodatkowo obejmujących zaprojektowanie, implementację i wdrożenie rozwiązania intranetowego opartego o platformę Microsoft SharePoint Server wraz z implementacją niestandardowych modułów biznesowych z wykorzystaniem narzędzi programistycznych Microsoft Visual Studio; A.III.1., tj. za każde ponad minimum dwa zrealizowane zamówienia systemów informatycznych klasy Elektroniczny Obieg Dokumentów (wraz z instalacją i wdrożeniem) o wartości przekraczającej 500 000 PLN brutto za każdą wykonaną usługę, wdrożonych w architekturze zapewniającej wysoką dostępność oraz obsługujących korespondencję przychodzącą, wewnętrzną i wychodzącą realizowaną zgodnie z instrukcją kancelaryjną opartą o wykaz akt oraz spełniających wszystkie poniższe wymagania: 1) Dotyczy wdrożenia systemu zrealizowanego w sieci WAN lub Internet dla co najmniej 500 użytkowników w rozproszonych lokalizacjach; 2) Dotyczy wdrożenia systemu zrealizowanego dla co najmniej 10 lokalizacji; 3) Dotyczy wdrożenia systemu zapewniającego możliwość składania i weryfikowania podpisu elektronicznego; 4) Dotyczy wdrożenia systemu obsługującego min. 5 dedykowanych procesów obiegu dokumentów Zamawiającego (z wyłączeniem procesów obiegu standardowych pism); 5) Dotyczy wdrożenia systemu zrealizowanego z wykorzystaniem technologii (łącznie): a) Microsoft Windows 2003 Server bądź nowszy; b) Microsoft SQL Server 2005 bądź nowszy; c) Microsoft SharePoint 2007 lub nowszy; d) Microsoft .NET Framework; e) Microsoft Active Directory; f) Microsoft Exchange 2007 lub nowszy. A.V., tj. za każde ponad minimum dwa zrealizowane zamówienia na bazodanowy system informatyczny, o wartości przekraczającej 500 000 PLN brutto za każdą wykonaną usługę, przy czym zamówienia muszą spełniać wszystkie poniższe wymagania: 1) Zamówienia polegały na budowie systemów bazodanowych masowego gromadzenia i przetwarzania danych z wieloma punktami wprowadzania danych na terenie Polski w zakresie funkcjonalnym, w przypadku każdego z systemów dla minimum 100 nazwanych użytkowników wewnętrznych pracujących jednocześnie; 2) Zamówienia polegały na zaprojektowaniu i budowie systemów internetowych pozwalających na dostęp do danych zawartych w systemach bazodanowych, w przypadku każdego z systemów dla minimum 100 anonimowych użytkowników zewnętrznych pracujących jednocześnie; 3) Zamówienia polegały na integracji każdego z systemów bazodanowych z systemami elektronicznego obiegu dokumentów w celu obsługi i przetwarzania dla potrzeb systemów bazodanowych dokumentów elektronicznych w formacie xml. A.VI., tj. za każde ponad minimum dwa zrealizowane zamówienia na systemy informatyczne klasy Broker Integracyjny (szyna ESB), o wartości przekraczającej 500 000 PLN brutto za każdą wykonaną usługę o charakterze podobnym do przedmiotu zamówienia, tzn. zrealizowane w sieci WAN lub Internet obsługujące transakcje od co najmniej 500 użytkowników (osób, organizacji, agencji etc.), w minimum 10 lokalizacjach każde w

