**Specyfikacja System SZT**

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa Systemu Zarządzania Tożsamością wraz z kompletem niezbędnych licencji czasowych (w modelu subskrypcyjnym), przeprowadzenie Wdrożenie zgodnie z warunkami Umowy, w tym wykonanie i dostarczenie Projektu Technicznego, Planu Testów Akceptacyjnych, Dokumentacji powykonawczej oraz Dokumentacji eksploatacyjnej, zapewnienie wsparcia producenta (Opieki serwisowej), świadczenie Gwarancji przez Wykonawcę oraz świadczenie Usługi Wsparcia przez okres 36 miesięcy oraz przeprowadzenie warsztatów z wdrożonego rozwiązania dla administratorów wskazanych przez Zamawiającego osób i użytkowników kluczowych SZT.

1. Specyfikacja Systemu SZT

II. Architektura SZT

2.1. Platforma sprzętowa Zamawiającego składa się z dwóch ośrodków przetwarzania danych, macierzy dyskowych, puli serwerów oraz środowiska wirtualizacyjnego.

2.2. SZT musi składać się z trzech wyodrębnionych środowisk - produkcyjnego (PROD), testowo-szkoleniowego (TEST) i deweloperskiego (DEV) przy założeniu, iż środowiska będą funkcjonowały na jednej platformie sprzętowej udostępnionej przez Zamawiającego. Środowisko DEV i TEST musi być objęte integracją z podłączonymi systemami testowymi.

III. Architektura sieciowa.

3.1. SZT musi zostać zaprojektowany w sposób umożliwiający jego poprawne funkcjonowanie w posiadanej obecnie przez Zamawiającego architekturze sieciowej pomiędzy CPD I WAN.

4. SZT oraz jego wszystkie niezbędne komponenty oprogramowania muszą zostać zainstalowane na udostępnionych maszynach wirtualnych Zamawiającego.

4.1. Zamawiający w ramach środowiska produkcyjnego dla SZT udostępni maksymalnie trzy maszyny wirtualne o parametrach wskazanych przez Wykonawcę.

4.2. Zamawiający w ramach środowiska testowo-szkoleniowego dla SZT udostępni maksymalnie trzy maszyny wirtualne o parametrach wskazanych przez Wykonawcę.

4.3. Zamawiający w ramach środowiska deweloperskiego dla SZT udostępni maksymalnie trzy maszyny wirtualne o parametrach wskazanych przez Wykonawcę.

4.4. Zamawiający zapewni System operacyjny na powyższych serwerach: Windows Server 2012 R2 lub nowszy.

4.5. Zamawiający posiada na potrzeby środowiska pod bazę danych SZT Microsoft SQL Server standard – w najnowszej wersji i zapewni licencje na potrzeby wdrażanego rozwiązania. Jeżeli Wykonawca zaoferuje rozwiązanie wymagające innego rozwiązania do zarządzania relacyjną bazą danych to musi je dostarczyć w ramach wdrożenia SZT i zapewnić Zamawiającemu licencje.

4.6. System Zarządzania Tożsamością musi mieć możliwość pracy na poniższych systemach operacyjnych:

• Windows Server 2012 R2 i wyższych

• Red Hat Enterprise Linux Server release 6.6 i wyższych.

4.7. System Zarządzania Tożsamością musi zapewnić zakładany poziom integracji Centralnego Repozytorium Informacji z następującymi systemami:

• Windows Server (wersja 2012 R2 i wyższe);

• Red Hat Enterprise Linux Server (release 6.6 i wyższe);

• Active Directory (LDAP v.3 i wyższe);

• Microsoft Exchange (wersja 2010 i wyższe);

• Microsoft SQL Server (wersja 2014 i wyższe);

• IFS Applications 7.5 (wszystkie moduły);

• SOD, SKD;

5.System SZT musi gwarantować możliwość uruchamiania komponentów odpowiedzialnych za synchronizację (konektorów) na lokalnym serwerze SZT oraz serwerach zdalnych, gdzie uruchomione są integrowane systemy.

5.1. System SZT musi gwarantować zapewniać bezpieczeństwo i spójność przesyłanych danych pomiędzy SZT oraz konektorami uruchomionymi na zdalnych serwerach.

5.2. System SZT musi posiadać możliwość integracji z rozwiązaniami PAM (Privileged User Management) .

5.3. System SZT musi wspierać agregowanie kont i praw dostępów z systemów klasy PAM.

5.4. System SZT musi wspierać standard SCIM 2.0 w komunikacji z innymi systemami klasy IDM oraz w komunikacji z systemami zarządzanymi.

5.5. System SZT musi wspierać mechanizmy sugerowania podczas przeglądu dostępów oraz wnioskowania o dostępy poprzez przekazywanie informacji mogących pomóc użytkownikowi w podjęciu decyzji odnośnie przypisania ról i uprawnień do tożsamości.

