Ogłoszenie o zamiarze przeprowadzenia dialogu technicznego z potencjalnymi wykonawcami systemu do Zarządzania Tożsamością poprzedzającego ogłoszenie postępowania o udzielenie zamówienia publicznego na wykonanie Systemu Zarządzania Tożsamością na potrzeby projektu pn. „Wdrożenie nowych i modernizacja posiadanych technologii informacyjno-komunikacyjnych w WWCOiT im. M. Kopernika w Łodzi", zwane też „Ogłoszeniem".

Podstawa prawna: art. 31a i art. 31b ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t. j.: Dz. U. z 2018 r., poz. 1986 z późn. zm.), zwanej dalej „ustawą". Wszelką korespondencję kierowaną do Zamawiającego należy opatrzyć dopiskiem: *„Dialog techniczny – Zarządzanie Tożsamością".*

1) DANE KONTAKTOWE ZAMAWIAJĄCEGO

1. Nazwa i adres Zamawiającego

Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi, zwane dalej Zamawiającym.
Adres do korespondencji:
Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi
Dział Informatyki
ul. Pabianicka 62, 93-513 Łódź

2. Osoby wyznaczone do kontaktu

Piotr Błasiak, Jacek Filipczak; tel.: 42 207-44-91
Tomasz Zdzianicki; tel.: 42 207-44-55
e-mail: dialogi_informatyka@kopernik.lodz.pl

Wszelką korespondencję kierowaną do Zamawiającego należy opatrzyć dopiskiem: **„Dialog techniczny związany z postępowaniem o udzielenie zamówienia publicznego na** wykonanie Systemu Zarządzania Tożsamością na potrzeby projektu pn. „Wdrożenie nowych i modernizacja posiadanych technologii informacyjno-komunikacyjnych w WWCOiT im. M. Kopernika w Łodzi",

Użyte w ogłoszeniu sformułowania zostały zdefiniowane w pkt 1 „Regulaminu Przeprowadzania Dialogu Technicznego"

2) PODSTAWA PRAWNA

Dialog techniczny prowadzony jest na podstawie art. 31a - 31c ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2018 r. poz. 1986, ze zm.) oraz zgodnie z „Regulaminem przeprowadzania dialogu technicznego" opublikowanym na stronie internetowej Zamawiającego.

3) OKREŚLENIE PRZEDMIOTU DIALOGU TECHNICZNEGO

1. Zamawiający ogłasza dialog techniczny w związku z przygotowywaniem postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest wykonanie Systemu Zarządzania Tożsamością na potrzeby projektu pn. „Wdrożenie nowych i modernizacja posiadanych technologii informacyjno-komunikacyjnych w WWCOiT im. M. Kopernika w Łodzi.
2. Celem dialogu technicznego (zwanego też „dialogiem") będzie uzyskanie informacji w zakresie niezbędnym do przygotowania postępowania o udzielenie zamówienia publicznego (opisu przedmiotu zamówienia, specyfikacji istotnych warunków zamówienia oraz określenia istotnych warunków umowy).
3. Dialog techniczny służyć będzie zapoznaniu się Zamawiającego z najnowszymi rozwiązaniami funkcjonalnymi, technicznymi oraz organizacyjnymi w dziedzinie właściwej dla zamówienia, a także skonfrontowaniu potrzeb Zamawiającego z możliwościami ich realizacji.
4. Dialog techniczny prowadzony będzie w języku polskim i ma charakter jawny, z zastrzeżeniem § 6 „Regulaminu przeprowadzania dialogu technicznego". Do dokumentów sporządzonych w innych językach niż polski powinny być dołączone tłumaczenia na język polski.
5. Termin zakończenia dialogu przewidywany jest do 15 marca 2019 r., jednak okres ten może zostać zmieniony.
6. Wstępna Koncepcja Systemu Zarządzania Tożsamością znajduje się w załączniku nr 1 do ogłoszenia.

do dnia 19.02.2019 r. do godz. 10:00 w Kancelarii Szpitala na formularzu stanowiącym Załącznik nr 2. Koperta powinna być zatytułowana **„Wniosek do udziału w dialogu technicznym dla Systemu Zarządzania Tożsamością" oraz mailem na adres dialogi_informatyka@kopernik.lodz.pl**

2. Zamawiający zaprosi do udziału w dialogu maksymalnie 5 podmiotów, które uzyskają najwyższą liczbę punktów, zgodnie ze wskazaniem poniżej:
   Maksymalna liczba punktów do uzyskania to 10:
   a) Wykonawca wdrożył system informatyczny umożliwiający pełne zarządzanie Tożsamością pracowników – 1 pkt za każde dodatkowe ponad wskazane w ppkt 9. **pkt 4)** wdrożenie (maksymalnie można przedstawić 5 wdrożeń)
   b) System określony w pkt a) posiadał integrację z usługą Microsoft AD Zamawiającego – dodatkowo 1 pkt za każde takie wdrożenie.

