Załącznik nr 1 do SIWZ

Opis przedmiotu Zamówienia

1. Wymagania w zakresie dostaw oprogramowania standardowego

Przedmiotem Zamówienia są dostawy oprogramowania standardowego, prawa do jego uaktualniania, prawa do uaktualniania posiadanego oprogramowania, dostawy standardowych usług hostowanych oraz dostawa standardowego pakietu usług wsparcia technicznego – dalej łącznie nazywanych Produktami.

Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).

Zamawiający wymaga praw uaktualniania oprogramowania, dostępności usług hostowanych oraz realizacji wsparcia technicznego w okresie minimum 35 miesięcy od dnia zawarcia umowy.

Zamawiający dopuszcza możliwość rozszerzenia umowy w trakcie jej trwania w zakresie przewidzianym przezUstawę.

Tabela 1 Specyfikacja ilościowa przedmiotu Zamówienia – Produkty:

Lp	Numer katalogowy	Nazwa	ilość
		Profil 1 Enterprise	
1	76A-00028	EntCAL ALNG LicSAPk MVL UsrCAL wSrvcs	1549
		Profil 2 Factory Worker	
2	269-12445	OfficeProPlus ALNG LicSAPk MVL Pltfrm	250
3	CX2-00094	WinEntforSAwMDOP ALNG UpgrdSAPk MVL Pltfrm	250
4	76A-00010	EntCAL ALNG LicSAPk MVL Pltfrm UsrCAL wSrvcs	250
5	AAA-10740	EntCloudSuiteAddOn ShrdSvr ALNG SubsVL MVL touserECAL	1
		Profil 3 Field Worker	
6	269-12445	OfficeProPlus ALNG LicSAPk MVL Pltfrm	1
7	CX2-00094	WinEntforSAwMDOP ALNG UpgrdSAPk MVL Pltfrm	1
8	W06-01066	CoreCAL ALNG LicSAPk MVL Pltfrm UsrCAL	1
9	AAA-10742	EntCloudSuiteAddOn ShrdSvr ALNG SubsVL MVL touserCoreCal	1
		Profile 4: ECS	
10	AAA-10756	EntCloudSuite ShrdSvr ALNG SubsVL MVL PerUsr	2373
		Profil 5	
11	CX2-00090	WinEntforSAwMDOP ALNG UpgrdSAPk MVL	1
12	76A-00028	EntCAL ALNG LicSAPk MVL UsrCAL wSrvcs	1
		Profil 6	
13	269-05623	OfficeProPlus ALNG LicSAPk MVL	1900
14	76A-00028	EntCAL ALNG LicSAPk MVL UsrCAL wSrvcs	1900
		Profil 7	
15	W06-00445	CoreCAL ALNG LicSAPk MVL UsrCAL	300
		Additional Products	
16	076-01776	Prjct ALNG LicSAPk MVL	1

17	H30-00237	PrjctPro ALNG LicSAPk MVL w1PrjctSvrCAL	9
18	D87-01057	VisioPro ALNG LicSAPk MVL	6
19	9ED-00071	VSPremwMSDN ALNG LicSAPk MVL	4
20	9JD-00050	VSUltwMSDN ALNG LicSAPk MVL	5
21	FUD-00936	CISDataCtr ALNG LicSAPk MVL 2Proc	2
22	395-02412	ExchgSvrEnt ALNG LicSAPk MVL	1
23	312-02177	ExchgSvrStd ALNG LicSAPk MVL	1
24	7WC-00112	FrfrntIdnttyMgrCAL ALNG LicSAPk MVL UsrCAL	4 000
25	H22-00479	PrjctSvr ALNG LicSAPk MVL	1
26	5HU-00215	SfBSvr ALNG LicSAPk MVL	1
27	H04-00232	SharePointSvr ALNG LicSAPk MVL	4
28	P71-07280	WinSvrDataCtr ALNG LicSAPk MVL 2Proc	5
29	P73-05897	WinSvrStd ALNG LicSAPk MVL 2Proc	1
30	WSB-00068	DsktpOptmztnPkforSA ALNG SubsVL MVL PerDvc forWinSA	1
31	6QK-00001	AzureMonetaryCommit ShrdSvr ALNG SubsVL MVL Commit	9
32	DSD-00030	DynCRMOnlnPro ShrdSvr ALNG SubsVL MVL Restricted PerUsr	1
33	AAA-11392	EntVoiceAddOntoECS ShrdSvr ALNG SubsVL MVL AddOn toEntCloudSte	2373
34	7YY-00014	PowerBI ShrdSvr ALNG SubsVL MVL PerUsr forSPOP2/E3/E4	78

Zamawiający wymaga dostarczenia wymienionych Produktów lub produktów w pełni równoważnych.