5.6. System SZT musi pozwalać na konfiguracje i realizacje przeglądu kompozycji ról biznesowych.

6. SZT musi posiadać możliwość odzwierciedlenia struktury organizacyjnej Zamawiającego. Tożsamości muszą być możliwe do przeglądania hierarchicznie wg przypisania do struktury organizacyjnej (rozwijane drzewo struktury organizacyjnej).

6.1. SZT musi posiadać możliwość rozbudowy o kolejne jednostki organizacyjne lub redukcji w przypadku reorganizacji struktury organizacyjnej.

6.2. Architektura SZT musi uwzględniać fakt, że część systemów (aplikacji) wykorzystywanych przez Zamawiającego nie jest objęta projektem SZT wymagane jest jednak tworzenie kont użytkowników w tych systemach przy udziale administratorów tych systemów. Informacje te muszą być przechowywane w SZT.

6.3. Architektura rozwiązania zapewniać musi tworzenie unikalnych ID (loginów) dla użytkowników w SZT oraz w systemach podłączonych (IFS Applications 7.5) zgodnie z regułami stosowanymi w tych systemach.

6.4. System Zarządzania Tożsamością ma umożliwiać efektywne zarządzanie tożsamościami oraz uprawnieniami dla 14 000 użytkowników (dotyczy tożsamości aktywnych i dezaktywowanych).

6.5. SZT musi mieć możliwość dowolnego modelowania procesów workflow bez konieczności wprowadzania zmian kodu źródłowego aplikacji.

6.6. Logowanie do SZT musi być oparte o uwierzytelnienie domenowe. SZT nie może wymagać odrębnego loginu i hasła

6.7. Funkcjonalność SZT musi zapewniać możliwość konfigurowania i rozbudowy synchronizacji danych pomiędzy Centralnym Repozytorium Informacji, a systemami podłączonymi.

6.8. System SZT musi oferować mechanizm przywracania właściwych wartości w systemie podłączonym, tzn., że wszelkie zmiany naniesione w systemach podłączonych przez nieautorytatywne źródło informacji (np. administratora), powinny zostać nadpisane właściwymi wartościami atrybutów z poziomu SZT. Wywołanie tej operacji powinno być definiowane w zależności od obsługiwanego SZT.

6.9. System SZT musi umożliwiać użytkownikom dostęp do Centralnego Repozytorium, modułu WorkFlow i raportów według określonych uprawnień nadawanych przez Administratorów SZT, a także na podstawie przynależności do struktury organizacyjnej i pełnionego stanowiska. Uprawnienia muszą zarówno określać dostęp do funkcjonalności SZT jak i do zakresu dostępnych danych. W szczególności użytkownik może mieć dostęp tylko do swoich danych, ale także do danych użytkowników umiejscowionych niżej w strukturze organizacyjnej.

6.10. Dostęp do każdego z modułów (WorkFlow, raportowanie, certyfikacja, centralne repozytorium, zarządzanie hasłem itp.) musi być dostępny z poziomu portalu użytkownika.

6.11. System SZT musi dawać możliwość uruchomienia w trybie wysokiej dostępności (High Availability) w ramach ośrodków przetwarzania Zamawiającego.

7. SZT musi umożliwiać zmianę hasła w systemach powiązanych (konektor/api), tj.

• AD (logowanie Windows), Quatra, KeyCloack ;

• SZT musi umożliwiać użytkownikom samodzielną zmianę haseł w systemach powiązanych, bez udziału administratorów system informatycznego za pomocą dedykowanego narzędzia (portal lub aplikacja) poprzez mechanizm synchronizacji haseł.

7.1. SZT musi umożliwiać identyfikację tożsamości za pomocą zbioru definiowalnych pytań pomocniczych.

7.2. SZT musi wymuszać zmianę hasła w systemie powiązanym w wykonania operacji w systemie źródłowym.

7.3. Każde żądanie zmiany hasła w systemach powiązanych musi być potwierdzone w formie wiadomości e-mail na skrzynkę mailową użytkownika oraz odkładać się w logach SZT.

7.4. Samodzielna zmiana hasła (do AD i systemów powiązanych) musi być dostępna z poziomu logowania się użytkownika do systemu Windows, np. w przypadku blokady konta, zapomnienia hasła. Możliwość taka musi być oparta o odrębne mechanizmy uwierzytelnienia typu „pytanie pomocnicze”.

7.5. Wszystkie komunikaty dla użytkownika końcowego muszą być dostępne w języku polskim.

8. W ramach powyższego środowiska SZT musi spełniać wszystkie następujące wymagania niefunkcjonalne:

8.1. SZT musi posiadać wbudowane Centralne Repozytorium Informacji o użytkownikach i ich uprawnień w SI wraz z przynależnością do struktury organizacyjnej.

8.2. System SZT musi umożliwiać zarządzanie tożsamością człowieka, aplikacji, robota lub innego dowolnego bytu który posługuje się dostępami w środowisku informatycznym Zamawiającego.

