

Opis posiadanego SZT i koncepcja zmian

Spis treści

I.	Wstęp	2
II.	Stan obecny	2
1.	Posiadane licencje oprogramowania	6
2.	Posiadana infrastruktura.....	8
3.	Wykorzystywane konektory.....	13
4.	Funkcjonalności biznesowe dostępne w SZT	14
5.	Zasoby obsługiwane poprzez SZT.....	15
III.	Wstępne wymagania techniczne dla SZT	16
IV.	Migracja SZT	25
	ETAP M1 – Przygotowanie infrastruktury COO i ZCOO, w tym dla środowiska developerskiego i przedprodukcyjnego oraz plan migracji danych z zachowaniem funkcjonalności	25
	ETAP M2 – Przygotowanie środowiska aplikacyjnego COO i ZCOO, przeprowadzenie migracji danych oraz uruchomienie środowiska developerskiego i przedprodukcyjnego	27
	Warsztaty.....	28
V.	Rozwój funkcjonalny SZT	28
	ETAP R1 – Opracowanie projektu i wdrożenie zmian wynikających z integracji SZT i SWEZ.....	28
	ETAPY R2 – R5: Budowa/Przebudowa Konektorów.....	30
	ETAP R6 – Manualny Provisioning	33
	ETAP R7 – Monitorowanie i raportowanie	33
	ETAP R8 – Moduł Administracyjny.....	35
	ETAP R9 – Moduł Zarządzania Kontami Uprzywilejowanymi	35
	Warsztaty.....	39

I. Wstęp

1. W ramach realizacji zamówienia Wykonawca będzie zobowiązany do:
 - 1) przeprowadzenia Migracji SZT zgodnie z wymaganiami określonymi w rozdziale IV niniejszego dokumentu, w terminie nieprzekraczającym **26 tygodni** od daty zawarcia Umowy na realizację przedmiotu zamówienia;
 - 2) świadczenia Usług Wykonawcy, poprzez świadczenie Usługi utrzymania i Usług serwisowych na zasadach określonych w dokumencie Metryki Usług Wykonawcy przez cały okres realizacji przedmiotu zamówienia, tj.:
 - a. SZT posiadanego przez Zamawiającego, którego opis zawarty jest w dokumencie Szczegółowy opis działania obecnego SZT,
 - b. SZT po Migracji SZT, w trakcie jego rozwoju i po zakończeniu wszystkich Zleconych przez Zamawiającego etapów Rozwoju funkcjonalnego SZT, o którym mowa w rozdziale V niniejszego dokumentu, przez okres czterech lat od daty zawarcia Umowy;
 - 3) świadczenia na rzecz Zamawiającego Usług dodatkowych, przez cały okres trwania Umowy.

Poprzez Usługę dodatkową rozumie się rodzaj usługi świadczonej przez Wykonawcę, w ramach której Wykonawca na Zlecenie i użytek Zamawiającego zapewnia: współpracę przy dostosowywaniu SZT do zmian organizacyjnych Zamawiającego, współpracę przy dostosowywaniu SZT do zmian zintegrowanych z nim systemów, współpracę przy dostosowaniu SZT do objęcia monitorowaniem i raportowaniem kolejnych elementów wynikających ze zmian organizacyjnych Zamawiającego wraz z opracowaniem Dokumentacji, transfer wiedzy do przedstawicieli Zamawiającego w postaci instruktaży w zakresie niezbędnym do utrzymania SZT na poziomie określonym w Metrykach usług Wykonawcy, inne wynikające z zakresu realizacji przedmiotu zamówienia, niemożliwe do zrealizowania w zakresie Metryk usług Wykonawcy
 - 4) realizacji Rozwoju funkcjonalnego SZT zgodnie z **rozdziałem V** niniejszego dokumentu oraz w dokumencie Koncepcja zmian biznesowych wniosku o uprawnienia do SWEZ w SZT.
2. Przez cały okres realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do przestrzegania procedur obowiązujących u Zamawiającego oraz do:
 - 1) przeniesienia autorskich praw majątkowych do przekazywanych Produktów;
 - 2) opracowania i aktualizacji dokumentacji dla SZT w szczególności dokumentacji wynikającej z realizacji cyklu projektowego (w tym: harmonogramy realizacji, dokumentacja analityczna, plany testów, dokumentacja techniczna, dokumentacja użytkownika, dokumentacja administratora, materiały szkoleniowe, Procedury administratorskie, Procedury eksploatacyjne, Standardy IT ZUS, instrukcje, utworzenie/aktualizacja pozostałej dokumentacji użytkownika systemu wynikających ze Zleceń);
 - 3) przekazywania Kodów źródłowych i ich aktualizacji po wprowadzeniu każdej zmiany Oprogramowania.
3. Kryteria odbioru poszczególnych etapów Rozwoju funkcjonalnego SZT będą uszczegółowione w Zleceniu.

Realizacja przedmiotu zamówienia w zakresie Migracji SZT i Rozwoju funkcjonalnego SZT będzie następowała etapami, zadania z nich wynikające będą mogły być realizowane równolegle.

II. Stan obecny

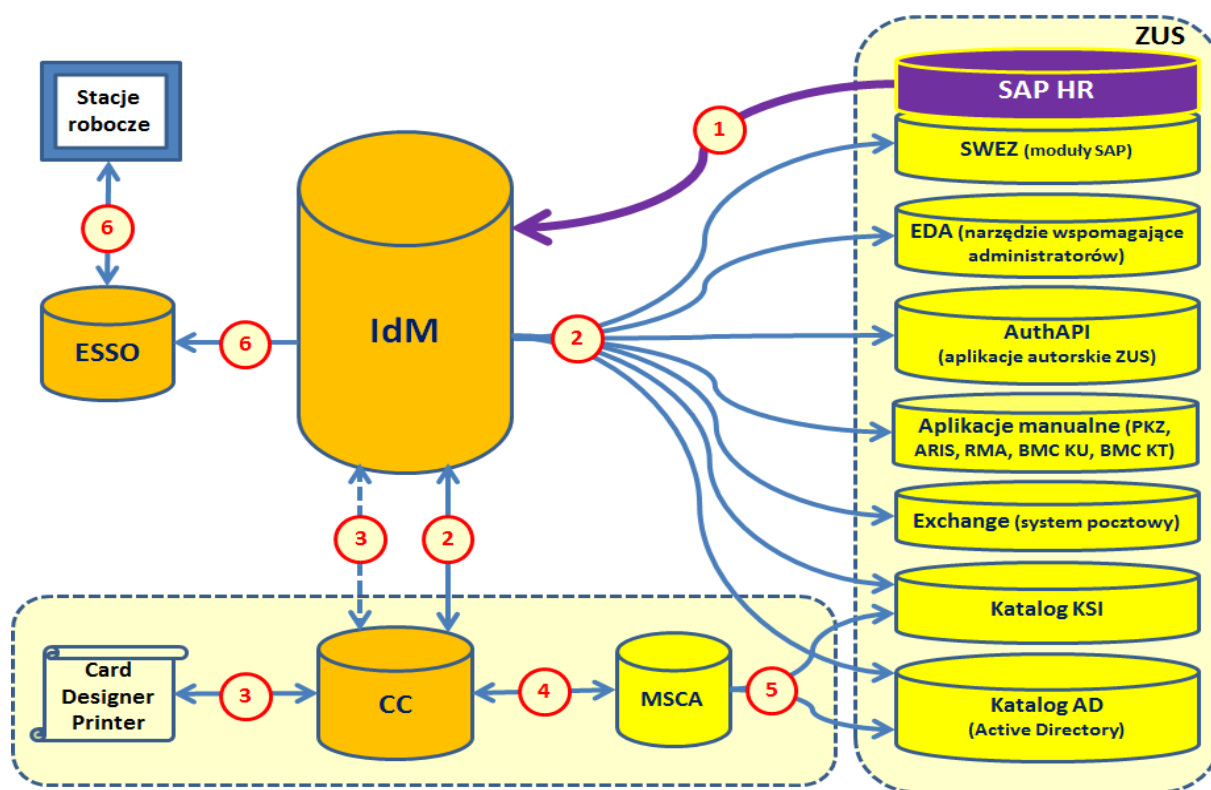
Posiadany przez Zamawiającego SZT został wdrożony w 2014 r. jest to System Oracle Identity Manager w wersji 11G. Baza SZT, jest częściowo zasilana automatycznie. Dane w zakresie pracowników i struktury organizacyjnej Zamawiającego są pobierane z systemu SAP HR, który jest

częścią Systemu Wspomagania Ekonomiki Zakładu (SWEZ). Dane dotyczące Pracowników zewnętrznych wprowadzane są do SZT przez uprawnionych pracowników Zamawiającego.

W skład użytkowanego u Zamawiającego SZT wchodzi:

1. IdM - Moduł Zarządzania Tożsamością - centralna baza tożsamości zasilana danymi z systemu SAP HR. Moduł odpowiada za zasilanie aplikacji i systemów informatycznych użytkowanych u Zamawiającego Kontami Użytkowników, nadawanie uprawnień w systemach informatycznych (zgodnie z przepływami pracy). Moduł IdM komunikuje się z systemami za pomocą gotowych lub wytworzonych Konektorów. Moduł ten udostępnia interfejs wnioskowania o uprawnienia do Zasobów, pozwala na raportowanie aktualnych i historycznych danych dotyczących dostępów i uprawnień użytkowników w systemach zintegrowanych z SZT. W skład modułu wchodzi następujące komponenty:
 - 1) Oracle Identity Manager (OIM) - oprogramowanie pozwalające zaimplementować logikę zarządzania Kontami i uprawnieniami w zarządzanej infrastrukturze;
 - 2) Oracle SOA Suite (SOA) - implementacja workflow, zapewniająca możliwość konfiguracji procesu przepływu zadań w systemie IdM (Oracle Identity Manager);
 - 3) Oracle BI Publisher - platforma raportowa dostarczająca funkcjonalności budowania zestawień na podstawie danych audytowych znajdujących się w repozytorium Tożsamości systemu IdM oraz repozytorium Centrum Certyfikacji (historia certyfikacji pracownika);
 - 4) Oracle Weblogic Application Server (WLS) - serwer aplikacyjny, na którym uruchomione są usługi aplikacyjne (JEE Application Server);
 - 5) Oracle HTTP Server (OHS) - serwer WWW, który powstał w oparciu o produkt Apache HTTP Server;
 - 6) Oracle Identity Manager Connector - komponent instalowany i uruchamiany w kontekście Oracle Identity Manager'a (OIM). Zadaniem komponentu jest tłumaczenie decyzji podejmowanych po stronie OIM na konkretne akcje;
 - 7) Oracle Entitlement Server (OES) - komponent wewnętrzny modułu IdM, zapewniający możliwość definiowania ról systemowych, nadających uprawnienia administracyjne w procesie zarządzania Tożsamością.
2. Centrum Certyfikacji (CC) - moduł w skład którego wchodzi serwery usług Certyfikatów zbudowane na bazie Windows Serwer 2008 R2, sprzętowe moduły kryptograficzne, oprogramowanie do personalizacji Kart elektronicznych. Główna funkcjonalność modułu, to: wydawanie i unieważnianie Certyfikatów, publikowanie list CRL, personalizacja Kart elektronicznych. Certyfikaty zapisywane są na Kartach elektronicznych oraz są przekazywane do Katalogu AD i do Katalogu KSI. Funkcjonalność tego modułu realizowana jest poprzez kilka składników oprogramowania:
 - 1) Urzędy Certyfikujące – czyli urzędy odpowiedzialne za wydawanie Certyfikatów klucza publicznego uruchomione u Zamawiającego jako ZUSRrootCA i ZUSIssuingCA;
 - 2) Card Designer Printer - oprogramowanie do personalizacji Kart elektronicznych. Dane do personalizacji Karty elektronicznej pobierane są z bazy zasilanej za pomocą modułu IdM, u Zamawiającego istnieje zdefiniowany wzór Kart elektronicznych;
 - 3) Konektor do modułu IdM i komponenty pośredniczące w wymianie danych (CC);
 - 4) Synchronizer - oprogramowanie odpowiedzialne za synchronizację i publikację Certyfikatów w Katalogu KSI. Komponent ten odpowiada również za aktualizację informacji o Certyfikatach w Katalogu KSI (odnowienie, unieważnienie). Komponent ten pobiera dane z bazy CC;
 - 5) Scheduler – oprogramowanie pośredniczące między bazą CC a usługami Infrastruktury klucza publicznego (PKI) udostępnianymi przez serwery MSCA (serwery Centrum Certyfikacji). Oprogramowanie odpowiada za obsługę wniosków o Certyfikaty trafiających z systemu IdM do bazy CC. Na podstawie wniosków z bazy CC Scheduler generuje, odnawia, unieważnia Certyfikaty i je publikuje;

- 6) CertTools – oprogramowanie dedykowane przeznaczone do wykonywania operacji związanych z zapisywaniem Certyfikatów do plików (PFX/P12), a także wsadowym wydawaniem dowolnych Certyfikatów dla urządzeń i Użytkowników;
 - 7) HSM – 2 moduły kryptograficzne (Thales nShield Connect 1500) wykorzystywane w procesie generowania Certyfikatów.
3. ESSO - Moduł Enterprise Single-Sign On - oprogramowanie realizujące operacje jednokrotnego logowania do aplikacji użytkowanych u Zamawiającego. Moduł ESSO korzysta z Katalogu AD (Active Directory) jako centralnego repozytorium ESSO oraz instalowany jest na stacjach roboczych pracowników Zamawiającego. Moduł odpowiada za realizację operacji uwierzytelniania do aplikacji, które wymagają podania nazwy Logowania i Hasła – z wyłączeniem Aplikacji interakcyjnych (Aplikacji KSI). Aplikacje interakcyjne korzystają z rodzimego mechanizmu uwierzytelniania (Certyfikat zapisany na Karcie elektronicznej). W skład ESSO wchodzi:
- 1) ESSO-LM - ang. Oracle Enterprise Single Sign On Logon Manager;
 - 2) ESSO-AM - ang. Oracle Enterprise Single Sign On Authentication Manager;
 - 3) ESSO-PG - ang. Oracle Enterprise Single Sign On Provisioning Gateway;
 - 4) ESSO-PR - ang. Oracle Enterprise Single Sign On Password Reset.