   W przypadku uzyskania takiej samej liczby punktów przez co najmniej 2 podmioty, rozstrzygającym kryterium będzie wielkość podmiotów, w których wdrożono systemy (ilość pracowników objętych systemem).
3. Ocena warunków będzie się odbywać w oparciu o złożenie stosownych oświadczeń we wniosku o dopuszczenie do udziału w dialogu.
4. Po zakończeniu oceny wniosków Zamawiający prześle drogą elektroniczną Uczestnikom dopuszczonym do udziału w dialogu zaproszenie do dialogu oraz informacje o niedopuszczeniu do dialogu dla uczestników którzy nie zostali zakwalifikowani. Zamawiający dopuszcza możliwość zmiany terminu przesłania Uczestnikom zaproszenia do udziału w dialogu z jednoczesną stosowną zmianą kolejnych terminów.
5. W odpowiedzi na zaproszenie do udziału w dialogu, każdy Uczestnik zaproszony do udziału w dialogu zobowiązany będzie do przesłania Zamawiającemu w terminie do 5 dni od otrzymania zaproszenia do udziału w dialogu opracowania merytorycznego zawierającego przedstawienie syntetycznych informacji dot. poszczególnych zagadnień opisanych w Załączniku nr 1 (koncepcji) Ogłoszenia. Opracowanie merytoryczne powinno zostać przekazane w postaci edytowalnego pliku tekstowego o objętości max 50 stron A4 (czcionka Arial 11, akapit 1,5). Dokumenty należy przesłać w formie i na adres wskazany w **pkt 5)** ppkt 1.
6. Nieprzesłanie przez Uczestnika zaproszonego do udziału w dialogu opracowania, o którym mowa powyżej lub przesłanie jedynie samej struktury zagadnień będzie rozumiane jako odmowa wzięcia udziału w spotkaniach dialogowych.
7. Zamawiający w toku oceny wniosków o dopuszczenie do udziału w dialogu oraz merytorycznych materiałów wstępnych ma prawo wezwać Uczestnika do złożenia wyjaśnień i/lub uzupełnień dotyczących przekazanych materiałów, w terminie przez siebie wyznaczonym.
8. Zamawiający zamierza prowadzić dialog techniczny z potencjalnymi wykonawcami poprzez indywidualne spotkania z każdym z Uczestników zaproszonych do udziału w dialogu. Zamawiający planuje przeprowadzenie trzygodzinnych indywidualnych spotkań z każdym z Uczestników w miesiącu lutym i marcu, w ustalonych przez obie strony terminach. Zamawiający dopuszcza możliwość zmiany zaproponowanych terminów. Zamawiający dopuszcza możliwość przeprowadzenia spotkania/spotkań zbiorowych z Uczestnikami.