8.3. System musi umożliwiać zarządzanie tożsamością z uwzględnieniem powrotu do pracy (reaktywacji) jako pracownik wewnętrzny lub zewnętrzny bez potrzeby tworzenia duplikatu tożsamości i z zachowaniem historii cyklu życia tej tożsamości.

8.4. System musi umożliwiać przetwarzanie jednej tożsamości z wieloma aktywnymi źródłami np. w przypadku pracowników którzy są zatrudnieni na więcej niż jednej umowie i posiadają przypisanie do więcej niż jednego miejsca w strukturach biznesowych. System musi obsługiwać przynależność do wielu stanowisk, wielu jednostek struktury organizacyjnej oraz wielu przełożonych jednocześnie.

8.5. Centralne Repozytorium musi dostarczać funkcjonalność selektywnego dziedziczenia uprawnień użytkownika do dowolnych obiektów. Zapewniać również definiowanie uprawnień dostępu do dowolnych obiektów w bazie danych i ich atrybutów.

8.6. Centralne Repozytorium musi umożliwić szyfrowanie co najmniej danych uwierzytelniających i haseł zarówno w trakcie transmisji, jak i zapisu na dysku (np. SSL/TLS).

8.7. Wymagana jest możliwość centralnego administrowania CRI.

8.8. Centralne Repozytorium musi zapewnić możliwość przydzielania innym użytkownikom lokalnych uprawnień administracyjnych Zarządzanie musi odbywać się przy pomocy definiowalnych ról administracyjnych.

8.9. Centralne Repozytorium musi posiadać możliwość podpinania dokumentów (plików) do tożsamości użytkownika oraz możliwości ich podglądu z poziomu SZT. SZT powinien mieć możliwość podpięcia dokumentów pod wniosek do konkretnej tożsamości.

8.10. Centralne Repozytorium docelowo będzie obsługiwać min 14 000 aktywnych tożsamości, w tym min 1 000 tożsamości firm zewnętrznych. Wykonawca w ramach wdrożenia dostarczy licencję uwzględniającą ilość aktywnych tożsamości przewidzianą przez Zamawiającego.

8.11. Każda z tożsamości (w tym zewnętrznych) musi posiadać pole/flagę "odnotowano zgodę na przetwarzanie danych osobowych" – nadawaną automatycznie przy jej tworzeniu w przypadku pracowników ARiMR.

9. System SZT musi posiadać mechanizmy przetwarzania i obsługi zdarzeń, odpowiedzialne za regulowaną synchronizację informacji o użytkownikach oraz gotowe do użycia w momencie ich wyboru i zakupu konektory do obsługi i synchronizacji kont użytkowników obsługujące następujące systemy:

• Bazy danych: Oracle, MS SQL Server, My SQL, Sybase, Postgress oraz inne za pomocą sterowników ODBC;

• Usługi katalogowe i domenowe: Microsoft Active Directory, LDAP v.3 i wyższe;

• System pocztowy: Microsoft Exchange Online(M365);

• Systemy pracy grupowej: MS SharePoint;

• Systemy operacyjne: Microsoft Windows Server (2008 i wyższe), Red Hat.

10. System SZT powinien być wyposażony w mechanizm do dwukierunkowej wymiany informacji:

10.1. Wymiana musi odwzorować zdarzenie zachodzące w jednym systemie na zdarzenie w drugim systemie.

10.2. Zdarzenie zachodzące w module nadrzędnym (np. źródłowym systemie HR-Quadra Quatra ) np. utworzenie rekordu pracownika, musi być odzwierciedlone analogicznym zdarzeniem poprzez utworzenie konta z odpowiednim hasłem w odpowiednich, podłączonych systemach.

10.3. Podobnie w sytuacji zablokowania konta użytkownika w systemie nadrzędnym - zdarzenie to musi mieć odzwierciedlenie odpowiednią akcją (blokadą) w systemach podłączonych.

10.4. Kierunek i zakres przepływu danych musi być konfigurowalny za pomocą narzędzi będących integralną częścią SZT.

11. System SZT musi być wyposażony w możliwość przydzielania i delegowania uprawnień administracyjnych związanych z możliwością konfigurowania i zarządzanie przepływem i replikacją informacji o użytkownikach w zakresie Systemu Zarządzania Tożsamością.

12. System SZT musi umożliwiać możliwość zmiany haseł w systemach podłączonych (AD, IFS Applications 7.5) z poziomu SZT oraz z poziomu logowania do systemu Windows. Sekwencja synchronizacji musi być konfigurowalna przez SZT.

13. SZT musi posiadać możliwość parametryzacji parametrów synchronizacji danych z podłączonymi systemami informatycznymi z poziomu aplikacji.

14. System SZT musi być wyposażony w możliwość przydzielania i delegowania uprawnień (do zadań, wniosków, podglądu danych itp.) w ramach zastępstw nadawanych w SZT dla innego użytkownika. Zastępujący przejmuje wszelkie uprawnienia od osoby zastępowanej.