Rysunek: Ogólna architektura SZT

Opis przepływu danych pomiędzy elementami SZT zawarty jest w poniższej tabeli:

Przeptyw	Opis
1	Głównym źródłem informacji o Tożsamościach dla pracowników zatrudnionych u Zamawiającego jest system SAP HR, większość atrybutów opisujących Tożsamość pracownika ma określone wartości w tym systemie, niektóre informacje są także pobierane z innych źródeł np. Katalog AD. W przypadku niektórych atrybutów moduł IdM na podstawie zaimplementowanej logiki określa ich wartości – dla procesu zatrudnienia nowego pracownika np. są dla niego automatycznie tworzone:

	<ul style="list-style-type: none"> • Konto w Katalogu AD, • Konto w Katalogu KSI, • Konto w SWEZ, • skrzynka pocztowa Exchange, • Zasoby: Karta elektroniczna, Certyfikat AD, Certyfikat KSI i Certyfikat ENC. <p>Prezentują to przepływy opisane cyfrą 2 oraz 3.</p>
2	<p>Moduł IdM pozwala w sposób automatyczny tworzyć i aktualizować Konta w systemach eksploatowanych u Zamawiającego. W zależności od procesu biznesowego, Konta są tworzone automatycznie lub poprzez wygenerowanie odpowiedniego żądania przez przełożonego pracownika. Wykaz grup systemów, w których SZT tworzy Konta:</p> <ul style="list-style-type: none"> • Katalog AD (Active Directory) - domena ZUS.AD, pojedyncza domena, Katalogu Active Directory. Katalog jest jednolity dla całej organizacji. Każdy pracownik lub Pracownik zewnętrzny musi posiadać Konto w Domenie ZUS.AD, bez niego nie jest możliwe uzyskanie dostępu do systemów użytkowanych u Zamawiającego, • Exchange - system pocztowy eksploatowany u Zamawiającego, • Katalog KSI - katalog korporacyjny zbudowany w oparciu o katalog SUN One Directory Server. Katalog jest głównym i jedynym repozytorium informacji dla Aplikacji KSI. Uwierzytelnianie do tych aplikacji wymaga opublikowania w Katalogu KSI certyfikatu X509, • SWEZ (System Wspomagania Ekonomiki Zakładu) - moduły SAP, • AuthAPI – baza wykorzystywana do autoryzowania Użytkowników głównie dla aplikacji autorskich wytworzonych siłami IT Zamawiającego, • EDA – narzędzie wspomagające administratorów w realizacji ich zadań i zarządzanie IT. <p>Dodatkowo istnieją aplikacje manualne (obecnie: BMC KT, BMC KU, PKZ, ARIS, RMA), dla których operacje tworzenia Kont obsługiwane są za pomocą Manualnego Provisioningu.</p>
3	<p>Każdy pracownik Zamawiającego posiada Kartę elektroniczną, za pomocą której uwierzytelnia się w Domenie ZUS.AD.</p> <p>Karty elektroniczne są rejestrowane w module IdM oraz wstępnie personalizowane. Dane do personalizacji dostarczane są z modułu IdM. Rejestracja Karty elektronicznej polega na odczycie w aplikacji Card Designer Printer numeru seryjnego interfejsu stykowego i bezstykowego oraz zapisaniu tej informacji w bazie modułu CC. Konektor modułu IdM odczytuje te informacje i powiązuje je z odpowiednią Tożsamością. Personalizacja Karty elektronicznej polega na wykonaniu nadruku (wraz ze zdjęciem pracownika) oraz zapisaniu Certyfikatu na Karcie elektronicznej – graficzny wygląd Karty elektronicznej jest określony wewnętrznymi normami Zamawiającego. Żądanie Certyfikatu jest przesyłane z modułu IdM do modułu CC.</p>
4	<p>Moduł CC pełni, między innymi, funkcję modułu pośredniczącego, za pomocą którego wysyłane są żądania rejestracji, odnowienia, unieważnienia Certyfikatów do urzędu Certyfikatów zbudowanego na bazie Windows Server 2008 R2 (Microsoft Certificate Services Authority) zintegrowanego z Katalogiem AD. Komunikacja pomiędzy modułem CC a modułem IdM odbywa się na poziomie bazy danych (Oracle) modułu CC, do której moduł IdM dostaje się za pomocą odpowiedniego Konektora. Moduł CC wyposażony jest również w synchronizator, który zapewnia publikowanie Certyfikatów w Katalogu KSI.</p>

5	Certyfikaty są publikowane bezpośrednio w użytkowanych u Zamawiającego katalogach LDAP (Katalog AD i Katalog KSI). W przypadku Katalogu AD do publikacji wykorzystane są rodzime mechanizmy usług Certyfikatów na serwerach Windows 2008, w przypadku publikacji do Katalogu KSI użyty jest specjalny synchronizator.
6	<p>Część aplikacji u Zamawiającego korzysta z niestandardowych repozytoriów Kont i Haseł (inne niż Katalog AD i Katalog KSI) np. Auth API. Logowanie do tych aplikacji może odbywać się za pomocą modułu ESSO. Moduł ten zainstalowany jest na każdej stacji roboczej u Zamawiającego pracującej pod kontrolą systemu Windows (obecnie jest to Windows 7 lub Windows 10 - zmiana systemu Windows na wyższy jest dynamiczna – może nastąpić w trakcie trwania Umowy). Moduł ESSO zasilany jest za pomocą modułu IdM (nazwy Logowania i Hasła do aplikacji) przez co umożliwia Użytkownikom Uwierzytelnienie do poszczególnych aplikacji korzystających z nazw logowania i Haseł za pomocą wymaganej u Zamawiającego Karty elektronicznej. Moduł ESSO korzysta z Katalogu AD do przechowywania informacji niezbędnych do Uwierzytelnienia w aplikacjach.</p> <p>Wyjątkiem, dla których moduł ESSO nie ma zastosowania z woli Zamawiającego dotyczy logowania do Aplikacji KSI, które odbywa się za pomocą Certyfikatu zapisanego na Karcie elektronicznej.</p>

Tabela: Opis komunikacji pomiędzy modułami Systemu

1. Posiadane licencje oprogramowania

Zamawiający dysponuje ogólnie bezterminowymi licencjami Oracle do SZT:

Produkt i liczba licencji	
Oracle Identity Manager Connector - IBM RACF - Connector Perpetual	1
Oracle Identity Manager Connector - UNIX - Connector Perpetual	1
Oracle Identity Manager Connector - Sun Java System Directory - Connector Perpetual	1
Oracle Identity Manager Connector - SAP Enterprise Applications - Connector Perpetual	1
Oracle Identity Manager Connector - Microsoft Windows - Connector Perpetual	1
Oracle Identity Manager Connector - Microsoft Exchange - Connector Perpetual	1
Oracle Identity Manager Connector - Database User Management - Connector Perpetual	1
Oracle Identity Manager Connector - BMC Remedy User Management - Connector Perpetual	1
Oracle Identity and Access Management Suite Plus - Employee User Perpetual	50 000
Oracle Identity Manager Connector - Microsoft Active Directory - Connector Perpetual	1
Oracle Enterprise Single Sign-On Suite Plus - Named User Plus Perpetual	50 000
Oracle Advanced Security - Processor Perpetual	6
Oracle Database Enterprise Edition - Processor Perpetual	6

Tabela: Wykaz bezterminowych licencji firmy Oracle dla SZT

Szczegółowy wykaz licencji, uwzględniający również ww. wymienione, które są wykorzystywane przy SZT przedstawia poniższa tabela:

1	IdM - serwery Serwerownia Główna - 2 szt.	Licencje	Ilość
	Serwer, typ A Sun Server X3-2:	Licencja Oracle DataBase Enterprise Edition 1 CPU	4
	• 1 Intel(R) Xeon(R) E5-2609 4-	Licencja Oracle Advanced Security dla 1 CPU - Enterprise	4

	core 2.4 GHz processor (for factory installation) - sztuk: 2	Edition Option.	
		A97163 @ SOFTWARE UPDATE LICENSE & SUPPORT Okres obowiązywania od: 13/03/08 do: 14/03/07	8
		L90617 @ LICENCJA ORACLE SOLARIS CLUSTER ENTER.	8
2	IdM - serwery Serwerownia Zapasowa - 1 szt.		
	Serwer, typ B Sun Server X3-2: model family • 1 Intel(R) Xeon(R) E5-2609 4-core 2.4 GHz processor (for factory installation) - sztuk:2	Licencja Oracle DataBase Enterprise Edition 1 CPU	2
		Licencja Oracle Advanced Security dla 1 CPU - Enterprise Edition Option.	2
3	IdM – macierz - 1 szt.		
	StorageTek 2540 M2 array • One 3 TB 7200 rpm 3.5-inch SAS HDD with bracket (for factory installation) - sztuk:6	Licencja Enterprise Single Sign-On Suite Plus - Named User Plus Perpetual 50 000 NUP	1
		Licencja Identity Manager Connector - BMC Remedy User Management - Connector Perpetual, 1 connector	1
		Licencja Identity Manager Connector - Database User Management - Connector Perpetual, 1 connector	1
		Licencja Identity Manager Connector - IBM RACF - Connector Perpetual 1 connector	1
		Licencja Identity Manager Connector - Microsoft Active Directory - Connector Perpetual, 1 connector	1
		Licencja Identity Manager Connector - Microsoft Exchange - Connector Perpetual 1 connector	1
		Licencja Identity Manager Connector - Microsoft Windows - Connector Perpetual 1 connector	1
		Licencja Identity Manager Connector - SAP Enterprise Applications - Connector Perpetual, 1 connector	1
		Licencja Identity Manager Connector - Sun Java System Directory - Connector Perpetual, 1 connector	1
		Licencja Identity Manager Connector - UNIX - Connector Perpetual, 1 connector	1
		Licencje Identity and Access Management Suite Plus - Employee User Perpetual 50 000 employee	1
4	HSM Sprzętowy Moduł Kryptograficzny (Serwerownia Główna i Zapasowa)		
	HSM - nShield Connect 1500; F3; SEE Ready (no nTokens)	Additional 'soft' client licence - (does not include nToken	1
	HSM - nShield Connect 1500; F3; SEE Ready (no nTokens)	Additional 'soft' client licence - (does not include nToken	1
	Serwer wirtualny Centrum Certyfikacji	Additional Client Activation for standby or failover Connect (or netHSM) – REDUNDANT system (2 licenses)	1
	Serwer wirtualny	Additional Client Activation for standby or failover Connect (or netHSM) – REDUNDANT system (2 licenses)	1
	Serwer wirtualny Centrum Certyfikacji	Gold Support	1
	Serwer wirtualny Centrum Certyfikacji	Gold Support	1
5	Serwery wirtualne		
	Serwer wirtualny skanujący	Licencja NESSUS ProfessionalFeed	1

	Nessus	Tenable Certified Nessus Auditor Exam	1
		Tenable Nessus Vulnerability and Compliance Auditing - On Demand	1
		3 Year Nessus ProfessionalFeed Subscription (New) - 1049 dni od dnia 14.03.2013	1
	Serwer wirtualny Centrum Certyfikacji (wspólny klaster)	SteelEye DataKeeper Cluster Edit. v7.5 for Windows 2008	1
	Serwer wirtualny Centrum Certyfikacji (klaster)	SteelEye DataKeeper Cluster Edit. v7.5 for Windows 2008	1
	Serwer wirtualny Centrum Certyfikacji (wspólny klaster)	SteelEye Support DataKeeper CE v7.5 for MS Windows Server 2008, 1 year	1
	Serwer wirtualny Centrum Certyfikacji (klaster)	SteelEye Support DataKeeper CE v7.5 for MS Windows Server 2008, 1 year	1
	Serwer wirtualny WWW i Provisioning Gateway	Licencja Microsoft Windows Server Standard Assurance Pack Government OPEN 1 License No Level 2 PROC	1
	Serwer wirtualny aplikacji i WWW zapasowy	Licencja Microsoft Windows Server Standard Assurance Pack Government OPEN 1 License No Level 2 PROC	1
	Serwer wirtualny Provisioning Gateway i aplikacji zapasowy	Licencja Microsoft Windows Server Standard Assurance Pack Government OPEN 1 License No Level 2 PROC	1
	Serwer wirtualny aplikacji i Provisioning Gateway zapasowy	Licencja Microsoft Windows Server Standard Assurance Pack Government OPEN 1 License No Level 2 PROC	1
	Serwer wirtualny WWW	Licencja Microsoft Windows Server Standard Assurance Pack Government OPEN 1 License No Level 2 PROC	1
	Serwer wirtualny aplikacji	Licencja Microsoft Windows Server Standard Assurance Pack Government OPEN 1 License No Level 2 PROC	1

Tabela: Wykaz wszystkich licencji dla SZT użytkowanego u Zamawiającego

Zamawiający nie przewiduje konieczności zwiększenia ilości dostępnych licencji na czas utrzymywania obecnego SZT przez Wykonawcę, do czasu przeprowadzenia Migracji SZT.

2. Posiadana infrastruktura

Konfiguracja sprzętowa obecnie użytkowanego u Zamawiającego SZT przedstawia się następująco.

Serwery bazodanowe IdM i CC		
1.	COO	Ilość
	Sun Server X3-2: model family	2
	3.5-inch HDD filler panel (for factory installation)	2
	Sun Storage 6 Gb SAS PCIe RAID HBA, Internal: 8 port and 512 MB cache (for factory installation)	1
	1 Intel(R) Xeon(R) E5-2609 4-core 2.4 GHz processor (for factory installation)	2
	Heatsink (for factory installation)	1
	One 8 GB DDR3-1600 DIMM (for factory installation)	8
	3.5inch 600GB SAS 15K RPM HDD	2
	Sun Quad Port GbE PCIe 2.0 Low Profile Adapter, UTP (for factory installation)	1
	StorageTek 8 Gb Fibre Channel PCIe HBA dual port QLogic (for factory	1

		Installation)	
		Sun Server X3-2: 1 RU base chassis with motherboard, 2 PSUs, slide rail kit	1
		PCIe filler panel (for factory installation)	1
		Four 3.5-inch drive slots disk cage	1
		Power cord: Europe, 2.5 meters, CEE7NII plug, C13 connector, 10 A (for factory installation)	2
		Single processor I/O cover kit (for factory installation)	1
		StorageTek 2540 M2 array (macierz dyskowa)	1
		One 3 TB 7200 rpm 3.5-inch SAS HDD with bracket (for factory installation)	6
		1 AC power supply (for factory installation)	2
		Power cord: Europe, 2.5 meters, CEE7NII plug, C13 connector, 10 A (for factory installation)	2
		1 drive filler panel (for factory installation)	7
		StorageTek 2540 M2 array: dual FC controller with four 8 Gb/sec FC ports and 2 GB cache, and rail kits	1
2.	ZCOO		Ilość
	Sun Server X3-2: model family		1
		Sun Storage 6 Gb SAS PCIe RAID HBA, Internal: 8 port and 512 MB cache (for factory installation)	1
		1 Intel(R) Xeon(R) E5-2609 4-core 2.4 GHz processor (for factory installation)	2
		Heatsink (for factory installation)	1
		One 8 GB DDR3-1600 DIMM (for factory installation)	8
		3.5inch 600GB SAS 15K RPM HDD	1
		One 3 TB 7200 rpm 3.5-inch SAS HDD with bracket (for factory installation)	3
		Sun Quad Port GbE PCIe 2.0 Low Profile Adapter, UTP (for factory installation)	1
		Sun Server X3-2: 1 RU base chassis with motherboard, 2 PSUs, slide rail kit	1
		PCIe filler panel (for factory installation)	1
		Power cord: Europe, 2.5 meters, CEE7NII plug, C13 connector, 10 A (for factory installation)	2
		Single processor I/O cover kit (for factory installation)	1
Serwery aplikacyjne Centrum Certyfikacji			
1.	COO		Ilość
	serwer wirtualny	<ul style="list-style-type: none"> • liczba rdzeni – 1 • RAM – 4 GB • SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB • SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 40 GB • vNIC 1- 1 adres IP 	1
	serwer wirtualny	<ul style="list-style-type: none"> • liczba rdzeni – 4 • RAM – 4 GB • SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB • SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 50 GB • SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – S: 50 GB • vNIC 1- 1 adres IP 	2
	nShield	<ul style="list-style-type: none"> • Dual, hot-swap power supplies, each with IEC 320 mains socket & 	1