6) ZASADY PROWADZENIA DIALOGU TECHNICZNEGO

1. Dialog techniczny będzie prowadzony zgodnie z postanowieniami Regulaminu przeprowadzenia dialogu technicznego", stanowiącego załącznik nr 4 do niniejszego ogłoszenia.
2. Dialog techniczny będzie prowadzony w sposób zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie jego uczestników oraz przyszłych oferentów i oferowanych przez nich rozwiązań, w szczególności Zamawiający przekaże pozostałym wykonawcom informacje, które uzyskał i przekazał podczas przygotowania postępowania.
3. Dialog techniczny będzie prowadzony w języku polskim.
4. Zamawiający przewiduje, że dialog techniczny będzie prowadzony do czasu przesłania informacji o zakończeniu dialogu, w formie spotkań w siedzibie Zamawiającego, wymiany e-maili i/lub telekonferencji. Zamawiający zastrzega możliwość wymiany korespondencji z Uczestnikami także po zakończeniu rund/spotkań.
5. Przystępujący do dialogu technicznego udziela zgody na wykorzystanie przez Zamawiającego przekazanych informacji w przygotowaniu opisu przedmiotu zamówienia, specyfikacji istotnych warunków zamówienia, innych dokumentów wynikających z procedury udzielania zamówienia publicznego, dokumentacji aplikacyjnej dla projektu oraz określeniu warunków umowy.
6. Zamawiający nie ujawni w toku Dialogu ani po jego zakończeniu informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz. U. 2003 Nr 153, poz. 1503 ze zm.), jeżeli Uczestnik, nie później niż wraz z przekazaniem informacji Zamawiającemu, zastrzegł, że przekazywane informacje nie mogą być udostępniane innym podmiotom, z zastrzeżeniem ppkt 5..
7. Zamawiający informuje, iż przeprowadzenie dialogu technicznego nie rodzi po stronie Zamawiającego obowiązku wszczęcia postępowania o udzielenie zamówienia publicznego objętego dialogiem technicznym.

– prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
– **na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO**.

* ***Wyjaśnienie:*** *skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

** ***Wyjaśnienie:*** *prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*

8) WYKAZ ZAŁĄCZNIKÓW

1. Załącznik nr 1 – Wstępna Koncepcja ~~platformy regionalnej~~
2. Załącznik nr 2 – Wniosek o dopuszczenie do udziału w dialogu
3. Załącznik nr 3 – Oświadczenie o poufności
4. Załącznik nr 4 – Regulamin przeprowadzania dialogu technicznego

Z-ca STĘPCA DYREKTORA
ds. Leczniczych

System zarządzania tożsamością

Zaawansowane zarządzanie cyklem życia roli

System Zarządzania Tożsamością powinien cechować się innowacyjnym i solidnym mechanizmem wykrywania ról oraz zarządzania ich cyklem życia. SYSTEM powinien zapewniać osobom odpowiedzialnym za zarządzanie bezpieczeństwa tworzenie i modyfikacje ról użytkowników, które odzwierciedlają niezbędne uprawnienia jakie należy przydzielić pracownikom. SYSTEM powinien posiadać również wbudowane narzędzie analityczne, które umożliwia przeprowadzenie analizy bezpieczeństwa w zakresie przydzielonych w systemach informatycznych uprawnień. Wynikiem takiej analizy ma być opracowanie ról użytkowników, którzy realizują określone zadania w tych systemach wskazując poprawny pod względem niezbędności zakres uprawnień dla określonej grupy użytkowników oraz każdego użytkownika indywidualnie. Uwzględniając liczbę użytkowników mnogość systemów informatycznych zakres analizy dotyczy setek tysięcy pojedynczych uprawnień we wszystkich systemach. System ma zapewnić wyeliminowanie nadmiarowych uprawnień, jakie omyłkowo mogły zostać przydzielone użytkownikom. Proces taki stanowi spełnienie podstawowych wymagań określonych w zasadach bezpieczeństwa zawartych m.in. w OPBI (zatwierdzonej przez Zarząd Województwa Łódzkiego):

-> **Zasada przywilejów koniecznych** - Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;

-> **Zasada wiedzy koniecznej** - Każdy pracownik posiada wiedzę o systemie do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań

Uwzględniając liczbę użytkowników, mnogość systemów informatycznych zakres analizy dotyczy setek tysięcy pojedynczych uprawnień w systemach informatycznych użytkowanych w Szpitalu. W związku z tym przeprowadzenie takiej analizy „ręcznie" bez aplikacyjnego narzędzia jakim jest powyżej opisany proces jest praktycznie niemożliwe.

SYSTEM musi umożliwiać przeaudytowanie aktywności użytkowników na poszczególnych rolach. Wszystkie odstępstwa od określonych reguł muszą zostać zatwierdzone przez osoby odpowiedzialne za właściwy poziom bezpieczeństwa, a w przypadkach nieuzasadnionych – wycofane.