15. Oferowane rozwiązanie musi umożliwiać zarządzanie użytkownikami z więcej niż jednym kontem (login/hasło) dla integrowanych systemów (aplikacji).

16. System SZT musi umożliwiać zarządzanie dodatkowymi kontami technicznymi użytkownika (operator, administrator, itp.). Proces zarządzania powinien być zrealizowany w oparciu o moduł Workflow.

17. Uprawnienia (dostęp) do zintegrowanych systemów informatycznych muszą być nadawane na podstawie ról zaakceptowanych w procesie wnioskowania.

18. System SZT powinien umożliwiać tworzenie Profili uprawnień przypisanych do stanowisk lub do struktury organizacyjnej Zamawiającego.

19. System SZT musi umożliwiać tworzenie profili uprawnień dla użytkowników wraz ze ścieżkami akceptacji tych profili przez wskazanych użytkowników lub grupy użytkowników.

20. System SZT musi umożliwiać zmianę jednostki organizacyjnej lub stanowiska przez pracownika z uwzględnieniem automatycznego odebrania/nadania uprawnień wynikających z takiej zmiany (opcjonalnie wymuszając proces przegląd uprawnień).

21. System SZT musi zapewnić możliwość monitorowania i raportowania przypisanych ról do tożsamości użytkowników, w szczególności tych, które dają dostęp do kont uprzywilejowanych.

22. Nadawanie uprawnień do kont może być bezterminowe lub ograniczone w czasie (obowiązuje data wygaśnięcia takiego uprawnienia).

23. System SZT musi posiadać wbudowane mechanizmy do realizacji obiegów akceptacyjnych i zatwierdzania ról oraz dostępu i uprawnień w podłączonych systemach.

23.1. Moduł Workflow musi być integralną częścią SZT i pochodzić od tego samego producenta.

23.2. Moduł Workflow musi zapewniać możliwość budowania jedno lub wielostopniowego rozgałęzionego procesu akceptacyjnego do nadawania dostępu do dowolnego systemu/zasobu w jednym wniosku.

23.3. Moduł Workflow musi zapewniać możliwość zbudowania jedno lub wielostopniowego rozgałęzionego procesu akceptacyjnego do nadawania roli dla dowolnego użytkownika.

23.4. Moduł Workflow musi być oparty na technologii WWW.

23.5. Moduł workflow musi być integralną częścią dostarczanego SZT i korzystanie z niego nie może wymagać ponownego logowania.

23.6. System SZT musi zapewniać użytkownikowi końcowemu obsługę portalu użytkownika SZT i Workflow w języku polskim. Wszystkie elementy interfejsu użytkownika, komunikaty systemowe, opisy, treść pomocy itp. (np. tzw. tooltip). muszą być dostępne w języku polskim.

23.7. Mechanizm powiadamiania wykorzystywany przez SZT oraz Workflow musi oferować możliwość tworzenia szablonów komunikatów w języku polskim.

23.8. Moduł Workflow powinien zawierać mechanizm umożliwienia osobie wydającej decyzję na delegowanie obsługi wszystkich przydzielonych procesów innej osobie na czas określony (tzw. zastępstwa). Funkcjonalność dostępna z poziomu administratora i użytkownika dla wszystkich użytkowników.

23.9. Moduł Workflow musi zawierać mechanizm umożliwienia osobie wydającej decyzję na delegowanie wybranego procesu (lub procesów) innej osobie.

23.10. Moduł Workflow musi posiadać funkcjonalność umożliwiającą zdefiniowanie procesu akceptacji w sposób równoległy (tj. w taki sposób, aby w jednym wniosku można było obsłużyć akceptację częściową, np. akceptowane są tylko 2 z 3 wnioskowanych obiektów) lub sekwencyjny (stopniowy). Każdy efekt decyzji musi być odwzorowany zarówno w śladzie audytowym oraz raportach.

23.11. Mechanizmy workflow musi zapewnić możliwość przypisania nadawania uprawnień dostępu lub roli na ściśle określony i wybrany w trakcie akceptacji okres.

23.12. Workflow musi dostarczać środowisko graficzne, w którym istniała będzie możliwość przeprowadzenia operacji konfiguracji i planowania procesu oraz ścieżki akceptacyjnej w sposób graficzny.

23.13. Moduł Workflow musi monitować użytkowników (zakładać zadanie dla administratora SI, wysyłać komunikat), konieczność odebrania uprawnień przyznanych na określony czas (szczególnie gdzie integracja nie jest pełna), częstotliwość i okres wysyłania monitów musi być konfigurowalny i jednolity dla wszystkich wygasających uprawnień

23.14. System SZT musi zapewniać możliwości tworzenia raportów przedstawiających pełną ścieżkę akceptacyjną dla potrzeb audytu.

23.15. Moduł Workflow musi zapewnić użytkownikom (inicjatorom) możliwość monitorowania procesu akceptacji nadawania uprawnień.

23.16. Moduł Workflow musi dysponować funkcjonalnością zezwalającą na wprowadzanie zmian w procesie akceptacyjnym. Naniesione zmiany powinny być uwzględnione wraz z rozpoczęciem nowego procesu.