	Connect 1500; F3; SEE Ready (no nTokens) (HSM)	<ul style="list-style-type: none"> rocker switch Mains cable retaining bracket, supplied with cable retainers 2x 1 Gigabit Ethernet ports Slide rails (one pair per HSM) Smart cards for administrators and operators (15 cards sold as standard with each unit) 5 pack standard nCipher smartcards (one per HSM) Additional 'soft' client licence - (does not include nToken) - 2 sztuki Additional Client Activation for standby or failover Connect (or netHSM) – REDUNDANT system (2 licenses) 	
2.	ZCOO		Ilość
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 1 RAM – 4 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 40 GB vNIC 1- 1 adres IP 	1
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 4 RAM – 4 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 50 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – S: 50 GB vNIC 1- 1 adres IP 	1
	nShield Connect 1500; F3; SEE Ready (no nTokens) (HSM)	<ul style="list-style-type: none"> Dual, hot-swap power supplies, each with IEC 320 mains socket & rocker switch Mains cable retaining bracket, supplied with cable retainers 2x 1 Gigabit Ethernet ports Slide rails (one pair per HSM) Smart cards for administrators and operators (15 cards sold as standard with each unit) 5 pack standard nCipher smartcards (one per HSM) Additional 'soft' client licence - (does not include nToken) - 2 sztuki Additional Client Activation for standby or failover Connect (or netHSM) – REDUNDANT system (2 licenses) 	1
	Stacje do personalizacji kart elektronicznych	<p>Komputer - V260ST G630 4GB 500GB DVD-RW GeForce620 _1GB:</p> <ul style="list-style-type: none"> Producent Dell Typ obudowy komputera Slim Tower Ilość zainstalowanych procesorów 1 szt. Typ zainstalowanego procesora Intel Pentium Dual-Core Kod procesora G630 Częstotliwość procesora 2,7 GHz Częstotliwość szyny QPI/DMI 5 GT/s Pojemność pamięci cache [L3] 3 MB Ilość zainstalowanych dysków 1 szt. Pojemność zainstalowanego dysku 500 GB Typ zainstalowanego dysku SATA II Pojemność zainstalowanej pamięci 4096 MB Rodzaj zainstalowanej pamięci DDR3 Częstotliwość szyny pamięci 1333 MHz Ilość banków pamięci 2 szt. Producent chipsetu zainstalowanej płyty głównej Intel 	3

		<ul style="list-style-type: none"> • Typ zainstalowanego chipsetu H61 • Typ zainstalowanej karty graficznej NVIDIA GeForce GT 620 • Zainstalowana pamięć wideo 1024 MB • Zintegrowana karta dźwiękowa Tak • Zintegrowana karta sieciowa Tak • Typ zintegrowanej karty sieciowej 10/100/1000 Mbit/s • Ilość slotów PCI-E 1x 3 szt. • Ilość wolnych slotów PCI-E 1x 3 szt. • Ilość slotów PCI-E 16x 1 szt. • Interfejsy 1 x 15-stykowe D-Sub (wyjście na monitor) • 1 x HDMI • 8 zewnętrznych portów USB 2.0 • 1 x RJ-45 (LAN) • 1 x wyjście słuchawkowe (na froncie obudowy) • 1 x wejście na mikrofon (na froncie obudowy) • 1 x wejście na mikrofon • 1 x wejście liniowe • 1 x wyjście liniowe • Dodatkowe informacje o portach USB 2.0/3.0 • 6 x USB 2.0 (tylny panel) • 2 x USB 2.0 (przedni panel) • Napędy wbudowane (zainstalowane) DVD±RW Super Multi (+ DVD-RAM) Dual Layer • Moc zasilacza (zasilaczy) 300 Wat • System operacyjny Microsoft Windows 7 Professional PL 64-bit • Klawiatura - US-Euro (Qwerty) Dell KB212-B Quietkey USB Klawiatura Czarny C0424376 • Mysz - Dell Optical Scroll USB 2 Buttons Black Mouse • Czytnik kart - ACS ACR38 USB 	
		<p>Monitor - Dell E170S 17" 5:4 1280x1024 VGA</p> <ul style="list-style-type: none"> • Klasa produktu Monitor LCD /LCD-TV/ LED • Producent Dell • Format ekranu monitora standardowy • Przekątna ekranu 17 cali • Wielkość plamki 0,264 mm • Typ panela LCD TFT TN • Technologia podświetlenia CCFL • Matryca "błyszcząca" (glare) Nie • Nakładka dotykowa na ekran Nie • Zalecana rozdzielczość obrazu 1280 x 1024 pikseli • Częst. odświeżania przy zalecanej rozdzielczości 60 Hz 	3
		<p>Evolis Primacy (z czytnikiem stykowym i zbliżeniowym)</p> <ul style="list-style-type: none"> • Feeder capacity: 100 cards (0.76 mm - 30 mil) • Output hopper capacity: 100 cards (0.76 mm - 30 mil) • Reject tray: 30 cards (0.76 mm - 30 mil) • Card thickness: 0.25 to 1.25 mm (10 to 50 mil), gauge adjustment (0.25mm / 10 mil cards for monochrome printing only) • Types of cards: Types of cards : All PVC, Composite PVC cards, PET, RPET, ABS1 and special varnished1 cards • Card format ISO CR80 - ISO 7810 (53.98mm x 85.60 mm) 	3
Serwery aplikacyjne IdM			

1.	COO		Ilość
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 2 RAM – 8 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 50 GB vNIC 1- 1 adres IP 	2
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 6 RAM – 39 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 100 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – S: 10 GB (nie wykorzystywany) vNIC 1- 1 adres IP 	2
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 4 RAM – 4 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 50 GB vNIC 1- 1 adres IP 	2
2.	ZCOO		Ilość
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 2 RAM – 8 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 50 GB vNIC 1 - 1 adres IP 	1
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 6 RAM – 32 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 100 GB vNIC 1- 1 adres IP 	1
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 4 RAM – 4 GB SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 50 GB vNIC 1- 1 adres IP 	2
Urządzenia sieciowe			
1.	COO		Ilość
	Huawei S5300 Series Ethernet Switch	<ul style="list-style-type: none"> S5328C-EI-24S Mainframe (24 100/1000Base-X,4 Combo GE (10/100/1000 BASE-T), Chassis,Dual Slots of power, Without Flexible Card and Power Module) 2-Port 10GE SFP+ Optical Interface Card (jedna na przełącznik) AC Power Module (dwa na przełącznik) 	2
2.	ZCOO		Ilość
	Huawei S5300 Series Ethernet Switch	<ul style="list-style-type: none"> S5328C-EI-24S Mainframe(24 100/1000Base-X,4 Combo GE(10/100/1000 BASE-T),Chassis,Dual Slots of power, Without Flexible Card and Power Module) 2-Port 10GE SFP+ Optical Interface Card (jedna na przełącznik) AC Power Module (dwa na przełącznik) 	1
Serwer skanujący Nessus			
1.	COO		Ilość
	serwer wirtualny	<ul style="list-style-type: none"> liczba rdzeni – 4 RAM – 4 GB 	1

	<ul style="list-style-type: none"> • SCSI Controller 0 – LSI Logic SAS – HDD 1 (System) – C: 40 GB • SCSI Controller 0 – LSI Logic SAS – HDD 2 (Dane) – D: 50 GB • vNIC 1- 1 adres IP 	
--	--	--

Tabela: Konfiguracja sprzętowa SZT

3. Wykorzystywane konektory

System Oracle Identity Manager w wersji 11G uruchomiony u Zamawiającego, dostarczony jest z następującymi gotowymi Konektorami:

Nazwa Konektora	Opis
Database Applications Table	Współpraca z bazami danych: MS SQL, IBM DB2, Oracle. Konektor umożliwia wykonywanie operacji na tabelach danych.
Database User Management	Współpraca z bazami danych: MS SQL, IBM DB2, Oracle, Informix. Konektor umożliwia wykonywanie operacji na kontach bazodanowych.
IBM RACF Advanced	Konektor obsługuje systemy IBM RACF.
Microsoft Active Directory Management	Konektor obsługuje operacje na Użytkownikach i grupach Katalogu AD (Active Directory).
Microsoft Exchange	Konektor umożliwia tworzenie i usuwanie Kont na systemie poczty MS Exchange.
Unix	Współpraca z HP-UX, AIX, Solaris.
SAP	Konektor, a w zasadzie rodzina Konektorów umożliwia operacje na Kontach w systemach SAP oraz pobieranie informacji z systemów SAP HR m.in. z wykorzystaniem SAP CUA będącego składnikiem systemu SAP za pomocą, którego tworzone są Konta w systemach SAP oraz przypisywane role SAP do pracowników Zamawiającego.
Sun Java System Directory	Konektor do obsługi katalogu LDAP Sun Java One.

Tabela: Wykaz Konektorów

Oracle Identity Manager (OIM) użytkowany u Zamawiającego posiada wbudowany Konektor do obsługi plików płaskich (CSV). Konektor umożliwia pobieranie danych do SZT z odpowiednio przygotowanych plików źródłowych. Istnieje również gotowy Webservice w OIM umożliwiający zarządzanie Tożsamościami polegające na ich tworzeniu, modyfikowaniu i usuwaniu. Dodatkowo na potrzeby Zamawiającego w ramach Wdrożenia SZT wytworzone zostały następujące Konektory:

Nazwa Konektora	Opis
AuthAPI	Konektor w technologii ICF odpowiadający za połączenia z bazą AuthAPI opartą o MS SQL.
EDA	Konektor w technologii ICF odpowiadający za połączenia z bazą EDA opartą o MS SQL Server.

Tabela: Dedykowane Konektory

Konektory zostały szczegółowo opisane w dokumencie Szczegółowy opis działania obecnego SZT.

4. Funkcjonalności biznesowe dostępne w SZT

Obecnie użytkowany u Zamawiającego SZT, każdemu Użytkownikowi umożliwia podgląd swoich danych i uprawnień do systemów informatycznych oraz odnowienie Certyfikatów niezbędnych do pracy w systemach informatycznych, a w przypadku zablokowania Karty elektronicznej umożliwia jej odblokowanie bez konieczności wysyłania jej do administratora (funkcjonalność nie obejmuje możliwości odblokowania Kart elektronicznych PKZ). W przypadku Logowania do Domeny AD przy użyciu loginu i Hasła lub Karty elektronicznej pracownik może sam zmienić Hasło za pomocą odpowiedzi na pytania kontrolne ustawiane przy pierwszym Logowaniu do SZT. Poniżej wykaz istotnych funkcji biznesowych dostępnych w obecnym SZT:

1. pierwsze Logowanie do SZT - rejestracja przez Użytkownika odpowiedzi na pytania mające w przypadku konieczności odblokowania Konta pomóc w weryfikacji jego Tożsamości;
2. aktywacja Karty elektronicznej w SZT;
3. możliwość zmiany kodu PIN w SZT i ponownej aktywacji Karty elektronicznej w SZT;
4. możliwość wystawienia wniosku/zlecenia:
 - 1) wniosek o nadanie uprawnień,
 - 2) wniosek o zmianę uprawnień,
 - 3) wniosek o likwidację Kont i Zasobów,
 - 4) wniosek o natychmiastowe odebranie uprawnień,
 - 5) wniosek o natychmiastowe przywrócenie uprawnień,
 - 6) wniosek o zablokowanie dostępu z powodu długotrwałej nieobecności,
 - 7) wniosek o odblokowanie dostępu z powodu powrotu po długotrwałej nieobecności,
 - 8) wniosek o zarejestrowanie Pracownika zewnętrznego,
 - 9) wniosek o zarejestrowanie Pracownika zewnętrznego – firma,
 - 10) wniosek o wyrejestrowanie Pracownika zewnętrznego,
 - 11) wniosek o zmianę okresu zatrudnienia Pracownika zewnętrznego,
 - 12) wniosek o zmianę danych Pracownika zewnętrznego,
 - 13) wniosek o zmianę sposobu logowania,
 - 14) wniosek o zmianę sposobu logowania dla użytkowników VIP,
 - 15) wniosek o zmianę Hasła,
 - 16) wniosek o zmianę hasła do stacji roboczej,
 - 17) wniosek o przypisanie roli systemowej IdM,
 - 18) wniosek o odebranie roli systemowej IdM,
 - 19) wniosek o zawieszenie uprawnień w RMA/wniosek o przywrócenie uprawnień w RMA;
5. rejestrowanie wniosku/zlecenia, spośród zdefiniowanych w systemie, ze wskazaniem:
 - 1) Beneficjenta (zgodnie z strukturą organizacyjną),
 - 2) systemów informatycznych (zintegrowanych z SZT),
 - 3) wnioskowanych ról (wprowadzone do SZT uprawnienia do systemów zintegrowanych- definiowanie ról realizowane poza SZT, ale zgodne ze Standardami IT ZUS),
 - 4) uzasadnienia z terminem wejścia w życie wnioskowanej zmiany;
6. automatyczny podział wniosku na zadania/zlecenia z uwagi na:
 - 1) wielu Beneficjentów, wiele systemów informatycznych,
 - 2) uprawnienia Akceptantów (ilość wniosków odpowiada liczbie Grup Akceptantów);
7. podgląd wniosku, podgląd uprawnień, podgląd Zasobów;
8. wycofanie wniosku;
9. cedowanie uprawnień tj. udzielenie pełnomocnictwa w SZT;
10. podgląd danych, Zasobów i uprawnień;
11. zarządzanie zdjęciami – dodawanie, usuwanie;
12. obsługa zadania/zlecenia:
 - 1) udostępnianie Zasobu,
 - 2) modyfikowanie udostępnionego Zasobu,

- 3) anulowanie udostępnionego Zasobu,
- 4) wyłączanie udostępnianego Zasobu,
- 5) włączanie udostępnianego Zasobu);
13. obsługa odrzuconych zadań/zleceń;
14. obsługa wniosków o nadanie, zmianę bądź usunięcie uprawnień dla systemu RMA;
15. odnowienie Certyfikatu w SZT;
16. automatyczne reagowanie SZT na wystawione w SAP HR Zdarzeń kadrowych (w zależności od typu zdarzenia może to być: założenie/ blokowanie/ likwidowanie Konta, nadawanie/ blokowanie/ usuwanie uprawnień);
17. reset Hasła do repozytorium AuthAPI;
18. podgląd przez Użytkowników swoich danych i uprawnień;
19. możliwość zmiany danych przez Użytkowników w zakresie numeru telefonu i biura;
20. samodzielne odblokowanie Konta/Karty elektronicznej (z wyłączeniem Karty elektronicznej PKZ) z wykorzystaniem odpowiedzi ustawionych podczas pierwszego Logowania.

Szczegółowy opis działających funkcjonalności biznesowych SZT działającego u Zamawiającego znajduje się w dokumencie Szczegółowy opis działania obecnego SZT.

5. Zasoby obsługiwane poprzez SZT

W SZT obsługiwane są następujące Zasoby:

Lp.	Nazwa zasobu	Dodatkowe informacje
1.	Katalog AD	Liczba zdefiniowanych grup: 9979.
2.	SWEZ	Liczba modułów, do których można wnioskować w ramach Zasobu: 14. Liczba ról, o które można wnioskować w ramach modułów znajdujących się w Zasobie: 302 079 (w ramach 36 zdefiniowanych systemów). Liczba Kont aktywnych dla 1 Użytkownika: więcej niż 1.
3.	Katalogu KSI	Liczba aplikacji, do których można wnioskować w ramach Zasobu: 83. Liczba ról, o które można wnioskować w ramach aplikacji znajdujących się w Zasobie: 636. Liczba Kont aktywnych dla 1 Użytkownika: 1, więcej niż 1 w przypadku wielozatrudnienia.
4.	AuthAPI	Liczba aplikacji autorskich, do których można wnioskować w ramach Zasobu: 49. Liczba ról, o które można wnioskować w ramach aplikacji znajdujących się w Zasobie: 243. Liczba Kont aktywnych dla 1 Użytkownika: 1.
5.	EDA	Liczba aplikacji, do których można wnioskować w ramach Zasobu: 4. Liczba ról, o które można wnioskować w ramach aplikacji znajdujących się w Zasobie: 32. Liczba Kont aktywnych dla 1 Użytkownika: 1.
6.	Karta elektroniczna	Aktywna Karta elektroniczna dla 1 Użytkownika: 1.
7.	Certyfikat AD	Aktywny Certyfikat dla 1 Użytkownika: 1.
8.	Certyfikat KSI	Aktywny Certyfikat dla 1 Użytkownika: 1, więcej niż 1 w przypadku oddelegowania lub wielozatrudnienia.
9.	Certyfikat ENC	Aktywny Certyfikat dla Tożsamości: 1.
10.	BMC KT	Liczba ról, o które można wnioskować w Zasobie: 3, Liczba Kont aktywnych dla 1 Użytkownika: 1.
11.	BMC KU	Liczba ról, o które można wnioskować w Zasobie: 2. Liczba Kont aktywnych dla 1 Użytkownika: 1.
12.	PKZ	Liczba ról, o które można wnioskować w Zasobie: 1.