architekturze zapewniającej wysoką dostępność, z wykorzystaniem technologii (łącznie): a) Microsoft Windows 2003 Server bądź nowszy; b) BizTalk Server 2006 lub nowszy; c) Microsoft SQL Server 2005 bądź nowszy; d) Microsoft .NET Framework; e) Windows Communication Foundation; A.VIII., tj. za każde ponad minimum jedno zamówienie polegające na budowie systemu informatycznego, którego elementem było wykonanie projektu technicznego łącznie z wykonaniem polityki bezpieczeństwa i wykonaniem infrastruktury PKI, w tym dostarczenie narzędzi do weryfikacji certyfikatów PKI zgodnych ze standardem X.509 v3 i podpisów elektronicznych XaDES o wartości przekraczającej 250 000 PLN brutto za wykonaną usługę. W zależności od ilości zamówień wykazanych ponad minimum, oddzielnie dla każdej z części wykazu, wymienionych w punktach A.I.1., A.III.1., A.V., A.VI. oraz A.VIII., zostaną przyznane punkty wg następującej zasady: 1) za 1-2 zamówienia (ponad minimalną wymaganą ilość) – 1 pkt, 2) za 3-5 zamówień – 5 pkt, 3) za 6-15 zamówień – 10 pkt, 4) za więcej niż 15 zamówień – 15 pkt. Suma punktów uzyskanych z poszczególnych zadań zadecyduje o ustaleniu kolejności Wykonawców (począwszy od Wykonawcy z największą ilością punktów). Jeżeli dwóch lub więcej Wykonawców otrzyma tą samą liczbę punktów, o kolejności Wykonawców decydować będzie większa liczba punktów uzyskanych z pkt. A.III.1. (Elektroniczny Obieg Dokumentów). Jeżeli nadal dwóch lub więcej Wykonawców otrzyma tą samą liczbę punktów o kolejności Wykonawców decydować będzie sumaryczna wartość (kwota brutto) wykonanych, udokumentowanych zrealizowanych zamówień wymienionych w punktach A.I.1., A.III.1., A.V., A.VI. oraz A.VIII., a jeśli nadal nie będzie można ograniczyć ilości. Wykonawców do 5, to Zamawiający zaprosi do składania ofert wszystkich, którzy zajęli sporne ostatnie miejsce w klasyfikacji.

IV.1.3) **Zmniejszenie liczby wykonawców podczas negocjacji lub dialogu**

IV.2) **KRYTERIA UDZIELENIA ZAMÓWIENIA**

IV.2.1) **Kryteria udzielenia zamówienia**

Oferta najkorzystniejsza ekonomicznie z uwzględnieniem kryteriów kryteria określone poniżej

1. Cena oferty. Waga 70

2. Jakość. Waga 30

IV.2.2) **Wykorzystana będzie aukcja elektroniczna**

Nie

IV.3) **INFORMACJE ADMINISTRACYJNE**

IV.3.1) **Numer referencyjny nadany sprawie przez instytucję zamawiającą**  
63/SISP/PO/2011

IV.3.2) **Poprzednie publikacje dotyczące tego samego zamówienia**

Nie

IV.3.3) **Warunki uzyskania specyfikacji i dokumentów dodatkowych**

Termin składania wniosków dotyczących uzyskania dokumentów lub dostępu do dokumentów 9.9.2011 - 11:00

Dokumenty odpłatne Nie

IV.3.4) **Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu**

9.9.2011 - 11:00

IV.3.5) **Data wysłania zaproszeń do składania ofert lub do udziału zakwalifikowanym kandydatom**

IV.3.6) **Język(i), w których można sporządzać oferty lub wnioski o dopuszczenie do udziału w postępowaniu**  
polski.

IV.3.7) **Minimalny okres, w którym oferent będzie związany ofertą**

IV.3.8) **Warunki otwarcia ofert**

**SEKCJA VI: INFORMACJE UZUPEŁNIAJĄCE**

VI.1) **JEST TO ZAMÓWIENIE O CHARAKTERZE POWTARZAJĄCYM SIĘ**

Nie

VI.2) **ZAMÓWIENIE DOTYCZY PROJEKTU/PROGRAMU FINANSOWANEGO ZE ŚRODKÓW WSPÓLNOTOWYCH**

Tak

odniesienie do projektów i/lub programów: Niniejsze postępowanie prowadzone jest w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007–2013 (POIG), VII osi priorytetowej „Społeczeństwo informacyjne– Budowa elektronicznej administracji”, współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego, przyznanych Polsce decyzją Komisji Europejskiej z dnia 2.10.2007 r., ze środków przewidzianych w budżecie projektu System Informacyjny Statystyki Publicznej (SISP) na lata 2008–2013.

VI.3) **INFORMACJE DODATKOWE**

Wykonawca obowiązany jest złożyć oświadczenie o spełnieniu warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy.

Formularz (wzór) Wniosku o dopuszczenie do udziału w postępowaniu wraz z załącznikami dotyczący zamówienia (sprawa numer: 63/SISP/PO/2011) jest dostępny na stronie internetowej Zamawiającego pod adresem: [www.stat.gov.pl](http://www.stat.gov.pl) w zakładce [www.stat.gov.pl/bip](http://www.stat.gov.pl/bip). Wniosek o dopuszczenie do udziału w postępowaniu oraz dokumenty dla których Zamawiający określił wzory powinny być sporządzone zgodnie z tymi wzorami co do treści i opisu kolumn.