23.17. Moduł Worflow powinien mieć możliwość konfiguracji dostępnych opcji dla użytkownika w zależności od jego uprawnień.

23.18. SZT powinien mieć możliwość konfiguracji modułu workflow i ograniczenie dla wybranych użytkowników możliwości inicjowania wniosków.

23.19. Moduł Worflow musi mieć możliwość tworzenia grup i administratorów (managerów) dla tych grup z określonymi uprawnieniami ograniczonymi tylko do zarządzania wnioskami i rolami dla poszczególnej grupy.

23.20. Moduł Workflow musi posiadać możliwość tworzenia własnych formularzy do wnioskowania oraz akceptacji nadawania uprawnień.

23.21. Moduł Workflow musi posiadać możliwość podpinania dokumentów określonego typu (słownik określony w SZT) - plików w formacie pdf, doc, xls, zip do wniosków o dostępy (a rezultacie końcowym do tożsamości użytkownika).

23.22. SZT musi pozwalać na generowanie szablonów dokumentów (upoważnień, pełnomocnictw) na określonym kroku w procesie wraz z uzupełnionymi danymi pracownika i wnioskowanymi uprawnieniami.

23.23. Moduł Workflow powinien umożliwiać zwrócenie wniosku do inicjatora celem uzupełnienia.

23.24. System SZT musi zapewniać możliwość definiowania ról powiązanych z określonymi uprawnieniami użytkownika w zintegrowanych systemach informatycznych i aplikacjach.

23.25. Rola (wyższego poziomu) musi umożliwiać objęcie zasięgiem uprawnień w kilku odrębnych systemach I aplikacjach.

23.26. System SZT musi mieć możliwość nadawania, odbierania i modyfikowania ról przydzielonych użytkownikowi.

23.27. Obsługa ról musi uwzględniać możliwość definicji na dowolnym poziomie hierarchii uprawnień ról wzajemnie wykluczających się oraz system musi mieć możliwość kontrolowanego (akceptacja) nadawania ról, które się wzajemnie wykluczają ze względu na separację obowiązków.

23.28. System SZT musi posiadać wbudowany mechanizm ostrzegający przed nadawaniem użytkownikowi ról, które zostały zdefiniowane jako wzajemnie się wykluczające.

23.29. Obsługa ról musi umożliwiać definicję ról hierarchicznych, to znaczy musi istnieć możliwość definicji w SZT ról jako sumy innych ról.

23.30. System SZT musi mieć możliwość nadania użytkownikowi określonej roli na określony czas.

23.31. System SZT musi dawać możliwość użytkownikowi przeglądania informacji o przydzielonych rolach w portalu użytkownika.

23.32. System SZT musi dawać możliwość użytkownikowi jak i jego przełożonemu wnioskowania o rolę oraz śledzenia statusu tego wniosku.

23.33. System SZT musi mieć możliwość tworzenia raportów/zestawień ze wszystkich nadanych lub odebranych użytkownikowi ról (wraz ze wszystkimi danymi o danej tożsamości). W raporcie powinny być również widoczne osoby akceptujące te operacje wraz z datami poszczególnych operacji.

23.34. System SZT musi umożliwiać składanie wniosków o przydzielenie roli zarówno pracownikowi jak i przełożonemu pracownika. Przełożony musi mieć możliwość wnioskowania o przydział roli dla swoich podwładnych. Każdy przełożony ma dostęp do listy rozwijanej podwładnych. Domyślnie lista powinna być ograniczona do bezpośrednich podwładnych z możliwością rozwinięcia do wszystkich podwładnych według przynależności do struktury organizacyjnej.

23.35. System SZT musi umożliwiać budowę zaawansowanych (wielostopniowa akceptacja) obiegów workflow z akceptacją dla wniosku o przydział roli.

23.36. System SZT musi posiadać graficzną konsolę obsługiwaną przez określone przeglądarki umożliwiającą odczytanie aktualnych ról użytkownika.

23.37. Dostarczany System SZT musi wspierać procesy dodawania, modyfikowania oraz usuwania ról w oparciu o proces akceptacyjny.

23.38. System SZT musi wspierać okresową re-certyfikację uprawnień użytkowników, udokumentowaną odpowiednimi raportami.

23.39. System SZT musi posiadać możliwość ograniczenia przetwarzania danych np. tylko do podglądu, tylko do edycji. Wskazane przez administratora operacje muszą odkładać się w logach SZT i być dostępne z poziomu aplikacji.

23.40. System SZT musi pozwalać na konfigurację praw dostępów z systemów klasy PAM poprzez standardowy model ról biznesowych w oparciu o przypisywanie i odbieranie ról biznesowych tożsamościom.

23.41. System SZT musi pozwalać na nadawanie ról i uprawnień czasowo: od - do. Po osiągnięciu czasu "do" system musi automatycznie odbierać obiekty oraz wynikające z nich dostępy.