		Liczba Kont aktywnych dla 1 Użytkownika: 1.
13.	ARIS	Liczba ról, o które można wnioskować w Zasobie: 2. Liczba Kont aktywnych dla 1 Użytkownika: 1.
14.	RMA	Liczba ról, o które można wnioskować w Zasobie: 30. Liczba Kont aktywnych dla 1 Użytkownika: więcej niż 1.
15.	eDOK	Liczba ról, o które można wnioskować w zasobie: 3 Liczba Kont aktywnych dla 1 Użytkownika: więcej niż 1.
16.	Emir	Liczba ról, o które można wnioskować w zasobie: 34 Liczba Kont aktywnych dla 1 Użytkownika: więcej niż 1.

Liczba modułów/aplikacji/grup/ról podana w powyższej tabeli zmienia się dynamicznie. Powyższe dane prezentują stan na dzień 08.05.2018 r.

III. Wstępne wymagania techniczne dla SZT

1. W przypadku zaoferowania systemu wymagającego większej mocy obliczeniowej i liczby licencji, niż obecnie wykorzystywane/posiadane przez Zamawiającego, Wykonawca dostarczy Sprzęt oraz niezbędne oprogramowanie systemowo-narzędziowe i licencje (w tym systemowe) umożliwiające ich uruchomienie i eksploatację. Dotyczy to wszystkich środowisk SZT.
2. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie zapewnić Zamawiającemu dostęp do strony producenta oprogramowania systemowo-narzędziowego dostarczonego wraz ze Sprzętem w celu możliwości bezpośredniego zgłoszenia przez Zamawiającego Błędu związanego z użytkowanym Oprogramowaniem oraz pobrania Pakietów instalacyjnych z nowymi lub poprawionymi wersjami tego Oprogramowania wraz z dokumentacją techniczną.
3. W przypadku zaoferowania przez Wykonawcę rozwiązania wymagającego doposażenia/rozbudowy istniejącej infrastruktury wymagane jest zachowanie kompatybilności dostarczonych elementów z wykorzystywaną przez Zamawiającego dotychczas infrastrukturą. Zamawiający zakłada, że ewentualny wzrost wymagań dotyczący parametrów systemu i liczby licencji będzie optymalny kosztowo i uzasadniony korzyściami dla Zamawiającego.
4. Wykonawca zapewni współpracę zaoferowanego rozwiązania z systemem backupowym posiadanym przez Zamawiającego (EMC Networker) zapewniającym niezależnie kopie systemów operacyjnych oraz baz danych, zgodnie z polityką wykonywania kopii bezpieczeństwa obowiązującą u Zamawiającego.
5. W przypadku zaoferowania rozwiązania opartego o licencje Oracle, dostępne przez Zamawiającego licencje powinny ulec przemapowaniu przez Wykonawcę do wdrażanej wersji, a w razie konieczności uzupełnione.
6. W przypadku dostarczenia rozwiązania równoważnego Wykonawca dostarczy Zamawiającemu wszystkie licencje na Oprogramowanie wymagane w ramach realizacji przedmiotu zamówienia.

Wymagania funkcjonalne

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WF-0001	SZT musi umożliwiać parametryzację przez administratorów formatek ekranowych przy użyciu graficznego narzędzia.
DZU/01/2016/ZP/1-WF-0002	SZT musi umożliwiać zrealizowanie funkcjonalności Single Sign-on dla Użytkowników końcowych i operatorów systemu.
DZU/01/2016/ZP/1-WF-0003	SZT musi posiadać wewnętrzne mechanizmy archiwizacji lub usuwania rekordów historycznych lub niepotrzebnych bez względu na ich status.
DZU/01/2016/ZP/1-WF-0004	SZT musi umożliwić tworzenie historii posiadanych uprawnień,

	w tym znakowanie datą uprawnień w bazie SZT dla każdego systemu.
DZU/01/2016/ZP/1-WF-0005	SZT musi umożliwić wyłączenie ról globalnie i usunięcie ich z Tożsamości w SZT z jednoczesnym odpisaniem tej informacji w bazie SZT (z zachowaniem wymagania DZU/01/2016/ZP/1-WF-0004) przy Tożsamościach celem późniejszego raportowania (role wycofane odgórnie z użytku) oraz przeniesienie tej informacji do systemów źródłowych celem ich usunięcia z Kont Użytkowników.
DZU/01/2016/ZP/1-WF-0006	SZT musi umożliwiać konsolidację i wersjonowanie ról w zakresie Tożsamości.
DZU/01/2016/ZP/1-WF-0007	SZT musi uniemożliwiać wnioskowanie o role już posiadane dla danej Tożsamości, z uwzględnieniem daty jej ważności jeśli taka występuje.
DZU/01/2016/ZP/1-WF-0008	SZT musi umożliwić wyświetlanie w SZT w wykazie posiadanych uprawnień wszystkich aktualnych ról w danym Zasobie.
DZU/01/2016/ZP/1-WF-0009	SZT musi umożliwiać wyłączenie z procesu wnioskowania wskazanych ról.
DZU/01/2016/ZP/1-WF-0010	SZT musi umożliwiać analizę uprawnień wszystkich Tożsamości pod kątem wydziałów/ stanowisk/ Zasobów/ aplikacji, co pozwoli na definiowanie i wdrażanie produkcyjnie nowych zestawów minimalnych uprawnień w kontekście wydziałów/ stanowisk/ Zasobów/ aplikacji powiązanych z odbieranymi Zdarzeniami kadrowymi.
DZU/01/2016/ZP/1-WF-0011	SZT musi umożliwić przypisanie Tożsamości do następujących profili: <ol style="list-style-type: none"> 1) Pracownik stały, 2) Pracownik zewnętrzny, 3) Pracownik zewnętrzny – firma, 4) Konto techniczne, 5) Konto testowe, 6) Konto szkoleniowe, 7) innych, zdefiniowanych przez Zamawiającego w trakcie trwania Umowy.
DZU/01/2016/ZP/1-WF-0012	SZT musi umożliwiać podanie jednoznacznego zestawu reguł dotyczącego łączenia ról (np. w przypadku, gdy aplikacja lub system posiada role A_ROLA1, A_ROLA2, A_ROLA3 zabronione jest posiadanie przez Użytkownika równocześnie ról A_ROLA1 oraz A_ROLA2). System na podstawie zdefiniowanych reguł powinien tylko informować Użytkownika, iż wnioskuje o nadanie uprawnień tzw. wrażliwych (uprawnienia wrażliwe to wskazane przez Zamawiającego role w ramach Zasobów, o które może wnioskować uprawniony Użytkownik SZT, a ich posiadanie przez Użytkowników jest szczególnie monitorowane), a następnie kierować taki wniosek do akceptacji zgodnie ze zdefiniowanymi przez Zamawiającego regułami.
DZU/01/2016/ZP/1-WF-0013	SZT musi umożliwiać mapowanie ról samego SZT zgodnie z funkcjonującymi u Zamawiającego Standardami IT ZUS poprzez stworzenie i przypisanie następujących ról i funkcji w ramach: <ol style="list-style-type: none"> 1) Zasobu, 2) struktury organizacyjnej,

	3) pełnionej funkcji u Zamawiającego.
DZU/01/2016/ZP/1-WF-0014	Interfejs SZT musi umożliwiać konfigurację zakresu i sposobu prezentacji informacji wyświetlanych w poszczególnych oknach.
DZU/01/2016/ZP/1-WF-0015	Interfejs SZT musi umożliwić filtrowanie zleceń (wniosków) wystawionych oraz zleceń (wniosków) do realizacji po filtrach określonych przez Zamawiającego.
DZU/01/2016/ZP/1-WF-0016	Interfejs SZT musi umożliwić z poziomu SZT odbieranie uprawnień wszystkim Użytkownikom w danym Zasobie z jednoczesnym odpisaniem uzasadnienia w bazie SZT przy danej Tożsamości.
DZU/01/2016/ZP/1-WF-0017	Interfejs SZT musi umożliwić prezentowanie opisów ról w systemie wnioskowania.
DZU/01/2016/ZP/1-WF-0018	Interfejs SZT musi umożliwić definiowanie filtrów na podstawie danych zapisanych w bazie danych SZT.
DZU/01/2016/ZP/1-WF-0019	Interfejs SZT musi zapewnić wyświetlanie przełożonym tylko pracowników zatrudnionych (pracownicy znajdujący się w tzw. poczekalni nie powinni być widoczni – brak możliwości składania jakichkolwiek wniosków na takie osoby).
DZU/01/2016/ZP/1-WF-0020	Interfejs SZT musi umożliwić implementację obsługi nowych typów Zdarzeń kadrowych przez Zamawiającego w oparciu o procesy zdefiniowane w systemie.
DZU/01/2016/ZP/1-WF-0021	Interfejs SZT musi umożliwić wycofanie wprowadzonego Zdarzenia kadrowego z kolejki przetwarzania (błądny IDOC);
DZU/01/2016/ZP/1-WF-0022	Interfejs SZT musi umożliwić obsługę wielozatrudnienia na Kontach Użytkowników tj. obsługę Tożsamości, które u Zamawiającego posiadają więcej niż jedną umowę o pracę i świadczyć mogą równocześnie stosunek pracy w różnych komórkach organizacyjnych w ramach jednej Jednostki organizacyjnej lub w różnych Jednostkach organizacyjnych w związku z czym posiadają więcej niż jednego przełożonego, z których każdy powinien mieć możliwość równoczesnego wnioskowania o nadanie/ zmianę/ odebranie uprawnień w ramach swojej właściwości.
DZU/01/2016/ZP/1-WF-0023	Interfejs SZT musi umożliwić obsługę zmiany atrybutów Tożsamości, tj. imię, nazwisko (szczegółowy zakres danych możliwych do zmiany dla Tożsamości, zostanie przekazany Wykonawcy w Zleceniu).
DZU/01/2016/ZP/1-WF-0024	Interfejs SZT musi umożliwić monitorowanie i informowanie wskazanej grupy o nadawaniu/ posiadaniu uprawnień tzw. wrażliwych z jednoczesną możliwością odebrania przez nią tych uprawnień, z koniecznym uzasadnieniem widocznym na Koncie Wnioskującego oraz informacją przy danej Tożsamości, której to dotyczy.
DZU/01/2016/ZP/1-WF-0025	Interfejs SZT musi umożliwić zmianę tworzenia procesów wnioskowania przez Zamawiającego – w systemie ścieżka wnioskowania (procesu) powinna być możliwa do modyfikowania przez Zamawiającego na etapie użytkownika systemu.
DZU/01/2016/ZP/1-WF-0026	Interfejs SZT musi umożliwić obsługę numeru MPK – Miejsce Powstania Kosztu (opis i skrót) w zakresie raportowym.
DZU/01/2016/ZP/1-WF-0027	Interfejs SZT musi umożliwić wnioskowanie o uprawnienia w zakresie wszystkich systemów eksploatowanych przez Zamawiającego.

DZU/01/2016/ZP/1-WF-0028	Interfejs SZT musi umożliwić ciągłe monitorowanie działania serwerów i bazy, zapis historyczny parametrów, analizę systemu pod względem dostępnych patchy, występujących Błędów i niedostępności za pomocą dostarczonego, dedykowanego narzędzia.
DZU/01/2016/ZP/1-WF-0029	Interfejs SZT ma zapewnić zwracanie komunikatów o błędach systemowych np. 500 itp., w formie zrozumiałego i przyjaznego komunikatu dla Użytkownika zgodnie z zatwierdzoną treścią przez Zamawiającego.
DZU/01/2016/ZP/1-WF-0030	Interfejs SZT musi umożliwić weryfikację otrzymania przez Użytkownika e-mail z loginem i Hasłem dla poszczególnych systemów oraz ponowienie jego wysłania.
DZU/01/2016/ZP/1-WF-0031	Interfejs SZT musi umożliwić tworzenie szablonów powiadomień i definiowanie adresatów tych powiadomień.
DZU/01/2016/ZP/1-WF-0032	Interfejs SZT musi umożliwić wysyłanie e-maili do Wnioskodawców z informacją o realizacji, niepowodzeniu, odrzuceniu wniosku zawierającego komplet informacji np. kogo dotyczyło zlecenie (Beneficjent), jego numer, jakiego zasobu/roli, powód odrzucenia.
DZU/01/2016/ZP/1-WF-0033	Interfejs SZT musi umożliwić przypisanie przy poszczególnych aplikacjach/roli/Zasobie/koncie technicznemu właściciela biznesowego oraz ich prezentacja na etapie wnioskowania czy obsługi wniosku.
DZU/01/2016/ZP/1-WF-0034	Interfejs SZT musi umożliwić modyfikację obsługi wniosku o system RMA – polegającą np. na: dokument tworzony i drukowany powinien być dynamicznie z uwzględnieniem ilości zawnioskowanych ról (brak pustych stron), możliwość dodania checkboxów z „nadaj uprawnienia do wszystkich jednostek istniejących w ramach Oddziału”.
DZU/01/2016/ZP/1-WF-0035	Interfejs SZT musi umożliwić zapisanie zlecenia na poszczególnych etapach realizacji.
DZU/01/2016/ZP/1-WF-0036	Interfejs SZT musi umożliwić automatyczne (tj. bez ingerencji Użytkownika) ustawianie dat „od-do”, z uwzględnieniem profilu Tożsamości, w systemach, dla których należy wskazać ważność ról np. SWEZ z możliwością ich zmiany podczas składania wniosku.
DZU/01/2016/ZP/1-WF-0037	Interfejs SZT musi umożliwić usuwanie uprawnień dla kilku Użytkowników na raz na podstawie jednego zlecenia (wniosku).
DZU/01/2016/ZP/1-WF-0038	Interfejs SZT musi umożliwić przypisanie do jednej wnioskowanej roli kilku jednostek organizacyjnych.
DZU/01/2016/ZP/1-WF-0039	Interfejs SZT musi umożliwić wprowadzenie ograniczenia ilości ról o jakie można zawnioskować w jednym zleceniu głównym (uniemożliwienie błędnego wystawienia zlecenia na nadanie uprawnień do wszystkich ról istniejących w ramach Zasobu oraz pozwalające na swobodne przeprocesowanie uprawnień za pośrednictwem Konektora do danego systemu).
DZU/01/2016/ZP/1-WF-0040	Interfejs SZT musi umożliwić sygnalizowanie użytkownikowi np. w formie komunikatu o zdefiniowanej treści, iż wnioskuje o dużą ilość/wszystkie uprawnienia w zakresie jednego Zasobu (np. Katalog AD) – powyżej definiowanego przez Zamawiającego parametru.
DZU/01/2016/ZP/1-WF-0041	Interfejs SZT musi umożliwić wnioskowanie poprzez wybór roli,