Wieloetapowy proces akceptacyjny

Zgodnie z Polityką Bezpieczeństwa Informacji obowiązującą w Szpitalu w procesie przydzielania pracownikowi aktywów oraz uprawnień uczestniczy jego bezpośredni przełożony. Zmiany wprowadzone do systemów informatycznych muszą być zrealizowane zgodnie z obowiązującymi procedurami. Na dzień dzisiejszy procesy tego typu są realizowane w sposób tradycyjny w oparciu o wnioski w wersji papierowej. W ramach przedmiotowego systemu planowane jest realizowanie procesów przy udziale systemu. Zatem system musi umożliwiać dostosowanie procesu akceptacji wniosków o uprawnienie (rolę) do potrzeb Szpitala oraz umożliwiać utworzenie wieloetapowych, wieloosobowych procesów akceptacyjnych zgodnych z zasadami określonymi przez Politykę Bezpieczeństwa i procedury wewnętrzne. Planowane rozwiązanie musi spełniać te wymogi, umożliwiać wprowadzenie złożonego zapytania wnioskowego oraz złożonego procesu akceptacyjnego opartego o akceptacje pochodzące od wielu osób np. Kierownika, Administratora Bezpieczeństwa Informacji, Dyrektora.

Łatwa Certyfikacja Tożsamości

W miarę wprowadzenia coraz większej ilości aplikacji i rozwoju Organizacji, certyfikacja – czyli proces weryfikacji uprawnień – staje się coraz bardziej niezbędną i bardziej złożona. Proces certyfikacji uprawnień musi być automatyczny, szybki, wspierany analizą ryzyka i prosty w obsłudze. Podczas procesu Certyfikacji Tożsamości (przeprowadzenie audytu zgodności) system musi nie tylko udostępniać informacje o tym „kto ma jakie uprawnienie", ale również dogłębna analiza musi zostać zobrazowana w formie grafów, pozwolić na szybkie odebranie uprawnienia, pokazać całą ścieżkę i historię akceptacji, nakreślić niezgodności. Certyfikacja ma zostać wykonana przez pojedynczą jednostkę, jak również np. przez kooperujące ze sobą działy IT, Bezpieczeństwa

oraz Biznesu. Proces Certyfikacji musi być przeprowadzany przy udziale Kierowników poszczególnych obszarów (kierowników komórek organizacyjnych), którzy są odpowiedzialni za realizację określonych zadań przez komórki organizacyjne. Kierownicy określają potrzeby w zakresie przydzielanych personelowi uprawnień a system musi umożliwiać monitorowanie i analizę zasadność jak również poprawności przydzielonych uprawnień.

Zarządzanie kontami uprzywilejowanymi

Praktycznie w każdej organizacji posługującej się systemami informatycznymi istnieją konta uprzywilejowane służące zarządzaniu tymi systemami – np. Administrator czy root. Konta te są często współdzielone przez kilka osób, co uniemożliwia rozliczalność i monitorowanie odpowiedzialności. W takiej sytuacji trudno jest wykazać zgodność z wymaganiami prawnymi np. dotyczącymi ochrony danych osobowych. System musi pozwalać na efektywne zarządzanie kontami uprzywilejowanymi w sposób identyczny jak zarządzanie standardowymi kontami użytkowników. Każde użycie konta uprzywilejowanego musi być monitorowane i raportowane. Ponadto rozwiązanie musi wymuszać na administratorach logowanie się do danego systemu którym administrują za pośrednictwem specjalnego interfejsu dostępowego który zezwoli im na dostęp do systemu i zapisze ich sesję, co umożliwi odtworzenie działań administratora, nie tylko celem udowodnienia popełnienia błędu czy przestępstwa ale także udowodnienie niewinności. Czynności wykonane przez osoby korzystające z takich kont mają być rejestrowane co zagwarantuje pełną rozliczalność czyli zapewnienie zgodności z obowiązującymi normami prawnymi. System musi umożliwiać administratorom niższego stopnia uzyskanie dostępu wyższego poziomu w sytuacjach krytycznych, kiedy administratorzy posiadający standardowo wyższe uprawnienia są niedostępni (np. wykonanie poleceń innego administratora, który nie ma możliwości podłączenia się do systemów Szpitalnych). Wówczas administrator uzyskujący „wyższe" uprawnienia musi potwierdzić konieczność ich przydzielenia, co zostanie zarejestrowane w Systemie. Taka funkcjonalność ma za zadanie umożliwienie utrzymania ciągłości działania w określonych sytuacjach krytycznych. Planowane rozwiązanie pozwala nie tylko obniżyć poziom ryzyka związanego z niedostępnością zasobów informatycznych w określonych sytuacjach ale przede wszystkim spełnienie wymagań określonych prawem.