24. System SZT musi posiadać wbudowany i zintegrowany moduł raportowania i audytu dostarczony przez tego samego producenta, który dostarcza główny system zarządzania tożsamością.

24.1. System SZT musi zbierać i przechowywać informacje o użytkownikach i ich kontach oraz uprawnieniach w podłączonych SI, a także wszystkich operacjach i plikach powiązanych bezpośrednio lub pośrednio (przez wnioski) z tożsamością.

24.2. System SZT musi mieć możliwość automatycznego uruchamiania przygotowanych wcześniej raportów o tożsamości użytkowników w określonych dowolnie definiowanych porach i dniach oraz mieć możliwość automatycznego wysyłania tych raportów za pomocą poczty elektronicznej (e-mail).

24.3. System SZT musi mieć możliwość tworzenia raportów o wnioskach workflow i przydzielanych użytkownikowi rolach i profilach (uprawnieniach).

24.4. Musi istnieć możliwość przeglądania informacji i zdefiniowanych wcześniej harmonogramach generowania raportów.

24.5. System SZT musi udostępniać możliwość samodzielnego definiowania wzorców raportów oraz ich eksportu do plików xls (lub csv), pdf.

24.6. Musi istnieć możliwość przygotowania wzorców raportów w języku polskim.

24.7. Musi istnieć możliwość dowolnej edycji i modyfikacji standardowych wzorców raportów dostarczonych przez producenta SZT z użyciem narzędzi wbudowanych w system.

24.8. System SZT w czasie rzeczywistym musi umożliwiać wgląd w dane historyczne związane z wnioskami, uprawnieniami i rolami, o które wnioskował użytkownik. SZT musi umożliwiać raportowanie tych danych w sposób definiowalny.

24.9. System SZT musi mieć możliwość wykrywania operacji zakładania lub modyfikacji kont i/lub grup użytkowników w MS Active Directory, które są realizowane poza (z pominięciem) Systemem Zarządzania Tożsamością. Po wykryciu cytowanych operacji system musi mieć możliwość realizacji każdej z tych akcji (razem lub osobno):

24.10. wysłania powiadomienia e-mailem do wyznaczonej osoby z podaniem podstawowych informacji o koncie;

24.11. uruchomienia obiegu workflow z określonym zdefiniowanym w systemie procesem automatycznego usunięcia takiej nieuprawnionej zmiany i operacji w MS AD.

24.12. Dla systemów z provisioningiem System SZT musi mieć możliwość wykrywania operacji dodawania, usuwania, blokowania, odblokowania kont użytkowników, dodawania i usuwania uprawnień, które są realizowane poza (z pominięciem) Systemem Zarządzania Tożsamością. Po wykryciu cytowanych operacji system musi mieć możliwość realizacji każdej z tych akcji (razem lub osobno):

24.13. wysłania powiadomienia e-mailem do wyznaczonej osoby z podaniem podstawowych informacji o koncie / uprawnieniu

24.14. System zbierania zdarzeń musi posiadać wydajność i pojemność umożliwiającą obsługę zdarzeń zachodzących w SZT w zakresie:

• błędne i poprawne zalogowania do SZT;

• każda zmiana, dodanie lub usunięcie tożsamości i uprawnień użytkownika;

• każda zmiana, dodanie lub usunięcie użytkownika systemu SZT;

• każdy krok procesów workflow zaimplementowanych w SZT;

• błędy i ostrzeżenia zachodzące w czasie komunikacji z systemami podłączonymi;

• błędy i ostrzeżenia związane z pracą komponentów SZT;

• informacje diagnostyczne związane z pracą SZT;

• ostrzeżenia dot. przekroczenia limitów wykorzystania licencji;

• wszystkie inne zdarzenia wymagane do realizacji procedur procesu zarządzania tożsamością lub zostaną określone w Projekcie Technicznym;

• Okres retencji logów nie może być krótszy niż 24 miesiące;

• Musi również istnieć możliwość pobierania danych z systemów i aplikacji (np. za pomocą konektorów do plików płaskich), które nie są bezpośrednio zarządzane przez System Zarządzania Tożsamością.

24.15. SZT musi rejestrować zmiany w tożsamości użytkowników (zmiana nazwiska, identyfikatora pracownika).

24.16. SZT musi rejestrować i przechowywać informacje o realizowanych wnioskach workflow i przydzielanych użytkownikowi rolach, profilach.

24.17. SZT musi umożliwiać raportowanie po każdym z parametrów tożsamości, wniosków, strukturze organizacyjnej i typów dokumentów przypisanych do tożsamości bezpośrednio lub pośrednio przez wnioski.

24.18. Wszystkie komunikaty w aplikacji użytkownika końcowego muszą być dostępne w języku polskim.

24.19. Wszystkie określone przez administratora SZT działania użytkowników (podgląd/edycja/usunięcie) muszą odkładać się w logach SZT dostępnych z poziomu aplikacji.