Wniosek o dopuszczenie do udziału w postępowaniu powinien być podpisany przez osoby upoważnione do reprezentowania Wykonawcy, zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze sądowym, albo przez osobę umocowaną przez osoby uprawnione, przy czym umocowanie (pełnomocnictwo) musi być złożone wraz z wnioskiem. Pełnomocnictwo może być złożone w formie oryginału lub kserokopii poświadczonej notarialnie.

Dokumenty składane wraz z wnioskiem o dopuszczenie do udziału w postępowaniu, o których mowa w Sekcji III.2) ogłoszenia mogą być złożone w oryginale lub kserokopii potwierdzonej za zgodność z oryginałem przez Wykonawcę. Poświadczenie za zgodność z oryginałem powinno być sporządzone w sposób umożliwiający identyfikację podpisu (np. wraz z imienną pieczętką osoby poświadczającej kopię dokumentu za zgodność z oryginałem).

Dokumenty sporządzone w języku obcym powinny być złożone wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę.

Wykonawca powinien dołączyć do wniosku o dopuszczenie do udziału w postępowaniu pełnomocnictwo upoważniające do jego złożenia, o ile prawo to nie wynika z innych dokumentów złożonych wraz z wnioskiem. Zamawiający przewiduje udzielenie zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 6 w wysokości 50 % zamówienia podstawowego.

W niniejszym postępowaniu wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują pisemnie, faksem lub drogą elektroniczną, z zastrzeżeniem wniosku o dopuszczenie do udziału w postępowaniu, który powinien być złożony w formie pisemnej. Także dokumenty i oświadczenia uzupełniane na podstawie art. 26 ust. 3 ustawy na wezwanie Zamawiającego powinny zostać złożone w formie oryginału lub kserokopii potwierdzonej za zgodność z oryginałem przez Wykonawcę, zgodnie z przepisami Rozporządzenia Prezesa Rady Ministrów w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy, oraz form, w jakich te dokumenty mogą być składane (DZ. U. z 2009 r., Nr 226, poz.1817).

W przypadku porozumiewania się faksem lub drogą elektroniczną Zamawiający wymaga niezwłocznego potwierdzenia (faksem lub e-mailem) faktu otrzymania oświadczenia, zawiadomienia lub informacji. We wszelkiej korespondencji dotyczącej niniejszego postępowania należy powoływać się na numer sprawy określony w punkcie IV.3.1) ogłoszenia.

Zamawiający nie ujawni informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503), jeżeli Wykonawca, nie później niż w terminie składania wniosków o dopuszczenie do udziału w postępowaniu, zastrzegł, że nie mogą one być udostępnione. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa, które Wykonawca pragnie utajnić, powinny być załączone na końcu wniosku w osobnej kopercie i opatrzone napisem: „Informacje stanowiące tajemnicę przedsiębiorstwa”, z zachowaniem kolejności numerowania stron wniosku o dopuszczenie do udziału w postępowaniu.

Zamawiający przewiduje udzielenie zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 6 w wysokości 50 % zamówienia podstawowego.

**VI.4) PROCEDURY ODWOŁAWCZE**

**VI.4.1) Organ odpowiedzialny za procedury odwoławcze**

Prezes Urzędu Zamówień Publicznych  
ul. Postępu 17 a  
02-676 Warszawa  
POLSKA  
Internet: <http://www.uzp.gov.pl>  
Faks +48 224587700

**VI.4.2) Składanie odwołań**

Dokładne informacje na temat terminów składania odwołań: Zgodnie z art. 182 ustawy:

1. Odwołanie wnosi się w terminie 10 dni od dnia przesłania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia - jeżeli zostały przesłane w sposób określony w art. 27 ust. 2 ustawy, albo w terminie 15 dni - jeżeli zostały przesłane w inny sposób.

2. Odwołanie wobec treści ogłoszenia o zamówieniu, a jeżeli postępowanie jest prowadzone w trybie przetargu nieograniczonego, także wobec postanowień specyfikacji istotnych warunków zamówienia, wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia specyfikacji istotnych warunków zamówienia na stronie internetowej.

3. Odwołanie wobec czynności innych niż określone w pkt 1 i 2 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

**VI.4.3) Źródło, gdzie można uzyskać informacje na temat składania odwołań**

Departament Odwołań Urzędu Zamówień Publicznych  
ul. Postępu 17 a  
02-676 Warszawa  
POLSKA  
E-mail: [odwolania@uzp.gov.pl](mailto:odwolania@uzp.gov.pl)  
Tel. +48 224587801  
Faks +48 224587800

**VI.5) DATA WYŚLANIA NINIEJSZEGO OGŁOSZENIA:**

8.8.2011