	która automatycznie będzie przypisywana do odpowiedniego Zasobu, zgodnie z konfiguracją oprogramowania możliwą do zmodyfikowania przez Zamawiającego z poziomu interfejsu Użytkownika dostarczonego rozwiązania.
DZU/01/2016/ZP/1-WF-0042	Interfejs SZT musi umożliwić tworzenie grup uprawnień zawierających kilka, kilkanaście uprawnień w zakresie różnych aplikacji, systemów możliwych do zawnioskowania w odniesieniu do pełnionej funkcji/ zajmowanego stanowiska/ komórki organizacyjnej w organizacji Zamawiającego (np. tworzenie minimalnych uprawnień dla grup pracowników w kontekście komórki organizacyjnej tj. wydziału, departamentu, zajmowanego stanowiska). Tworzenie grup powinno być możliwe na każdym poziomie organizacji z możliwością wyboru poziomu ich tworzenia (centralnie lub lokalnie).
DZU/01/2016/ZP/1-WF-0043	Interfejs SZT musi umożliwić wnioskowanie oparte na metodzie porównania z grupą pracowników z tego samego obszaru biznesowego (np. dla grup pracowników w kontekście komórki organizacyjnej tj. wydziału, departamentu, zajmowanego stanowiska).
DZU/01/2016/ZP/1-WF-0044	Interfejs SZT musi umożliwić, aby tworzone grupy uprawnień były możliwe do wyboru przez Wnioskującego w zależności od funkcji/ zajmowanego stanowiska/ komórki organizacyjnej w organizacji Zamawiającego.
DZU/01/2016/ZP/1-WF-0045	Interfejs SZT musi umożliwić na bieżąco (według potrzeb) zmianę minimalnego zakresu uprawnień dla nowo zatrudnionych pracowników w ramach różnych aplikacji i systemów.
DZU/01/2016/ZP/1-WF-0046	Interfejs SZT musi umożliwić sygnalizowanie, iż wnioskowane są uprawnienia niezgodne z zasadami łączenia ról.
DZU/01/2016/ZP/1-WF-0047	Interfejs SZT musi umożliwić stworzenie nowego wniosku na podstawie istniejącego wniosku niezależnie od jego statusu (np. zaakceptowany, odrzucony) w celu procedowania.
DZU/01/2016/ZP/1-WF-0048	Interfejs SZT musi umożliwić zwrócenie wniosku do poprawy.
DZU/01/2016/ZP/1-WF-0049	Interfejs SZT musi umożliwić wnioskowanie o role wrażliwe z jednoczesnym sygnalizowaniem tego faktu.
DZU/01/2016/ZP/1-WF-0050	Interfejs SZT musi umożliwić wnioskowanie o uprawnienia do systemów obsługiwanych obecnie poza SZT np. narzędzia pomocnicze, Zasoby, wnioskowanie o Konta na serwerach, VPN, itp.
DZU/01/2016/ZP/1-WF-0051	Interfejs SZT musi umożliwić parametryzację sposobu i zakresu danych wyświetlanych w interfejsie Użytkownika SZT np. Oddział/ Zasób (aplikacja)/ Wnioskodawca/ Beneficjent/ Nazwa składanego wniosku w procesie akceptacji.
DZU/01/2016/ZP/1-WF-0052	Interfejs SZT musi umożliwić odpisanie w zleceniu nadrzędnym informacji o wszystkich zleceniach podrzędnych utworzonych na jego podstawie, na zlecenia podrzędne powinno się przenieść uzasadnienie ze zlecenia nadrzędnego.
DZU/01/2016/ZP/1-WF-0053	Interfejs SZT musi umożliwić obsługę w procesie wnioskowania Dodatkowego kroku aprobaty, który może być przypisany do roli albo Konta w aplikacji/ systemie.
DZU/01/2016/ZP/1-WF-0054	Interfejs SZT musi zapewnić, że w przypadku, gdy utworzone zlecenie będzie zawierać zarówno role/ Konta, które

	<p>nie wymagają Dodatkowego kroku aprobaty jak i takie, które tej aprobaty wymagają, wówczas SZT utworzy zlecenia podrzędne:</p> <ol style="list-style-type: none"> 1) wymagające Dodatkowego kroku aprobaty – na każdą z Grup Akceptantów osobne zlecenie, 2) nie wymagające Dodatkowego kroku aprobaty – do automatycznego zatwierdzenia, 3) informacja o numerach zleceń podrzędnych będzie umieszczana w zleceniu. Każde ze zleceń powinno być realizowane niezależnie. W przypadku, gdy zlecenie zostanie odrzucone przez Akceptanta, przyczyny odrzucenia powinny zostać umieszczone w zleceniu.
DZU/01/2016/ZP/1-WF-0055	Interfejs SZT musi zapewnić, że Dodatkowy krok aprobaty nie będzie wymagana w przypadku odebrania uprawnień.
DZU/01/2016/ZP/1-WF-0056	Interfejs SZT musi umożliwić, że rolę Akceptanta można przypisać na wniosek przełożonego w SZT. Role systemowe w SZT będą podlegały aprobacie zgodnie z obowiązującymi regułami Zamawiającego.
DZU/01/2016/ZP/1-WF-0057	Interfejs SZT musi umożliwić ustanowienie pełnomocnika niezależnie od struktury organizacyjnej, poprzez zmianę filtrów przez samego wnioskodawcę na etapie jego przydzielania tzn. system przy ustawianiu Wnioskodawcy powinien wskazywać możliwe osoby zgodnie z podległością. Po zdjęciu automatycznie ustawionego filtru powinien umożliwić udzielić pełnomocnictwa osobie w ramach struktury swojej Jednostki organizacyjnej. Administrator SZT w uzasadnionych wypadkach powinien mieć możliwość ustanowienia pełnomocnictwa w ramach całego Zakładu.
DZU/01/2016/ZP/1-WF-0058	<p>Interfejs SZT musi umożliwić obsługę oddelegowań pomiędzy dwoma Jednostkami organizacyjnymi (oddelegowanie między Jednostkami organizacyjnymi nie jest rejestrowane w SAP HR) w następujący sposób:</p> <ol style="list-style-type: none"> 1) W SZT powinien znajdować się port umożliwiający osobom zarządzającym SZT obsługę: „Oddelegowanie pracownika” oraz „Powrót pracownika z oddelegowania”. 2) Wykonanie obsługi oddelegowania przez osoby zarządzające SZT – powinno odpisać się w Tożsamości pracownika np. być widoczne w treści zleceń. 3) Do obsługi „Oddelegowania pracownika” powinny wystarczyć następujące dane pracownika oddelegowanego: imię i nazwisko, nr osobowy, pesel, nr komórki organizacyjnej, do której pracownik jest przenoszony, stanowisko jakie będzie posiadał w nowej komórce. 4) Do obsługi „Powrót pracownika z oddelegowania” powinny wystarczyć dane pracownika: imię i nazwisko, nr osobowy, pesel, nr komórki organizacyjnej, do której pracownik wraca, stanowisko jakie zajmuje w komórce do której wraca. 5) Na podstawie przygotowanego portu służącego do zarejestrowania „Oddelegowania pracownika” Tożsamość pracownika powinna zostać przeniesiona automatycznie z komórki macierzystej do nowej komórki.

	6) Na podstawie przygotowanego portu służącego do zarejestrowania „Powrotu z oddelegowania” Tożsamość pracownika powinna zostać przeniesiona automatycznie z nowej komórki do komórki macierzystej.
DZU/01/2016/ZP/1-WF-0059	System musi posiadać możliwość eksportu i importu danych.
DZU/01/2016/ZP/1-WF-0060	System musi umożliwiać administratorowi definiowanie zakresu wymiany danych.
DZU/01/2016/ZP/1-WF-0081	Interfejs SZT musi posiadać zabezpieczenia przed okresową niedostępnością integrowanych Zasobów tj. umożliwiać wznowienie działania w momencie przywrócenia działania tego Zasobu np. w przypadku procesowania nadawania uprawnień do Katalogu KSI, w przypadku jego niedostępności, system SZT powinien odłożyć nadawanie uprawnień do momentu wznowienia jego działania jednocześnie zachowując kolejność wystawionych wniosków.
DZU/01/2016/ZP/1-WF-0082	Interfejs SZT musi umożliwić modyfikowanie przez Zamawiającego walidacji tworzenia Zasobów tj. zależności ich powstawania w procesie zmian kadrowych (dependencja między Zasobami).

Wymagania przejściowe

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0001	System musi umożliwiać wymianę danych w obu kierunkach (export i import danych).
DZU/01/2016/ZP/1-WP-0002	System musi mieć możliwość automatycznej wymiany danych w zadanych odstępach czasu (np. co noc, lub na koniec tygodnia) oraz jednorazowej inicjowanej przez administratora.
DZU/01/2016/ZP/1-WP-0003	System musi zapewniać ochronę swoich Zasobów przed nieautoryzowanym dostępem z zewnątrz i wewnątrz systemu.
DZU/01/2016/ZP/1-WP-0004	System musi zapewniać możliwość separacji danych o elementach konfiguracji w taki sposób, aby wyznaczone grupy Użytkowników (np. Oddziały) miały dostęp wyłącznie do danych przeznaczonych dla tej grupy, dotyczy to zarówno modyfikacji jak i widoczności danych.
DZU/01/2016/ZP/1-WP-0005	Uwierzytelnienie Użytkowników musi odbywać się przy użyciu identyfikatora Użytkownika (tzw. login'u) i Hasła pobieranego z Active Directory albo Certyfikatu zawartego na Karcie elektronicznej. Wymienione obie metody muszą być spełnione, ale nie jednocześnie tzn. w zależności od konfiguracji Użytkownik posiadający Konto w AD musi posiadać możliwość Uwierzytelnienia za pomocą loginu/Hasła lub odpowiedniego Certyfikatu na Karcie elektronicznej.
DZU/01/2016/ZP/1-WP-0006	System nie może wyświetlać Haseł na ekranie podczas ich wprowadzania przez Użytkownika.
DZU/01/2016/ZP/1-WP-0007	Hasła Użytkowników nie mogą być przekazywane przez sieć LAN i WAN w postaci jawnej.
DZU/01/2016/ZP/1-WP-0008	System musi rejestrować każdą udaną i nieudaną próbę dostępu do systemu.
DZU/01/2016/ZP/1-WP-0009	System musi obsługiwać mechanizm auditingu, czyli pozwalać

	na zapis historii tworzenia i zmian danych wraz z informacją kto, kiedy i jakie dane zmieniał lub wprowadzał, dla wskazanego przez administratora zakresu danych, a także umożliwiać raportowanie tych danych. Informacje te muszą być udostępniane do odczytu, w taki sposób by nawet osoba niezaangażowana w administrowanie systemem SZT mogła prześledzić poszczególne zdarzenia, jakie miały miejsce.
DZU/01/2016/ZP/1-WP-0010	Administrowanie infrastrukturą techniczną musi być scentralizowane. Administratorzy systemu muszą mieć możliwość nadzorowania i sprawnego zarządzania całym systemem. Role i uprawnienia do SZT muszą być zdefiniowane i raportowane.
DZU/01/2016/ZP/1-WP-0011	Maksymalna liczba aktywnych Użytkowników systemu: 50 000.
DZU/01/2016/ZP/1-WP-0012	Przewidywana liczba Tożsamości w systemie: do 85 000.
DZU/01/2016/ZP/1-WP-0013	Maksymalna liczba ról zmienianych jednym wnioskiem: 1 000.

Wymagania pozafunkcjonalne

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WNF-0001	SZT musi być oparty o bazę danych SQL, przy czym dopuszcza się rozwiązania hybrydowe, gdzie SZT oparty będzie zarówno o bazę danych (np. dla raportowania i wniosków) oraz usługę katalogową (np. dla repozytorium Tożsamości).
DZU/01/2016/ZP/1-WNF-0002	Interfejs SZT musi wyświetlać daty w formacie zdefiniowanym przez uprawnionego do tego administratora.
DZU/01/2016/ZP/1-WNF-0003	Interfejs SZT musi umożliwiać nawigowanie pomiędzy elementami interfejsu użytkownika zarówno przy użyciu myszki jak i klawiatury.
DZU/01/2016/ZP/1-WNF-0004	Interfejs SZT musi umożliwiać wyświetlanie interfejsu Użytkownikowi w kontekście posiadanych przez niego uprawnień systemowych.
DZU/01/2016/ZP/1-WNF-0005	Interfejs SZT musi być ergonomiczny i zapewniać nie mniej niż: <ol style="list-style-type: none"> 1) rozszerzanie okien aplikacji, 2) dostosowanie ilości elementów wyświetlanych na stronie i stronicowanie, 3) jednolity format wprowadzanych typów danych np. daty wprowadzane dd-mm-rrrr.
DZU/01/2016/ZP/1-WNF-0006	Interfejs SZT musi umożliwiać zaznaczanie tekstu i kopiowanie we wszystkich elementach tekstowych.
DZU/01/2016/ZP/1-WNF-0007	Interfejs SZT musi umożliwić obsługę Kont Użytkowników z nazwiskiem kilkuczłonowym, w tym bez myślnika.
DZU/01/2016/ZP/1-WNF-0008	Interfejs SZT musi prezentować nazwę wniosku zgodną z nazewnictwem stosowanym u Zamawiającego.
DZU/01/2016/ZP/1-WNF-0009	Interfejs SZT musi obsługiwać przetwarzanie kilku Zdarzeń kadrowych wystawionych w SWEZ w tym samym dniu dla jednego pracownika (kolejkowanie);
DZU/01/2016/ZP/1-WNF-0010	Interfejs SZT musi umożliwić automatyczną autentykację na podstawie poświadczeń AD np. kerberos.
DZU/01/2016/ZP/1-WNF-0011	Interfejs SZT musi być kompatybilny ze wzorcem systemowo-narzędziowym eksploatowanym u Zamawiającego określonym

	Standardami IT ZUS.
DZU/01/2016/ZP/1-WNF-0012	Interfejs SZT musi umożliwić Akceptantowi podgląd wszystkich zaaprobowanych zleceń.
DZU/01/2016/ZP/1-WNF-0013	Projektowany system ma zapewniać wysoką dostępność usług i możliwość zastosowania rozwiązań odpornych na awarie w celu zwiększenia niezawodności. Ponadto jego konfiguracja musi pozwalać administratorowi bez przeszkód wykonać wszystkie działania bez przerywania pracy systemu np. poprzez wyłączenie błędnie działającego Konektora lub innego modułu systemu.
DZU/01/2016/ZP/1-WNF-0014	System ma zapewnić odpowiednią wydajność uwzględniając reakcję na działania Użytkowników. Czas odświeżania/ odbudowy ekranu po czynności wykonanej przez Użytkownika nie może być dłuższy niż 1 sek. Warunek ten nie dotyczy funkcji, które są związane z wykonywaniem globalnych operacji na bazie danych takich, jak np. sporządzenie raportów i jednocześnie nie są wykonywane w trakcie codziennej, rutynowej pracy z SZT.
DZU/01/2016/ZP/1-WNF-0015	System ma zapewnić odpowiednią wydajność uwzględniając maksymalną liczbę 156 000 wniosków generowanych w systemie dziennie między 7:00 – 18:00. Zakładając, iż Zamawiający będzie wykorzystywał funkcjonalność masowego wystawiania wniosków w najbardziej prawdopodobnym przypadku istnieje możliwość np. masowego wydania wszystkim pracownikom Zamawiającego nowych Kart elektronicznych i Certyfikatów AD, KSI, ENC lub innych, np. Certyfikatów VPN. Przyjmując: Maksymalna liczba Użytkowników aktywnych do 2020 r. – 52 000 Liczba Zasobów, dla których należy wystawić wnioski - 3 Wyliczenia: 52 000 x 3= 156 000
DZU/01/2016/ZP/1-WNF-0016	System ma zapewnić odpowiednią wydajność uwzględniając ilość danych w nim zgromadzonych obejmujących informacje z okresu 48 m-cy o wszelkich operacjach wykonywanych na Tożsamościach, z uwzględnieniem m.in.: 1) Zasobów i posiadanych uprawnień w ramach tych Zasobów; 2) wniosków.
DZU/01/2016/ZP/1-WNF-0017	Interfejs SZT musi być w języku polskim.
DZU/01/2016/ZP/1-WNF-0018	Interfejs SZT musi być skalowany i obsługiwany przez urządzenia mobilne.
DZU/01/2016/ZP/1-WNF-0019	Interfejs SZT musi być kompatybilny z dostępnymi na rynku wersjami oprogramowania systemowo-narzędziowego (stacje i serwery).
DZU/01/2016/ZP/1-WNF-0020	Interfejs SZT musi być oparty tylko na aktualnie wspieranych pluginach i nie mających planowanego zakończenia wsparcia.