25. Opis Systemów Informatycznych objętych integracją z SZT:

25.1. W ramach wdrożenia SZT integracją zostaną objęte poniższe systemy informatyczne funkcjonujące w ARiMR, część z nich będzie wymagała budowy konektora, a znaczna większość będzie dotyczyć tylko obiegu wniosków z nimi związanych:

• Active Directory (konektor),

• KeyCloack,

• Quatra,

• PAM CyberArk

• Cisco ISE.

25.2. Zamawiający korzysta z usługi Microsoft Active Directory do zarządzania kontami użytkowników oraz dostępem do zasobów środowiska informatycznego. Usługa Active Directory jest podstawowym źródłem informacji o użytkownikach i nie jest uzależniona w tym względzie od innych systemów. Active Directory stanowi również podstawę do zarządzania kontami pocztowymi Exchange.

1. W chwili obecnej AD zawiera ok 11 500 kont użytkowników, których loginy są utworzone w konwencji nazwisko\_imie.
2. W docelowym systemie grupy Active Directory będą ścisłym odwzorowaniem struktury organizacyjnej firmy, a przynależność użytkownika do grupy będzie definiowana na podstawie jego stanowiska i komórki zatrudnienia, a także uprawnień nadanych w SZT.
3. Dodatkowo będą wykorzystywane grupy zabezpieczeń do projektów międzywydziałowych. Ich przynależność będzie ustalana przez dedykowane procedury w SZT.
4. Zakres integracji z SZT:
* Zakładanie kont dla nowo utworzonych użytkowników (źródłem informacji o użytkowniku będzie moduł kadrowy Quadra).
* Dodawanie użytkowników do grup AD przynależnych komórce zatrudnienia.
* Tworzenie grup AD na podstawie procesu SZT.
* Wyłączanie konta zwolnionego pracownika.
* Przenoszenie kont użytkowników w przypadku zmiany komórki zatrudnienia.
* Powyższe informacje muszą być przekazane zwrotnie do SZT wraz z odpowiednim statusem realizacji lub jego braku (wraz z podaniem przyczyny błędu).

25.3. System pocztowy Microsoft Exchange Online (konektor).

1) System Exchange wykorzystywany jest do obsługi poczty elektronicznej oraz jako centralna, elektroniczna książka adresowa. System Exchange bazuje na głównej usłudze Active Directory i jest z tą usługą ściśle zintegrowany.

2) Zakres integracji Microsoft Exchange Online z SZT:

• Założenie skrzynki pocztowej dla nowego pracownika.

• Ukrycie, dezaktywacja skrzynki lub archiwizacja skrzynki dla zwolnionego pracownika..

• Zarzadzanie uprawnieniami dla skrzynek aplikacyjnych.

• Tworzenie i modyfikacja grup dystrybucyjnych.

• Powyższe informacje muszą być przekazane zwrotnie do SZT wraz z odpowiednim statusem realizacji lub jego braku (wraz z podaniem przyczyny błędu).

25.4. System kadrowy Quatdra Max (konektor).

1) System kadrowy wspierający Agencję w obszarach:

• finanse;

• kadry-płace;

• personel;

• logistyka;

• portal pracownika;

• obieg dokumentów

2) Zakres integracji system Quatra Max z SZT:

* Wymagana jest pełna integracja (automatyczne zarządzanie kontami i uprawnieniami bez udziału administratorów tego systemu) z systemem kadrowym, tj.: Rejestracja tożsamości na podstawie danych pracownika z modułu Kadry-Płace;
* Zakładanie i parametryzacja kont;
* Nadawanie/odbieranie uprawnień;
* 25Blokowanie/usuwanie kont;
* 25.8.2.5. Przegląd uprawnień;
* 25.8.2.6. Przy przekazywaniu powyższych informacji w SZT musi być zachowywany status realizacji lub jego braku (wraz z podaniem przyczyny błędu)..

25.5 System SSO Keycloak

1)Wymagana jest pełna integracja (automatyczne zarządzanie kontami i uprawnieniami bez udziału administratorów tego systemu).

25.6 System Cisco ISE.

1)Wymagana jest pełna integracja (automatyczne zarządzanie kontami i uprawnieniami bez udziału administratorów tego systemu).

26. W ramach SZT wymagana jest także obsługa uprawnień w systemach informatycznych, do których nie będą budowane konektory. Muszą być jednak zewidencjonowane w SZT i brać udział w obiegu wniosków. Zarządzanie uprawnieniami w tych systemach będzie realizowane ręcznie przez administratorów. W ramach obiegu wniosku wymagane będzie wystawienie zlecenia w systemie do obsługi zgłoszeń IT, polegające na wysłaniu maila na odpowiednią skrzynkę mailową z treścią wniosku oraz linkiem do wniosku w SZT. SZT musi posiadać możliwość ręcznej modyfikacji uprawnień przypisanej Tożsamości w ramach tych systemów (dodaj/usuń). SZT musi zostać zasilony danymi o informacje o kontach wraz z uprawnieniami, które Zamawiający udostępni za pomocą plików płaskich. Udział w obiegu wniosków będą brały poniższe Systemy Informatyczne:

27. Zamawiający zakłada rozbudowę integracji SZT z nowymi systemami. Wykonawca ma zapewnić w systemie mechanizmy pozwalające na rozbudowę SZT zgodnie z wymaganiami określonymi w wymaganiach funkcjonalnych w niniejszym Załączniku.