Zarządzanie aktywami

Potencjalnie każdy pracownik Szpitala oprócz uzyskanych uprawnień dostępu do systemów informatycznych może otrzymać aktywa Szpitala niezbędne do realizacji jego obowiązków (np. laptop, karta dostępowa,) oraz szereg innych uprawnień (upoważnienie do reprezentowania Szpitala w określonych zadaniach np. nadzór nad umową, uprawnienie dostępu fizycznego do pomieszczeń) niezbędnych do realizacji powierzonych pracownikowi zadań. Uwzględniając zasoby kadrowe oraz rotację pracowników w skali roku sprawowanie nadzoru w tym obszarze jest trudnym w realizacji zadaniem. System musi umożliwiać nie tylko zarządzanie i nadzorowanie uprawnień w systemach informatycznych ale również innych uprawnień czy powierzonych pracownikowi aktywów. Sprawowanie właściwego nadzoru w tym obszarze jest podstawą Systemu Zarządzania Bezpieczeństwem Informacji.

Monitorowanie zdarzeń w obszarze przydzielanych uprawnień

System „na bieżąco śledzi" przez 24 godz/doba zdarzenia w zakresie udzielonych uprawnień w systemach zintegrowanych z systemem zarządzania tożsamością. Każda zmiana dokonana w tym obszarze jest monitorowana . Monitorowanie polega nie tylko na automatycznej rejestracji zdarzenia ale również na jednoczesnej weryfikacji zgodności zdarzenia z ustalonymi (zaprojektowanymi) politykami bezpieczeństwa. Wszelkie odstępstwa są natychmiast zgłaszane w postaci komunikatów alarmowych. System raportuje zmiany wg ustalonych kryteriów.

Łódź, dnia 19.03.2019

Nagranie z dialogu stanowi załącznik do protokołu.

Poniżej opisano istotniejsze kwestie poruszone podczas dialogu.
Dostarczone przez Enigma dokumenty zawierają koncepcję rozwiązania informatycznego pod nazwą:
- „Identifi Manager" (IDM) – rozwiązanie do zarządzania tożsamością, grupami, uprawnieniami bezpieczeństwa w systemach i aplikacjach,
- oraz „Privileged Access Manager" (PAM) – rozwiązanie podwyższające bezpieczeństwo kont uprzywilejowanych, zapewniające dostęp do podwyższonych uprawnień (eliminuje hasła wspólne, rejestruje żądania dostępu oraz sesje połączeń administratorów, okresowo zmiana hasła w systemach.

Przy pracach integracyjnych w zakresie budowy konektora proponowane jest podejście przyrostowe – wydawanie kolejnych implementacji kodów etapami poprzedzone krótkimi spotkaniami mającymi na celu ustalenie reguł integracyjnych.

IDM
Właściwości IDM:
- automatyzacja procesów przydzielania uprawnień – IDM monitoruje systemy i wykrywa zmiany w zakresie użytkowników (np. zwolnienie, zatrudnienie) a następnie uruchamia zaimplementowany proces np. tworzenia loginów i przypisania uprawnień.
- kontrola nad użytkownikami i hasłami
- work-flow – możliwość dowolnej konfiguracji zautomatyzowanego lub częściowo automatycznego procesu zmian w zakresie tożsamości użytkownika i przydzielanych uprawnień,
- Self-Service – użytkownicy mogą zalogować się do serwisu webowego celem aktualizacji swoich danych osobowych (np. dane kontaktowe, zmiana nazwiska),
- osoby zarządzające w danym obszarze mogą poprzez system żądać przydzielenia czy zmiany uprawnień dla podległego personelu,
- możliwość zarządzania uprawnieniami dostępu do innych zasobów niż informatyczne, np. dostęp do pomieszczeń,
- sprawowanie nadzoru nad przydzielonymi użytkownikowi środkami np. przydzielenie służbowego laptopa,
- budowanie raportów wg określonych kryteriów .
Procesy zarządzania mogą być zrealizowane w sposób:
- automatyczny,
- półautomatyczny.

W przypadku komunikacji IDM z bazą danych systemu lub web serwisem po zaistnieniu zmian w zarządzanych systemach należy realizować aktualizacji w ramach suportu lub poprzez administratora po odpowiednim przeszkoleniu.