Proces wnioskowania czy Provisioningu Użytkownika i działające przy tym mechanizmy audytowe nie powinny wpływać na stabilność pracy aplikacji i jej wydajność dla innych Użytkowników pracujących w aplikacji, a procesowanie zadań systemowych dla takiej skali Użytkowników nie powinno mieć wpływu na wydajność aplikacji w godzinach biznesowych.

IV. Migracja SZT

Migracja SZT powinna zostać zrealizowana w okresie nie dłuższym niż 26 tygodni od daty podpisania Umowy. Czynności związane z implementacją rozwiązania w środowisku produkcyjnym Zamawiającego powinny zostać zrealizowane w terminie nie dłuższym niż 3 dni kalendarzowe, z zastrzeżeniem:

- 1) Zamawiający zgadza się na okres wskazany jako Start produkcyjny oferowanego przez Wykonawcę rozwiązania zamrozić wnioskowanie i obsługę Zdarzeń kadrowych w obecnie wykorzystywanym SZT na okres nie dłuższy niż 3 dni kalendarzowe;
- 2) Zamawiający oczekuje, iż Start produkcyjny będzie obejmował jednorazowe włączenie przez Wykonawcę oferowanego przez siebie rozwiązania gotowego do realizacji zadań obecnie obsługiwanych w SZT Zamawiającego;
- 3) Zamawiający zakłada, że dane historyczne dot. zdarzeń, złożonych wniosków czy tworzenia i usuwania Tożsamości z eksploatowanego u Zamawiającego SZT przed Migracją SZT będą dostępne w celach kontrolnych/ audytowych. Dostęp do tych danych może być realizowany w trybie „na żądanie”, a ich pozyskanie nie powinno być czasochłonne - przewidywany maksymalny czas oczekiwania na dane to 2 Dni robocze. Dostęp do danych historycznych może być obsługiwany poprzez odrębne narzędzie. W takim przypadku także licencje niezbędne do jego użytkowania przez Zamawiającego powinny być odstąpione przez Wykonawcę bezterminowo. Zakres danych historycznych niepodlegających Migracji SZT zostanie uszczegółowiony na etapie realizacji przedmiotu zamówienia. Utrzymywanie danych historycznych będzie realizowane we wskazanej przez Zamawiającego lokalizacji.

Start produkcyjny poprzedzony będzie testami i odbiorem Produktów. Każdy z etapów zakończony będzie w momencie odbioru zmian bez zastrzeżeń i potwierdzony protokołem odbioru.

ETAP M1 – Przygotowanie infrastruktury COO i ZCOO, w tym dla środowiska developerskiego i przedprodukcyjnego oraz plan migracji danych z zachowaniem funkcjonalności

Wymagania przejściowe

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0014	<p>Przygotowanie infrastruktury COO i ZCOO</p> <p>Wykonawca zobowiązany jest do:</p> <ol style="list-style-type: none">1) Opracowania rozmieszczenia architektury sprzętowej opartej na dwóch lokalizacjach COO i ZCOO;2) Opracowania rozmieszczenia architektury serwerów, urządzeń we/wy w lokalizacji ZCOO oraz architektury systemowej dla środowisk nieprodukcyjnych (przedprodukcja i środowisko testowo-deweloperskie);3) Opracowania rozmieszczenia architektury serwerów, urządzeń we/wy w lokalizacji COO oraz architektury systemowej dla środowisk produkcyjnych;4) Określenia potrzeb w zakresie serwisu systemu operacyjnego/podsystemów;5) Określenia potrzeb w zakresie parametryzacji systemu/podsystemów;6) Zapewnienia wsparcia, poprawek, utrzymania systemu operacyjnego i podsystemów we wszystkich środowiskach

	<p>systemowych, zarówno Wykonawcy jak i producenta wdrożonego Oprogramowania;</p> <p>7) Określenia niezbędnych testów i weryfikacji warstwy sprzętowej, systemowej, narzędziowej oraz rekomendacji w zakresie warstwy aplikacyjnej;</p> <p>8) Przygotowania zmian w konfiguracji sieci KSI na potrzeby Wdrożenia SZT.</p>
DZU/01/2016/ZP/1-WP-0086	Opracowanie projektu wytworzenia środowiska developerskiego i przedprodukcyjnego zintegrowanego ze środowiskami testowymi systemów zintegrowanych z SZT oraz systemów, które docelowo mają być zintegrowane z SZT - jeśli istnieją, z uwzględnieniem, iż środowisko przedprodukcyjne SZT powinno być backupowane przed każdym testem, aby w razie potrzeby można było powtórzyć i przywrócić do stanu zbieżnego z produkcją stąd istotne jest zapewnienie Zasobów na backup (dot. bazy jak i aplikacji). Obydwa środowiska powinny umożliwiać rzetelne przeprowadzenie testów wprowadzanych zmian.
DZU/01/2016/ZP/1-WP-0088	Przygotowanie dokumentacji opisującej środowisko developerskie i przedprodukcyjne oraz ich backupowanie, w tym podłączenie środowisk testowych systemów zintegrowanych z SZT.
DZU/01/2016/ZP/1-WP-0089	Przygotowanie dokumentacji opisującej czynności niezbędne do przeniesienia danych ze środowiska produkcyjnego do przedprodukcyjnego.
DZU/01/2016/ZP/1-WP-0015	<p>Plan migracji danych z zachowaniem funkcjonalności:</p> <ol style="list-style-type: none"> 1) Wykonawca dostarczy projekt migracji niezbędnych danych do poprawnego funkcjonowania docelowego systemu, uwzględniający ciągłość działania Systemu Zarządzania Tożsamością w tym jednokrotnego logowania oraz spójność danych zapewniającą utrzymanie funkcjonalności dotychczas wykorzystywanego systemu, 2) Wykonawca przedstawi projekt odłożenia historii danych (wszystkie dane gromadzone przez SZT) dotyczącego posiadanych przez Tożsamości uprawnień i składanych dotychczas wniosków wraz z możliwością ich generowania w celach audytowych, 3) Wykonawca przedstawi projekt uruchomienia jednokrotnego logowania kompatybilnego z uruchamianym SZT, nie angażującego w to Użytkowników, 4) Wykonawca gwarantuje, iż wdrożone przez niego Oprogramowanie po migracji danych zapewnia funkcjonalność nie mniejszą niż obecnie wykorzystywany SZT i ESSO u Zamawiającego.

Kryteria odbioru etapu:

- 1) Harmonogram wraz ze wskazaniem „kamieni milowych” realizacji etapu oraz datami realizacji,
- 2) Lista osób wraz ze wskazaniem kompetencji każdej z nich, pełnioną rolą/funkcją,
- 3) Dokumentacja wytworzona w cyklu projektowym, w szczególności: zaakceptowany przez Zamawiającego projekt architektury opartej na dwóch lokalizacjach w COO oraz w ZCOO wraz ze specyfikacją opisującą konfigurację wymaganego Sprzętu uwzględniając jego rodzaj (fizyczny, wirtualny), dokumentacja opisująca środowisko developerskie i przedprodukcyjne

oraz ich backupowanie, w tym podłączenie środowisk testowych systemów zintegrowanych z SZT i koncepcja testów weryfikujących poprawność migrowanych danych wraz z zachowaniem funkcjonalności obecnie użytkowanego SZT.

- 4) Plan testów zawierający w szczególności koncepcję testów weryfikujących poprawność konfiguracji sprzętowej.

ETAP M2 – Przygotowanie środowiska aplikacyjnego COO i ZCOO, przeprowadzenie migracji danych oraz uruchomienie środowiska developerskiego i przedprodukcyjnego

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0016	<p>W ramach przygotowania środowiska aplikacyjnego COO i ZCOO oraz uruchomienia środowiska developerskiego i przedprodukcyjnego Wykonawca:</p> <ol style="list-style-type: none"> 1) Dostarczy sprzęt i licencje zgodne z przedstawioną specyfikacją, 2) Skonfiguruje Sprzęt w przedstawionym środowisku, 3) Przygotuje Środowiska: produkcyjne, przedprodukcyjne i testowo-developerskie (warstwa systemowa, bazy danych i aplikacji), zapewniające funkcjonalność nie mniejszą niż obecnie wykorzystywanego produkcyjnie SZT u Zamawiającego, 4) Udostępni interfejs dla środowisk developerskiego i przedprodukcyjnego, 5) Zrealizuje testy potwierdzające poprawność działania poszczególnych środowisk.
DZU/01/2016/ZP/1-WP-0017	<p>Migracja danych zostanie zrealizowana po poprawnym zakończeniu etapu M1:</p> <ol style="list-style-type: none"> 1) Wykonawca przeprowadzi migrację danych zgodnie z przygotowanym i zatwierdzonym przez Zamawiającego projektem, 2) Wykonawca uruchomi jednokrotne logowania zgodnie z zatwierdzoną przez Zamawiającego koncepcją, opracowaną w ramach etapu M1, 3) Wykonawca przeprowadzi odłożenie historii danych zgodnie z przygotowanym i zatwierdzonym przez Zamawiającego projektem w etapie M1, 4) Testy potwierdzające: poprawność migracji danych oraz zachowanie funkcjonalności obecnie użytkowanego SZT oraz możliwość wygenerowania danych audytowych w zakresie danych historycznych.

Kryteria odbioru etapu:

1. Harmonogram wraz ze wskazaniem „kamieni milowych” realizacji etapu oraz datami realizacji.
2. Lista osób wraz ze wskazaniem kompetencji każdej z nich, pełnioną rolą/funkcją.
3. Wykaz Sprzętu, Oprogramowania i licencji dostarczonych w celu realizacji Migracji SZT,
4. Raporty z testów weryfikujących poprawność konfiguracji sprzętowej każdego środowiska zgodnie z zatwierdzoną dokumentacją z etapu M1.
5. Przekazanie oraz konfiguracja Sprzętu w dwóch lokalizacjach w COO oraz w ZCOO.
6. Uruchomienie środowisk aplikacyjnych w docelowej architekturze sprzętowej.
7. Uruchomienie środowiska developerskiego i przedprodukcyjnego.

8. Produkcyjne Wdrożenie rozwiązania aplikacyjnego o zakresie funkcjonalnym nie mniejszym niż obecnie wykorzystywane przez Zamawiającego rozwiązania SZT.
9. Przeprowadzona migracja danych oraz zachowanie funkcjonalności z obecnie użytkowanego SZT oraz włączenie kompatybilnego jednokrotnego logowania zgodnego w zakresie funkcjonalnym z tym działającym u Zamawiającego bez konieczności angażowania w to Użytkowników.
10. Raporty z testów weryfikujących poprawność migracji danych i zachowania funkcjonalności z obecnie użytkowanego SZT i ESSO oraz możliwości wygenerowania danych audytowych w zakresie danych historycznych zatwierdzoną koncepcją z etapu M1.
11. Dokumentacja wytworzona w cyklu projektowym obejmująca Migrację SZT, w tym dokumentacja analityczna, dokumentacja techniczna, podręczniki użytkownika i administratora, dokumentacja eksploatacyjna - Procedury administracyjne, Procedury eksploatacyjne, Standardy IT ZUS, plan ciągłości działania SZT - która określa m.in. specyfikację, budowę, wdrożenie, parametryzację i konfigurację SZT oraz zależności dot. wszystkich związanych z nim komponentów, konektorów systemów, baz danych.

Warsztaty

Wykonawca będzie zobowiązany w ramach przeprowadzenia Migracji SZT do przeprowadzenia warsztatów m. in. w zakresie instalacji, konfiguracji, zmian w konfiguracji, utrzymania, rozbudowy i modyfikacji bazy SZT i modernizacji systemu. Wykonawca przeprowadzi warsztaty dla wskazanych przez Zamawiającego pracowników. Zamawiający w ramach Migracji SZT planuje przeszkolenie do 30 administratorów systemu oraz do 60 osób uczestniczących w procesie zarządzania uprawnieniami u Zamawiającego, na odrębnych warsztatach dedykowanych dla każdego z wymienionych adresatów. Warsztaty w ramach Migracji SZT będą trwały łącznie do 320 godzin, przy czym rzeczywista liczba godzin będzie uzależniona od podziału uczestników na grupy przez Zamawiającego oraz liczby godzin zajęć w zaakceptowanych przez Zamawiającego programach warsztatów.

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0090	Wykonawca zobowiązany będzie do przeprowadzenia warsztatów administracyjnych m. in. w zakresie instalacji, konfiguracji, zmian w konfiguracji, utrzymania, rozbudowy i modyfikacji bazy SZT i modernizacji systemu oraz z uwzględnieniem pełnej funkcjonalności systemu SZT.

V. Rozwój funkcjonalny SZT

Termin realizacji prac w ramach Rozwoju funkcjonalnego SZT: czas trwania Umowy od daty zakończenia Migracji SZT.

Zamawiający zakłada, iż poszczególne etapy wymienione w ramach Rozwoju funkcjonalnego SZT będą mogły być realizowane równolegle przez podzespoły składające się ze specjalistów Wykonawcy i Zamawiającego. Rozwój funkcjonalny SZT realizowany będzie poprzez Zlecenia.

ETAP R1 – Opracowanie projektu i wdrożenie zmian wynikających z integracji SZT i SWEZ

W ramach etapu Wykonawca przeprowadzi:

1. zmiany w systemie SWEZ i SZT realizowane będą zgodnie z przygotowanym przez Wykonawcę i zatwierdzonym przez Zamawiającego projektem z uwzględnieniem obowiązującej u Zamawiającego procedury zaangażowania strony trzeciej (obowiązująca procedura zostanie udostępniona na etapie Zlecenia),
2. testy potwierdzające poprawność wprowadzonych zmian.

Wymagania funkcjonalne

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WF-0061	Uruchomienie nowego klienckiego typu przy procesie zatrudniania (zatrudnienie, zmiana organizacyjna, przejście pracownika z innej Jednostki organizacyjnej, powierzenie i powrót z powierzenia, powrót z zawieszenia, przejście pracownika zawieszono) do rejestracji jednej lokalizacji miejsca wykonywania pracy (adres Jednostki organizacyjnej do wyboru ze słownika dostępnego w SWEZ).
DZU/01/2016/ZP/1-WF-0062	Utworzenie tabeli konfiguracyjnej dla lokalizacji wraz z adresami (adresy tj. nazwa Jednostki organizacyjnej, ulica, kod pocztowy, miejscowość) powiązanej ze słownikiem kodów jednostek KSI.
DZU/01/2016/ZP/1-WF-0063	Rozszerzenie struktury IDOC o nowy segment HRMD_A tak, aby dane te przesyłane były do SZT.
DZU/01/2016/ZP/1-WF-0064	Modyfikacja grup Zdarzeń kadrowych wyspecyfikowanej przez Zamawiającego o nowy typ informacji.
DZU/01/2016/ZP/1-WF-0065	Uzupełnienie danych dotyczących miejsca pracy pracownika w SWEZ oraz utworzenie raportów w SWEZ umożliwiających monitorowanie danych w zakresie wprowadzonych projektem zmian.
DZU/01/2016/ZP/1-WF-0066	Przekazywanie do SZT informacji o kodzie z Jednostki organizacyjnej zgodnej z Katalogiem KSI – miejsca zatrudnienia i miejsca wykonywania pracy.
DZU/01/2016/ZP/1-WF-0067	Umożliwienie na podstawie adresu i słownika jednostek katalogu KSI automatycznego uzupełniania w SWEZ podtypu infotypu 105 o nazwie KSI oraz podtypu 0001 i 0010 po utworzeniu kont poczty i loginu SAP.
DZU/01/2016/ZP/1-WF-0068	Rozszerzenie i implementacja zakresu danych pobieranych z SAP HR do Systemu Zarządzania Tożsamością o: <ol style="list-style-type: none"> 1) Funkcja (np. stanowisko ds. ważnych), 2) MPK (Miejsce Powstawania Kosztów), 3) Opis MPK (np. CE-OO Sprawy_Pracown), 4) oraz mapowanie dostępnych danych, w tym struktury organizacyjnej i przypisania KSI na Tożsamości w SZT.
DZU/01/2016/ZP/1-WP-0018	Przebudowa Konektora SAP – zgodnie z wymaganiami od DZU/01/2016/ZP/1-WF-0061 do DZU/01/2016/ZP/1-WF-0068 i projektem zmian biznesowych w procesie wnioskowania o SWEZ w SZT (dokument Koncepcja zmian biznesowych wnioskowania o uprawnienia do SWEZ w SZT) oraz uwzględnić możliwość filtrowania, tj. pobierania z SWEZ wyłącznie ról, których nazwa rozpoczyna się np. od litery „Z”. Przebudowa Konektora SAP wraz z loggerami umożliwiającymi bezpośrednią diagnozę jego funkcjonowania, uruchomienie w środowisku developerskim, przedprodukcyjnym i produkcyjnym. Przygotowanie dokumentacji opisującej funkcjonalność Konektora SAP i konfiguracja w Środowisku produkcyjnym i zalecaną w

Kryteria odbioru etapu:

1. Harmonogram wraz ze wskazaniem „kamieni milowych” realizacji etapu oraz datą realizacji.
2. Lista osób wraz ze wskazaniem kompetencji każdej z nich, pełnioną rolą/funkcją.
3. Plan testów zawierający koncepcję testów weryfikujących poprawność uruchamianych funkcjonalności SZT odwzorowujących zmiany w SWEZ oraz raporty z testów weryfikujących poprawność działania Konektora SAP.
4. Wprowadzenie zmian w SWEZ i SZT zgodna z zatwierdzonym przez Zamawiającego projektem.
5. Raporty z testów weryfikujących poprawność działania poszczególnych procesów po wprowadzeniu zmian.
6. Dokumentacja wytworzona w cyklu projektowym, w szczególności dokumentacja opisująca działanie konektora pomiędzy SWEZ i SZT po wprowadzeniu zmian oraz dokumentacja opisująca funkcjonalność Konektora SAP i jego konfigurację w środowisku produkcyjnym i zalecaną w środowisku developerskim i przedprodukcyjnym.