28. Opis funkcjonalności Systemu Zarządzania Tożsamością (SZT).

28.1. SZT w szczególności musi wspierać następujące procedury:

1) Tworzenie, przetwarzanie, przechowywanie, usuwanie informacji o tożsamościach użytkowników.

2) Tworzenie wniosków (o uprawnienia oraz nadawanie / modyfikacje / odbieranie uprawnień) oraz ich obieg.

3) Tworzenie, przetwarzanie, przechowywanie, usuwanie informacji o uprawnieniach w oparciu o role i uprawnienia.

4) Nadawanie szczególnych uprawnień w sytuacjach kryzysowych.

5) Okresową re-certyfikacja uprawnień w systemach informatycznych.

6) Realizacja audytu uprawnień w poszczególnych systemach informatycznych.

7) Realizacja delegowania uprawnień pomiędzy użytkownikami SZT.

8) Kopiowanie uprawnień z tożsamości na tożsamość.

9) Monitorowanie uprawnień w systemach informatycznych.

10) Badanie zgodności posiadanych przez użytkowników systemów informatycznych

 uprawnień pod kątem spełnienia polityk i regulaminów.

11) Zmiany predefiniowanej struktury organizacyjnej w systemie.

29. SZT w ramach Wdrożenia musi zostać zintegrowany z poniższymi systemami informatycznymi obecnie funkcjonującymi u Zamawiającego :

• Active Directory;

• Microsoft Exchange Online

• Quatra - System Kadrowy;

• System KeyCloak;

• Cisco ISE;

• PIM/PAM CyberArk

30. SZT musi także umożliwiać integrację z innymi, wskazanymi przez Zamawiającego systemami IT np. geoportalem oraz systemem PUDOR.

31. Nadawanie, modyfikowanie oraz odbieranie uprawnień w Systemie KeyCloak będzie odbywać się w sposób automatyczny – poprzez konektor do SZT.

32. W procesie zarządzania tożsamością autorytarnym źródłem informacji o tożsamościach będzie moduł kadrowy w systemie Quatra oraz w wyjątkowych sytuacjach dane wprowadzane przez uprawnionego pracownika poprzez formularz bezpośrednio do SZT.

IV. Wdrożenie

1) Przygotowanie 3 odrębnych środowisk - produkcyjnego (PROD), testowo-szkoleniowego (TEST) i deweloperskiego (DEV),

2) w ramach przygotowania środowisk zainstalowania oprogramowania / pakietów usług / komponentów na serwerach Zamawiającego (środowisko PROD i TEST),

3) przygotowanie odpowiedniej struktury danych do przechowywania użytkowników SZT oraz struktury organizacyjnej na środowisku testowo-szkoleniowym a następnie przeniesienia jej na środowisko produkcyjne,

4) budowy katalogów profili i ról (zdefiniowanie ról i profili zgodnie z Projektem technicznym), oraz implementacji wykluczeń w uprawnieniach, przypisania konkretnych ról i uprawnień do tożsamości,

5) zasilenie repozytorium danych udostępnionymi przez Zamawiającego danymi na środowisku testowo-szkoleniowym a następnie migracja danych na środowisko produkcyjne,

6) budowy i konfiguracji konektorów do systemów objętych integracją (Active Directory, Quatra - System Kadrowy, System KeyCloak, Cisco ISE),

7) konfiguracji portalu użytkownika na środowisku testowo-szkoleniowym a następnie przeniesienia jej na środowisko produkcyjne,

8) implementacji procesu obiegu wniosków zgodnie z Projektem technicznym na środowisku testowo-szkoleniowym a następnie przeniesienia jej na środowisko produkcyjne,

9) przygotowania konfiguracji raportowania SZT na środowisku testowo-szkoleniowym a następnie przeniesienia jej na środowisko produkcyjne,

10) przygotowania konfiguracji kont użytkowników SZT (w tym kont technicznych): administratorów i operatorów na środowisku testowo-szkoleniowym a następnie przeniesienia jej na środowisko produkcyjne,

11) integracji z systemami informatycznymi obecnie funkcjonującymi w ARiMR:Active Directory, Quatra - System Kadrowy, System KeyCloak, Cisco ISE,

12) uruchomienia produkcyjnego SZT,

13) przeprowadzenia procesu re-certyfikacji,

14) wykonania i dostarczenia Projekt Technicznego, Dokumentację powykonawczej, Dokumentacji eksploatacyjnej oraz Planu Testów Akceptacyjnych,

15) Przeprowadzenia warsztatów dla administratorów oraz kluczowych użytkowników ARiMR.