

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



Publikacja Suplementu do Dziennika Urzędowego Unii Europejskiej

2, rue Mercier, L-2985 Luksemburg Faks (352) 29 29-42670

E-mail: ojs@publications.europa.eu Informacje i formularze on-line: <http://simap.europa.eu>

OGŁOSZENIE DODATKOWYCH INFORMACJI, INFORMACJE O NIEKOMPLETNEJ PROCEDURZE LUB SPROSTOWANIE

Uwaga: Jeżeli sprostowanie lub dodanie informacji prowadzi do znaczącej zmiany warunków określonych w pierwotnym ogłoszeniu o zamówieniu, konieczne może okazać się przedłużenie początkowo przewidzianych terminów ze względu na zachowanie zasady równego traktowania oraz warunków konkurencyjności zamówienia.

SEKCJA I: INSTYTUCJA ZAMAWIAJĄCA

I.1) NAZWA, ADRESY I PUNKTY KONTAKTOWE

Oficjalna nazwa: [Główny Urząd Statystyczny](#)

Adres pocztowy: [al. Niepodległości 208](#)

Miejscowość: [Warszawa](#)

Kod pocztowy: [00-925](#)

Kraj: [Polska](#)

Punkt kontaktowy: [Główny Urząd Statystyczny, Biuro Administracyjno-Księgowe, al. Niepodległości 208, pok. 214](#)

Tel.: [+48 226083446](#)

Osoba do kontaktów: [Jan Kozłowski](#)

E-mail: j.kozlowski@stat.gov.pl

Faks: [+48 226083189](#)

Adres(y) internetowy(e) (jeżeli dotyczy)

OGólny adres instytucji zamawiającej (URL): www.stat.gov.pl

Adres profilu nabywcy (URL):

I.2) RODZAJ ZAMAWIAJĄCEGO

Instytucja zamawiająca (w przypadku zamówienia objętego przepisami dyrektywy 2004/18/WE)

Podmiot zamawiający (w przypadku zamówienia objętego przepisami dyrektywy 2004/17/WE – Zamówienia sektorowe)

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

II.1) OPIS

II.1.1) Nazwa nadana zamówieniu przez instytucję zamawiającą (podano w pierwotnym ogłoszeniu)

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) Krótki opis (podano w pierwotnym ogłoszeniu)

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 umożliwić 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,

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

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 SI:

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 16.06.2011 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,

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

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, natywne 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 października 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.

Wykonanie projektu technicznego, dostarczenie brakującej infrastruktury i licencji oraz budowa systemów: System Informacyjny Intranet, REGON, Broker

Komunikacyjny System Certyfikacji na potrzeby realizacji projektu SISP

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.

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

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;

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

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 umożliwia 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;

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

- 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, maszynę 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

Wykonanie projektu technicznego, dostarczenie brakującej infrastruktury i licencji oraz budowa systemów: System Informacyjny Intranet, REGON, Broker

Komunikacyjny, System Certyfikacji na potrzeby realizacji projektu SISP

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:

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

- 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 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 wspomaganie 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 wykorzystaniem 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) weryfikacji 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 użytkowników. 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 rozwiązanie 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,

Wykonanie projektu technicznego, dostarczenie brakującej infrastruktury i licencji oraz budowa systemów: System Informacyjny Intranet, REGON, Broker

Komunikacyjny System Certyfikacji na potrzeby realizacji projektu SISP

- 4) Zasilą 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 niepożądanym dostępem,
- 7) Chroni przed możliwością wprowadzania niespójnych informacji lub niezgodnych z polityką firmy do usług katalogowych LDAP

Moduł propagacji uprawnień udostępnia następujące usługi:

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

- 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, przedefiniowania 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 pracownika 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 Business/ 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 pracownika 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,

Wykonanie projektu technicznego, dostarczenie brakującej infrastruktury i licencji oraz budowa systemów: System Informacyjny Intranet, REGON, Broker

Komunikacyjny System Certyfikacji na potrzeby realizacji projektu SISP

- 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) Powiadamianie 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 dyskowe,
 - 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,

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

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 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

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

- 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.1.3) Wspólny Słownik Zamówień (CPV) (podano w pierwotnym ogłoszeniu)

	Słownik główny	Słownik uzupełniający (jeżeli dotyczy)
Główny przedmiot	48000000	
Dodatkowe przedmioty	48311100	
	30216110	
	72212000	
	72268000	
	72253200	
	72212211	

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

IV.1) RODZAJ PROCEDURY

IV.1.1) Rodzaj procedury (podano w pierwotnym ogłoszeniu)

- Otwarta
- Ograniczona
- Ograniczona przyspieszona
- Negocjacyjna
- Negocjacyjna przyspieszona
- Dialog konkurencyjny