ETAPY R2 – R5: Budowa/Przebudowa Konektorów

W ramach poszczególnych etapów (R2, R3, R4, R5) realizowane będą przez Wykonawcę usługi związane z przygotowaniem projektu budowy nowych bądź przebudowy istniejących konektorów, ich wdrożenie i uruchomienie w środowisku produkcyjnym zgodnie z poniższymi wymaganiami Zamawiającego. Etapy te mogą być Zlecane osobno.

Wymagania przejściowe:

Nazwa etapu [identyfikator wymagania]	Opis wymagania
ETAP R2 – Konektor AuthAPI [DZU/01/2016/ZP/1-WP-0020]	<p>Opracowanie projektu przebudowy/budowy Konektora AuthAPI:</p> <ol style="list-style-type: none"> 1) dostosowanie do nowej wersji bazy AuthAP, 2) zmiana sposobu komunikacji Konektora SZT z bazą AuthAPI. Komunikacja miałaby się odbywać za pośrednictwem serwisu. Serwis AuthAPI oferowałby metody niezbędne do komunikacji z SZT, np. realizowałby usługi wejściowe (przyjmujące dane i aktualizujące je w bazie AuthAPI): DodajKonto, UsunKonto, ModyfikujKonto, ZablokujKonto, ZmienHaslo, DodajRoleUzytkownika, UsunRoleUzytkownika, SynchronizujStrukture oraz usługi wyjściowe (SELECTy – zwracające dane z bazy AuthAPI): PobierzAplikacjeOrazRole, PobierzUzytkownikowZRolami. Wymienione wyżej usługi mogą wymagać rozszerzenia w miarę potrzeb komunikacji, 3) rozszerzenie danych Użytkownika o dodatkowe informacje (SID, login AD), 4) zmiana modelu nadawania ról – możliwość przypisania roli do jednostki – w konsekwencji Użytkownik może mieć role do wielu jednostek (w chwili obecnej można nadać role tylko w jednostce, do której jest przypisany Użytkownik),

	5) Dodatkowy krok aprobaty dla poszczególnych ról w aplikacjach autorskich.
ETAP R3 – Konektor CC [DZU/01/2016/ZP/1-WP-0022]	Opracowanie projektu przebudowy/ budowy Konektora CC: 1) rozszerzenie możliwości wnioskowania o nowe Zasoby typu Certyfikat zdefiniowane na podstawie nowych szablonów Certyfikatów w usłudze Active Directory Certificate Services (AD CS), 2) nagrywanie lub usuwanie z Kart elektronicznych dowolnych Certyfikatów, 3) wygenerowanie metodą wsadową dowolnej ilości Zasobów Karta elektroniczna i/lub Certyfikaty przy użyciu plików źródłowych (TXT, CSV, XML) zawierających właściwe dane, 4) możliwość zwiększenia obsługiwanych kluczy do co najmniej 4096 bit oraz algorytmu hashującego (hash algorithm) do SHA-512, 5) odnawianie Certyfikatów dowolnego typu znajdujących się na Karcie elektronicznej wraz z możliwością usunięcia odnowionych Certyfikatów z wyjątkiem Certyfikatu ENC, 6) wystawienie Użytkownikowi interfejsu, który automatycznie dopasuje wstawione przez niego zdjęcie do wymaganych rozmiarów.
ETAP R4 – Konektor HPSM [DZU/01/2016/ZP/1-WP-0023]	Opracowanie projektu przebudowy/budowy Konektora HPSM: 1) umożliwienie komunikacji z SZT za pomocą usług web service. Ze względu na złożoność struktury bazy danych HPSM oraz brak zapewnienia 100% relacyjności na poziomie motoru bazy jedynym dopuszczalnym sposobem komunikacji SZT z systemem HPSM jest wywoływanie przez SZT odpowiednich usług web service udostępnionych przez HPSM (zarówno w celu pozyskania informacji z HPSM jak i zapisania do HPSM), 2) zarządzanie uprawnieniami poprzez SZT powinno uwzględniać dla HPSM rozbudowany mechanizm uprawnień oparty o: a) role, które grupują uprawnienia do poszczególnych modułów HPSM. Za uprawnienia w poszczególnych modułach odpowiadają profile oraz uprawnienia wykonawcze, (słowa klucze), b) grupy. W HPSM równie ważną rolę pełni przynależność do grup przypisania, w module Incydentów oraz zmian. Przypisanie takie umożliwia obsługę zdarzeń, które zostały zgłoszone do danej grupy; 3) zakłada się etap akceptacji dla niektórych grup i ról. 4) Wnioskodawca będzie mógł wybrać odpowiednią rolę po wskazaniu, której zostanie poproszony o wskazanie grup obsługi Incydentów oraz grup obsługi zmian (pola wielokrotnego wyboru). Jeśli rola wymaga akceptacji taki wniosek jest przekazywany do komórki akceptującej. Zakłada się iż role „centralne”; dla Pracowników zewnętrznych oraz posiadające uprawnienia administratorskie powinny być potwierdzane przed nadaniem. Po potwierdzeniu roli wniosek o uprawnienia

	<p>powinien zostać przekazany do menadżerów grup przypisania Incydentów oraz osoby odpowiedzialnej za moduł zmian. Po zatwierdzeniu na wszystkich poziomach w Systemie Zarządzania Tożsamością powinien on przekazać za pomocą usług web service wcześniej ustalone parametry, a HP SM zareagować na nie w ustalony wcześniej sposób,</p> <p>5) jeden Użytkownik może mieć jedną rolę i może być członkiem wielu grup,</p> <p>6) wymagane jest aby SZT synchronizował z HPSM listę ról i grup.</p>
ETAP R5 – Konektor AD [DZU/01/2016/ZP/1-WP-0019]	<p>Opracowanie projektu przebudowy/budowy konektora AD:</p> <p>1) uruchomienie możliwości wnioskowania o utworzenie grupy AD poprzez SZT,</p> <p>2) wyświetlanie w SZT grup nadanych bezpośrednio w AD w procesie wnioskowania,</p> <p>3) przekazywanie do AD danych o przypisaniu organizacyjnym Użytkownika zgodnie z regulaminem organizacyjnym Zamawiającego, zamiast komórki wewnętrznej istniejącej tylko dla potrzeb SWEZ określonej jako Pion,</p> <p>4) przekazywanie do AD danych o numerze osobowym pracownika z SAP,</p> <p>5) rozszerzenie funkcjonalności wnioskowania o zmianę sposobu Logowania opisanej w pkt 4.1.1.14 dokumencie Szczegółowy opis działania obecnego SZT, w sposób umożliwiający zdefiniowanie przez Zamawiającego nowych grup (max. 10 grup liczonych w zakresie 0 do 9). Definiowanie nowych grup powinno opierać się na mechanizmie tzw. „Wizarda” albo na odpowiednich plikach konfiguracyjnych systemu SZT.</p>
DZU/01/2016/ZP/1-WP-0028	Przygotowanie poszczególnych Konektorów (z etapów: R2, R3, R4 i R5) wraz z loggerami umożliwiającymi bezpośrednią diagnozę ich funkcjonowania, uruchomienie w środowisku developerskim, przedprodukcyjnym i produkcyjnym.
DZU/01/2016/ZP/1-WP-0029	Przygotowanie dokumentacji opisującej funkcjonalność poszczególnych Konektorów i ich konfigurację w Środowisku produkcyjnym i zalecaną w środowisku developerskim i przedprodukcyjnym.

Kryteria odbioru etapów R2, R3, R4 i R5:

1. Przeprowadzona budowa/ przebudowa poszczególnych Konektorów i ich uruchomienie w Środowisku produkcyjnym.
2. Harmonogram realizacji danego etapu wraz ze wskazaniem „kamieni milowych” realizacji tego etapu oraz datami realizacji.
3. Lista osób wraz ze wskazaniem kompetencji każdej z nich, pełnioną rolą/funkcją.
4. Plan testów i raporty z testów weryfikujących poprawność działania poszczególnych Konektorów.
5. Dokumentacja wytworzona w cyklu projektowym, w szczególności dokumentacja opisująca funkcjonalność poszczególnych Konektorów i ich konfigurację w środowisku produkcyjnym i zalecaną w środowisku developerskim i przedprodukcyjnym.

Uwaga: odbiór poszczególnych elementów etapów R2, R3, R4 i R5 z zapewnieniem dla nich osobnych kryteriów odbioru zgodnie z pkt 1- 5.

ETAP R6 – Manualny Provisioning

W ramach etapu realizowane będą przez Wykonawcę usługi związane z przygotowaniem projektu, wdrożeniem i uruchomieniem w środowisku produkcyjnym rozbudowanej funkcjonalności w zakresie Manualnego Provisioningu zgodnie z poniższymi wymaganiami Zamawiającego.

Wymagania przejściowe

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0030	Opracowanie projektu uruchomienia w SZT obsługi Zasobów zarządzanych manualnie przy uwzględnieniu kilku możliwych ścieżek procesowania zarówno w zakresie aplikacji aktualnie zaimplementowanych do SZT jak i innych aplikacji wykorzystywanych u Zamawiającego np. umożliwienie kilku etapowej obsługi tego samego wniosku tj. wnioszek trafia najpierw do obsługi do grupy A, następnie do grupy B.
DZU/01/2016/ZP/1-WP-0031	Udostępnienie interfejsu umożliwiającego wyprowadzenie lub wycofanie Zasobu zarządzanego manualnie w dowolnym momencie, poprzez konto administratora SZT.
DZU/01/2016/ZP/1-WP-0032	Przygotowanie poszczególnych ścieżek procesowania Zasobu zarządzanego manualnie.
DZU/01/2016/ZP/1-WP-0033	Przygotowanie dokumentacji opisującej zarządzanie konkretnym Zasobem jak i ścieżką jego procesowania.

Kryteria odbioru etapu:

1. Uruchomienie produkcyjne poszczególnych ścieżek procesowania Zasobów zarządzanych manualnie i import danych przez Zamawiającego w środowisku produkcyjnym po akceptacji całego procesu implementacji na środowisku przedprodukcyjnym.
2. Harmonogram wraz ze wskazaniem „kamieni milowych” realizacji etapu oraz datami realizacji.
3. Lista osób wraz ze wskazaniem kompetencji każdej z nich, pełnioną rolą/funkcją.
4. Plan testów i raport z testów weryfikujących poprawność działania poszczególnych procesów.
5. Dokumentacja wytworzona w cyklu projektowym, w szczególności dokumentacja opisująca zarządzanie konkretnym Zasobem jak i ścieżką jego procesowania.

ETAP R7 – Monitorowanie i raportowanie

W ramach etapu realizowane będą przez Wykonawcę usługi związane z przygotowaniem projektu, wdrożeniem i uruchomieniem w środowisku produkcyjnym rozbudowanej funkcjonalności w zakresie monitorowania i raportowania zgodnie z poniższymi wymaganiami Zamawiającego.

Wymagania funkcjonalne

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WF-0069	Umożliwienie generowania raportów przefiltrowanych po parametrach i uprawnieniach strukturalnych (dotyczących SWEZ), roli, systemie, aplikacji, Zasobie, Tożsamości, w oparciu o numer osobowy i opis numeru MPK lub strukturę organizacyjną

	Zamawiającego (TJO/departament/wydział/stanowisko) przy wyborze jednego lub kilku tych samych parametrów.
DZU/01/2016/ZP/1-WF-0070	Raportowanie danych odpisywanych w zakresie Kont uprzywilejowanych.
DZU/01/2016/ZP/1-WF-0071	Uwzględnienie raportowania dla osób z wielozatrudnieniem.
DZU/01/2016/ZP/1-WF-0072	Wygenerowanie raportu o uprawnieniach nadanych bezpośrednio w systemach źródłowych.
DZU/01/2016/ZP/1-WF-0073	Wygenerowanie raportu w oparciu o zestaw zdefiniowanych uprawnień.
DZU/01/2016/ZP/1-WF-0074	Eksport do formatu XLS, HTML, XML, CSV do zdefiniowanej lokalizacji.
DZU/01/2016/ZP/1-WF-0075	Publikacja raportów dla określonych grup Użytkowników zgodnie z wymaganiami Zamawiającego.
DZU/01/2016/ZP/1-WF-0076	Udostępnienie interfejsu umożliwiającego monitorowanie i diagnostykę SZT, w tym m.in. liczby Użytkowników korzystających z SZT i liczby wniosków wystawianych w SZT (automatycznie, manualnie przez osoby posiadające stosowne uprawnienia).
DZU/01/2016/ZP/1-WF-0077	W ramach jednokrotnego logowania powinny być udostępnione mechanizmy monitorowania i raportowania w zakresie jego wykorzystania.

Wymagania przejściowe

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0034	Przygotowanie dokumentacji opisującej proces generowania raportów oraz pobierania do nich danych.
DZU/01/2016/ZP/1-WP-0035	Przygotowanie dokumentacji opisującej działanie interfejsu monitorującego działanie SZT.
DZU/01/2016/ZP/1-WP-0036	Przygotowanie dokumentacji opisującej zarządzanie procesami jednokrotnego logowania wraz z instrukcją dodawania nowych, zmiany/wycofania istniejących szablonów.

Kryteria odbioru etapu:

1. Wdrożenie produkcyjne funkcjonalności raportowania monitorujących, pozwalających m.in. na diagnostykę SZT w zakresie zajętości systemu (CPU, RAM, HDD, inne) oraz monitorowania i raportowania w zakresie wykorzystania jednokrotnego logowania zgodnych z wymaganiami Zamawiającego.
2. Harmonogram wraz ze wskazaniem „kamieni milowych” realizacji etapu oraz datami realizacji.
3. Lista osób wraz ze wskazaniem kompetencji każdej z nich, pełnioną rolą/funkcją.
4. Plan testów i raport z testów weryfikujących poprawność generowania raportów oraz weryfikujących poprawność działania poszczególnych procesów.
5. Dokumentacja wytworzona w cyklu projektowym, w szczególności dokumentacja opisująca proces generowania raportów i pobierania do nich danych oraz dokumentacja opisująca działanie interfejsu monitorującego działanie SZT i dokumentacja opisująca działanie jednokrotnego logowania.