Możliwe jest stosowanie konektorów integracyjnych:
- konektor programowany dla dedykowanego systemu,

- konektor generyczny –dla systemów AD,
- konektor PAM – dla systemów posiadających uprawnienia administratora, konta typu root,

Integracja IDM z HR jest jednostronna tzn. możliwy jest proces tworzenia konta w IDM automatycznie po utworzenia konta w systemie HR. Nie ma możliwości stworzenia konta w HR na podstawie utworzonego konta w IDM. W tym przypadku możliwe jest zmapowanie konta w IDM z kontem w HR.

Zdublowanie indentyfikatora (z atrybutami tożsamości) system IDM raportuje to oraz jest:
- możliwość usunięcia konta,
- lub połączenia z istniejącą tożsamością.

Jest możliwość stworzenia inicjalnych ról dla użytkowników w określonych strukturach.

IDM musi mieć zaimplementowaną strukturę organizacyjną. W tym celu musi być przeprowadzona analiza przedwdrożeniowa. Jedna ze struktur (np. organizacyjna) jest podstawą odzwierciedlona w IDM. Natomiast pozostałe struktury będą przypisane jako atrybuty w IDM (atrybuty są osłownikowane). Identyfikatory połączenia struktur są unikalne. Nie ma znaczenia zmiana nazwy atrybutu. Atrybuty są łączone jeden do jednego.

Dla systemów, które nie mogą być zintegrowane możliwy jest export danych tożsamości z systemów oraz import tych danych do IDM w celu walidacji poprawności wykonanych operacji przez administratora (walidacja poprzez plik płaski)

Polityki recertyfikacyjne – proces weryfikacji przez przełożonych przydzielonych uprawnień dla użytkowników.

Licencjonowanie – użytkownik aktywny (użytkownik, który jest weryfikowany przez system i ma powiązania z systemami).
Konta tożsamości można wyłączyć poprzez przeniesienie do archiwum. System nie zna tej tożsamości. W przypadku gdy użytkownik ma kolejną umowę i jest utworzony w HR to w IDM pojawia się nowa tożsamość. Ręcznie należy sprawdzić czy taka tożsamość jest w archiwum i czy ją połączyć. Tożsamość w archiwum ma zachowane atrybuty (połączenia z systemami).

W archiwum jest funkcjonalność wyszukania tożsamości po identyfikatorach.

Odpersonalizowania konta – jest możliwe. Realizacja procesu jest opisania w dokumentacji. Brak informacji czy jest możliwe wymuszenie podwójnej autoryzacji (?).

W ramach definiowanych ról jest możliwość wprowadzenia dla danej roli wprowadzenie „by pass" dla wybranych aktorów oraz wygenerowanie raportu z powiadomieniem. W tym wypadku należy powiadomić aktora (np. administratora) o tym że należy pominąć akceptację (interfejs umożliwi wyszukanie wniosków na wyższym poziomie akceptowalności).

Zalecenia w zakresie wdrażania. Łatwiej jest wdrażać częściowo systemy a potem uruchamiać integracje pozostałych (większa świadomość i doświadczenie administratora IDM).

Możliwość tworzenia polityk dla poszczególnych procesów w jaki sposób będą zamykane konta w systemach powiązanych.
Synchronizacja tożsamości z różnych systemów z kontem tożsamości tworzonej w IDM.
Delegacja uprawnień jednego użytkownika (nieobecnego) na drugiego użytkownika (czasowe).

Część atrybutów profilu może być zmieniania przez użytkownika (np. nr telefonu).
Help User – funkcjonalność umożliwiająca resetowanie hasła przez użytkownika i odzyskania hasła poprzez odpowiedź na wcześniej zapisane przez użytkownika pytania lub wysłanie sms na przypisany użytkownikowi numer telefonu.
Interfejsy: możliwość tworzenia odrębnych interfejsów dla poszczególnych grup użytkowników (np. administrator, użytkownik zwykły)

PAM
Pełna kontrola nad kontami administratorskimi (kto, co i gdzie robił).

W systemie PAM jest możliwe jest zarzadzanie kontem administratora lokalnego urządzenia (serwer administartor: serwer, komputer, urządzenia sieciowe itd.) oraz kontem administratora serwera (workstation) licencjonowanie „per point".

W przypadku użytkowania PAM zalecane jest utrzymanie IDM w dostępności HA (High Availability). Istnieje możliwość przydzielenia uprawnień wyższego rzędu na żądanie.