IV.2) INFORMACJE ADMINISTRACYJNE

IV.2.1) Numer referencyjny nadany sprawie przez instytucję zamawiającą /podmiot zamawiający (podano w pierwotnym ogłoszeniu, o ile dotyczy)

[63/SISP/PO/2011](#)

IV.2.2) Dane referencyjne ogłoszenia w przypadku ogłoszeń przesłanych drogą elektroniczną (jeżeli są znane):

Pierwotne ogłoszenie przesłane przez:

- SIMAP
- OJS eSender

Login: [ENOTICES_GUS](#)

Dane referencyjne ogłoszenia: [2011-111059](#) (rok i numer dokumentu)

IV.2.3) Ogłoszenie, którego dotyczy niniejsza publikacja (jeżeli dotyczy)

Numer ogłoszenia w Dz.U.: 2011/S	z dnia	(dd/mm/rrrr)
153-254777	11/08/2011	

IV.2.4) Data wysłania niniejszego ogłoszenia:

[08/08/2011](#) (dd/mm/rrrr)

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

VI.1) OGŁOSZENIE DOTYCZY

(o ile ma zastosowanie; zaznaczyć tyle punktów, ile jest to konieczne)

- Procedury niepełnej
 Sprostowania
 Informacji dodatkowych

VI.2) INFORMACJE NA TEMAT NIEPEŁNEJ PROCEDURY UDZIELENIA ZAMÓWIENIA

(o ile ma zastosowanie; zaznaczyć tyle punktów, ile jest to konieczne)

<input type="radio"/> Postępowanie o udzielenie zamówienia została przerwane.
<input type="radio"/> Postępowanie o udzielenie zamówienia uznano za nieskuteczne.
<input type="radio"/> Zamówienia nie udzielono.
<input type="radio"/> Zamówienie może być przedmiotem ponownej publikacji.

VI.3) INFORMACJE DO POPRAWIENIA LUB DODANIA

(o ile dotyczy; należy określić miejsce, w którym tekst lub daty mają być zmienione lub dodane, proszę zawsze podawać odpowiedni numer sekcji i akapitu pierwotnego ogłoszenia)

VI.3.1) Zmiana oryginalnej informacji lub publikacja w witrynie TED niezgodna z oryginalnymi informacjami.

- Zmiana oryginalnej informacji podanej przez instytucję zamawiającą
 Publikacja w witrynie TED niezgodna z oryginalną informacją, przekazaną przez instytucję zamawiającą
 W obu przypadkach

VI.3.2) Ogłoszenie lub odpowiednia dokumentacja przetargowa

- W ogłoszeniu pierwotnym
 W odpowiedniej dokumentacji przetargowej (więcej informacji w odpowiedniej dokumentacji przetargowej)
 W obu przypadkach (więcej informacji w odpowiedniej dokumentacji przetargowej)

VI.3.3) Tekst, który należy poprawić w pierwotnym ogłoszeniu (jeżeli dotyczy)

Miejsce, w którym znajduje się zmieniany tekst:	Zamiast:	Powinno być:

VI.3.4) Daty, które należy poprawić w pierwotnym ogłoszeniu (jeżeli dotyczy)

Miejsce, w którym znajdują się zmieniane daty:	Zamiast:		Powinno być:	
	(dd/mm/rrrr)	(gg:mm)	(dd/mm/rrrr)	(gg:mm)
IV.3.4)	09/09/2011	11:00	23/09/2011	11:00

Wykonanie projektu technicznego, dostarczenie brakującej infrastruktury i licencji oraz budowa systemów: System Informacyjny Intranet, REGON, Broker Komunikacyjny, System Certyfikacji na potrzeby realizacji projektu SISP
VI.3.5) Adresy i punkty kontaktowe, które należy poprawić (jeżeli dotyczy)

Miejsce, w którym znajduje się zmieniany tekst:	
Oficjalna nazwa:	
Adres pocztowy:	
Miejscowość:	Kod pocztowy:
Kraj:	
Punkt kontaktowy:	Tel.:
Osoba do kontaktów:	
E-mail:	Faks:
Adres(y) internetowy(e) (jeżeli dotyczy)	
Ogólny adres instytucji zamawiającej (URL):	
Adres profilu nabywcy (URL):	

VI.3.6) Tekst, który należy dodać do pierwotnego ogłoszenia (jeżeli dotyczy)

Miejsce, w którym należy dodać tekst	Tekst do dodania

VI.4) INNE DODATKOWE INFORMACJE (jeżeli dotyczy)

VI.5) DATA WYSŁANIA NINIEJSZEGO OGŁOSZENIA:

07/09/2011 (dd/mm/rrrr)