ETAP R8 – Moduł Administracyjny

W ramach etapu realizowane będą przez Wykonawcę usługi związane z przygotowaniem projektu, wdrożeniem i uruchomieniem w środowisku produkcyjnym funkcjonalności w zakresie Modułu administracyjnego zgodnie z poniższymi wymaganiami Zamawiającego.

Wymagania przejściowe

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0079	Opracowanie projektu uruchomienia w SZT panelu administracyjnego umożliwiającego przede wszystkim: 1) Zarządzanie słownikami niezależnie od ich wielkości, 2) Import i eksport słowników, 3) Możliwość definiowania obsługi Zdarzeń kadrowych, w szczególności poprzez zapewnienie możliwości: a) dodania/ usunięcia Zasobu, b) modyfikacji atrybutów Użytkownika, c) wyłączenia/ włączenia Zasobu oraz Użytkownika, d) definiowania kolejności wykonywanych operacji (np. dodanie Zasobu exchange zależy od prawidłowego dodania Zasobu AD), 4) Definiowanie nowych wniosków i sposobu ich przebiegu, 5) Edycję już zdefiniowanych zdarzeń i wniosków oraz sposobu ich przebiegu.
DZU/01/2016/ZP/1-WP-0080	Przygotowanie dokumentacji opisującej zarządzanie danymi znajdującymi się w panelu administracyjnym.

Wymagania funkcjonalne

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WF-0078	Wdrożenie interfejsu umożliwiającego zarządzanie danymi znajdującymi się w panelu administracyjnym.
DZU/01/2016/ZP/1-WF-0079	Przygotowanie poszczególnych ścieżek dokonywania zmian danych znajdujących się w panelu administracyjnym.

Kryteria odbioru etapu:

1. Wdrożenie produkcyjne interfejsu panelu administracyjnego.
2. Harmonogram wraz ze wskazaniem „kamieni milowych” realizacji etapu oraz datami realizacji.
3. Lista osób wraz ze wskazaniem kompetencji każdej z nich, pełnioną rolą/funkcją.
4. Plan testów i raport z testów weryfikujących poprawność działania panelu administracyjnego.
5. Dokumentacja wytworzona w cyklu projektowym, w szczególności dokumentacja opisująca zarządzaniem danymi znajdującymi się w panelu administracyjnym.

ETAP R9 – Moduł Zarządzania Kontami Uprzywilejowanymi

W ramach etapu realizowane będą przez Wykonawcę usługi związane z przygotowaniem projektu, wdrożeniem i uruchomieniem w środowisku produkcyjnym funkcjonalności w zakresie Modułu Zarządzania Kontami uprzywilejowanymi zgodnie z poniższymi wymaganiami Zamawiającego.

Wymagania przejściowe

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0037	Opracowanie projektu, który umożliwi zarządzanie Kontami uprzywilejowanymi oraz hasłami dla kont usług/Użytkowników na systemach i urządzeniach w środowisku informatycznym.
DZU/01/2016/ZP/1-WP-0038	Opracowanie projektu, który umożliwi monitorowanie działań na Kontach uprzywilejowanych w systemach operacyjnych, platformach, bazach danych oraz na urządzeniach sieciowych w sposób niezakłócający funkcjonowanie Środowisk produkcyjnych oraz pracy Użytkowników.
DZU/01/2016/ZP/1-WP-0039	Opracowanie projektu, który umożliwi nadawanie uprawnień dla Pracowników zewnętrznych realizujących zadania na rzecz Zamawiającego.
DZU/01/2016/ZP/1-WP-0040	Opracowanie projektu, który umożliwi kontrolę dostępu zewnętrznych dostawców do środowiska informatycznego.
DZU/01/2016/ZP/1-WP-0041	Opracowanie projektu, który umożliwia weryfikację kompletności zbioru Kont uprzywilejowanych zarządzanych przez moduł ze stanem faktycznym.
DZU/01/2016/ZP/1-WP-0042	Opracowanie projektu, który wspiera zarządzanie Hasłami Użytkowników, na co najmniej systemach takich jak: Unix, Linux, Windows, IBM, Mainframe, SUN, HP-UX, Oracle, SQL Server, SAP, Sybase, Microsoft SQL Server, MySQL, PostgreSQL, IBM DB2, VMware, Cisco, Check Point, LDAP, Active Directory – Użytkowanych u Zamawiającego.
DZU/01/2016/ZP/1-WP-0043	Opracowanie projektu, który wspiera realizowanie sesji wraz z rejestracją aktywności Użytkowników, do co najmniej systemów, platform jak: Unix, Linux, Windows, Oracle, SAP, Mainframe, VMware – użytkowanych u Zamawiającego.
DZU/01/2016/ZP/1-WP-0044	Opracowanie projektu, który oferuje wsparcie dla protokołów takich jak: ssh, rdp, telnet, vnc, http, https, SQLPlus Oracle, SQL Windows – użytkowanych u Zamawiającego.
DZU/01/2016/ZP/1-WP-0045	Opracowanie projektu, który udostępni administratorom oraz Użytkownikom interfejs przeglądarkowy wspierający różne typy dostępnych na rynku przeglądarek, takich jak: Internet Explorer, Chrome, FireFox Mozilla, Opera – użytkowanych u Zamawiającego.
DZU/01/2016/ZP/1-WP-0046	Opracowanie projektu, który zapewni zarządzanie poprzez interfejs przeglądarkowy udostępniony za pomocą protokołu HTTPS oraz z linii komend po zabezpieczonym protokole SSH.
DZU/01/2016/ZP/1-WP-0047	Opracowanie projektu, który posiada mechanizm wysyłania powiadomień e-mailowych (wbudowana usługa SMTP).
DZU/01/2016/ZP/1-WP-0048	Opracowanie projektu, który oferuje wbudowane w interfejs administratora komendy administracyjne w celu umożliwienia przeprowadzenia testów komunikacyjnych z docelowymi urządzeniami/ systemami/ platformami (np. ping, telnet, nslookup, tracert).
DZU/01/2016/ZP/1-WP-0049	Opracowanie projektu, który nagrywa sesje Użytkownika uprzywilejowanego w formie skompresowanej i zapisuje je w formie umożliwiającej analizę tekstową.
DZU/01/2016/ZP/1-WP-0050	Opracowanie projektu, który umożliwi funkcjonalność nadawania uprawnień do wykonania konkretnego polecenia/ komendy oraz

	blokowania dla użytkownika możliwości uruchomienia innego polecenia/ komendy.
DZU/01/2016/ZP/1-WP-0051	Opracowanie projektu, który umożliwi kontrole i audyt wykorzystania współdzielonych haseł administracyjnych.
DZU/01/2016/ZP/1-WP-0052	Opracowanie projektu, który wspiera zarządzanie Hasłami w szczególności potrafi zarządzać hasłami dla kont serwisowych w usługach na komputerach Windows – użytkowanych u Zamawiającego.
DZU/01/2016/ZP/1-WP-0053	Opracowanie projektu, który umożliwi udzielenie uprawnienia (w trakcie trwania sesji lub z zastosowaniem mechanizmu rozłączenia i ponownego jej zestawienia) do wgrania lub kopiowania plików z systemu, do którego taka sesja jest zestawiana.
DZU/01/2016/ZP/1-WP-0054	Opracowanie projektu, który oferuje mechanizm śledzenia za pomocą kompleksowego audytu, obejmującego polityki, uprawnienia oraz czynności wykonywane przez Użytkowników uprzywilejowanych.
DZU/01/2016/ZP/1-WP-0055	Opracowanie projektu, który wspiera funkcjonalność wysyłania zdarzeń dotyczących aktywności administratora lub Użytkownika do serwera SYSLOG.
DZU/01/2016/ZP/1-WP-0056	Opracowanie projektu, który umożliwi implementację indywidualnych polityk bezpieczeństwa Haseł dla różnych typów systemów w szczególności określenia jej złożoności, długości zabronionych znaków, powtarzania się znaków, minimalnej i maksymalnej długości, stosowanie dużych i małych liter, używania znaków alfanumerycznych, zabronionych znaków.
DZU/01/2016/ZP/1-WP-0057	Opracowanie projektu, który umożliwia monitorowanie, filtrowanie, Uwierzytelnianie i szeroko rozumiane zarządzanie sesjami zdalnymi, gdzie sesje te definiujemy, jako połączenia sieciowe wykorzystujące różne protokoły warstwy aplikacyjnej (np. ssh, telnet, rdp, vnc, citrix).
DZU/01/2016/ZP/1-WP-0058	Opracowanie projektu, który umożliwi monitorowanie/oglądanie online sesji Użytkowników do systemów, podczas monitorowania takiej sesji powinna być możliwość zakończenia sesji Użytkownika w sytuacji, kiedy wykonuje on niedozwolone aktywności.
DZU/01/2016/ZP/1-WP-0059	Opracowanie projektu, który ma możliwość automatycznego zamykania sesji w przypadku nieaktywności Użytkownika przez zadany okres czasu.
DZU/01/2016/ZP/1-WP-0060	Opracowanie projektu, w którym Użytkownik podczas wnioskowania o Hasło i sesję powinien mieć możliwość wprowadzenia uzasadnienia.
DZU/01/2016/ZP/1-WP-0061	Opracowanie projektu, który umożliwia rejestrowanie uderzeń użytkownika w klawiaturę i zapisywanie je w logu oraz umożliwia przeszukanie logu w celu wyszukania konkretnego ciągu znaków.
DZU/01/2016/ZP/1-WP-0062	Opracowanie projektu, który udostępnia zaindeksowany log z sesji, zawierający aktywności Użytkownika.
DZU/01/2016/ZP/1-WP-0063	Opracowanie projektu, który umożliwi przeszukiwanie logu z sesji za pomocą wyrażeń regularnych.
DZU/01/2016/ZP/1-WP-0064	Opracowanie projektu, który umożliwia implementację list dostępowych i polityk posiadających wewnętrzny zestaw uprawnień i ról regulujących dostęp do systemów/Kont uprzywilejowanych. Systemy oraz Konta muszą mieć możliwość grupowania

	i przyznawania do nich określonych uprawnień dla Użytkowników (np. administrator Linux nie zobaczy serwerów Windows).
DZU/01/2016/ZP/1-WP-0065	Opracowanie projektu, który wspiera mechanizm lokalnego Uwierzytelniania do portalu administracyjnego i Użytkowników przez integrację z AD/LDAP, Radius, certyfikat X.509, mechanizm dwuskładnikowego Uwierzytelniania za pomocą tokena (sprzętowego, softwareowego, SMS, e-mail).
DZU/01/2016/ZP/1-WP-0066	Opracowanie projektu, który umożliwia ukrywanie lub szyfrowanie rzeczywistych Haseł wymaganych do Uwierzytelnienia.
DZU/01/2016/ZP/1-WP-0067	Opracowanie projektu, który posiada wbudowane role, które określają dostęp do jego Zasobów oraz rejestrują zdarzenia w logu audytowym.
DZU/01/2016/ZP/1-WP-0068	Opracowanie projektu, który zapewnia wysoką dostępność, skalowalność oraz jakość działania.
DZU/01/2016/ZP/1-WP-0069	Opracowanie projektu, który posiada możliwość automatycznej detekcji kont na podłączanym systemie.
DZU/01/2016/ZP/1-WP-0070	Opracowanie projektu, który ma możliwość tworzenia szablonów do połączeń określonego typu systemów w interfejsie i ma możliwość podpinania podobnych, nowych.
DZU/01/2016/ZP/1-WP-0071	Opracowanie projektu, który posiada w interfejsie możliwość importu/ aktualizacji kolekcji zarządzanych systemów oraz import/ aktualizację grup.
DZU/01/2016/ZP/1-WP-0072	Opracowanie projektu, który wspiera możliwość zatwierdzania wniosków o Hasło, sesję lub transfer pliku do systemu docelowego poprzez użycie grup lub odpowiednich Użytkowników.
DZU/01/2016/ZP/1-WP-0073	Opracowanie projektu, który umożliwia zmianę przypisania właścicielstwa biznesowego dla Kont technicznych.
DZU/01/2016/ZP/1-WP-0074	Opracowanie projektu, który umożliwia określenie aktualnego statusu wniosków oraz ich historii.
DZU/01/2016/ZP/1-WP-0075	Opracowanie projektu, który ma możliwość usunięcia Konta uprzywilejowanego.
DZU/01/2016/ZP/1-WP-0076	Opracowanie projektu, który udostępni rozwiązania przewidziane do zarządzania Kontami uprzywilejowanymi, zgodnie z zatwierdzonym przez Zamawiającego projektem wsparcia Użytkowników w tym zakresie.
DZU/01/2016/ZP/1-WP-0077	Przygotowanie i uruchomienie w Środowisku produkcyjnym Zamawiającego poszczególnych ścieżek procesowania obsługi Kont uprzywilejowanych.
DZU/01/2016/ZP/1-WP-0078	Przygotowanie dokumentacji opisującej zarządzanie konkretnym Zasobem jak i ścieżką jego procesowania.

Kryteria odbioru etapu:

1. Projekt uruchomienia systemu wspomagania zarządzania Kontami uprzywilejowanymi.
2. Harmonogram wraz ze wskazaniem „kamieni milowych” realizacji etapu oraz datami realizacji.
3. Wdrożenie produkcyjne rozwiązania przewidzianego do zarządzania Kontami uprzywilejowanymi, zgodnie z projektem zatwierdzonym przez Zamawiającego.
4. Uruchomienie ścieżek procesowania zarządzania Kontami uprzywilejowanymi oraz procesów ich nadzoru/kontroli.
5. Lista osób funkcyjnych wraz z wykazem zadań w procesach zarządzania Kontami uprzywilejowanymi.

6. Plan testów i raport z testów weryfikujących poprawność działania poszczególnych procesów oraz raport testów z realizacji przez system wszystkich wymagań funkcjonalnych modułu.
7. Dokumentacja wytworzona w cyklu projektowym, w szczególności dokumentacja opisująca zarządzanie konkretnym Zasobem jak i ścieżką jego procesowania oraz dokumentacja opisująca działanie modułu zarządzania Kontami uprzywilejowanymi.

Warsztaty

Wykonawca będzie zobowiązany w ramach przeprowadzenia Rozwoju funkcjonalnego SZT do przeprowadzenia warsztatów m. in. w zakresie instalacji, konfiguracji, zmian w konfiguracji, utrzymania, rozbudowy i modyfikacji bazy SZT i modernizacji systemu. Wykonawca przeprowadzi warsztaty dla wskazanych przez Zamawiającego pracowników. Zamawiający w ramach rozwoju funkcjonalnego SZT planuje przeszkolenie do 20 administratorów systemu oraz do 20 osób uczestniczących w procesie zarządzania uprawnieniami u Zamawiającego, na odrębnych warsztatach dedykowanych dla każdego z wymienionych adresatów. Warsztaty w ramach Rozwoju funkcjonalnego SZT będą trwały łącznie do 180 godzin, przy czym rzeczywista liczba godzin będzie uzależniona od podziału uczestników na grupy przez Zamawiającego oraz liczby godzin zajęć w zaakceptowanych przez Zamawiającego programach warsztatów.

Identyfikator	Opis wymagania
DZU/01/2016/ZP/1-WP-0091	Wykonawca zobowiązany będzie do przeprowadzenia warsztatów administratorskich w zakresie utrzymania rozbudowanych/budowanych funkcjonalności zrealizowanych w ramach Zleceń.