2. Warunki równoważności

Przedmiotem Zamówienia jest zakup oprogramowania, prawa do jego uaktualniania i prawa do uaktualniania wyspecyfikowanego posiadanego oprogramowania oraz dostawa standardowego pakietu usług wsparcia technicznego (łącznie nazwanych Produktami) w okresie minimum 35 miesięcy od zawarcia umowy. W tabeli 1 wyspecyfikowanych został przedmiot Zamówienia. Poniżej Zamawiający przedstawia warunki równoważności dla Produktów oraz sposób ich weryfikacji.

Wymagania ogólne w zakresie dostaw:

1. Zamawiający wymaga zagwarantowania niezmienności cen na Produkty w całym okresie trwania umowy, z wyłączeniem zmian kursowych EUR/PLN.
2. Licencje muszą pozwalać na swobodne przenoszenie oprogramowania pomiędzy serwerami i pomiędzy stacjami roboczymi (np. w przypadku wymiany lub uszkodzenia sprzętu).
3. Licencje muszą zawierać prawo do uaktualniania wersji zakupionego oprogramowania będącego przedmiotem Zamówienia do najbardziej aktualnej dostępnej wersji w okresie trwania umowy.
4. Zamawiający dopuszcza jako ważne oferty:
   a) Zawiarające produkty następcze (w nowszej wersji) w stosunku do wymienionych,
   b) Produkty zawierające kilka opisanych Produktów w postaci jednego pakietu, który może zawierać dodatkowe, nie opisane w SIWZ rozszerzenia funkcjonalności oprogramowania.
5. Licencje muszą pozwalać na sublicencjonowanie dla jednostek stowarzyszonych (podmiotów wchodzących w skład Grupy Kapitałowej ENERGA).
6. Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej Produkty pochodzące od jednego Producenta (producenta Produktów lub jego spółek zależnych), umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego.
7. W związku z możliwością zwiększenia liczby użytkowników systemów w trakcie trwania umowy, Zamawiający wymaga zaoferowania licencjonowania umożliwiającego w okresie trwania umowy instalację dodatkowych licencji z zamawianego zakresu produktów z rozliczaniem się za nie post fatum - raz do roku.

8. W ramach warunków umowy licencyjnej Zamawiający ma mieć prawo do testowania oprogramowania i korzystania z oprogramowania w celach edukacyjnych oprogramowania Producenta bez dodatkowych opłat. Wówczas Zamawiający nabywa prawo do uruchamiania:
   a. 20 kopii każdego produktu w celach edukacyjnych (w wydzielonym pomieszczeniu, przeznaczonym do szkoleń) bez konieczności zakupu dodatkowych licencji.
   b. 10 kopii każdego produktu w celach testowych w 60-dniowym okresie ewaluacyjnym, po którym istnieje możliwość zamówienia odpowiedniej ilość licencji na testowany produkt.
9. Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych (możliwość instalacji oprogramowania na wielu urządzeniach przy wykorzystaniu jednego standardowego obrazu), z prawem do:
   a. wielokrotnego użycia jednego obrazu dysku w procesie instalacji,
   b. tworzenia kopii zapasowych
   c. masowej aktywacji oprogramowania przy użyciu jednego klucza aktywacyjnego dla danego typu oprogramowania.
10. Wraz ofertą Wykonawca złoży dokument Producenta opisujący zasady licencjonowania udzielane standardowo do oferowanego oprogramowania, nie gorsze od wymogów zawartych w SIWZ.
11. Wykonawca zapewni dostęp do spersonalizowanej strony Producenta pozwalającej upoważnionym osobom ze strony Zamawiającego na:
   a. Pobieranie zakupionego oprogramowania,
   b. Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,
   c. Sprawdzanie liczby zakupionych licencji w wykazie zakupionych Produktów.
12. Zamawiający wymaga udzielenia uprawnień na stronie producenta oraz dostępu do kodu zamawianego oprogramowania i kluczy licencyjnych w terminie do 5 dnia roboczego następnego miesiąca po podpisaniu umowy.
13. Po dziewięćdziesięciu (90) dniach od zakończenia okresu trwania umowy Wykonawca zapewni wyłączenie konta na spersonalizowanej stronie Zamawiającego i usunięcie jego danych.
14. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
15. Jeżeli nowa (następcza) wersja Produktu zawierać będzie bardziej restrykcyjne prawa do używania (pól eksploatacji) niż wersja, która była aktualna na dzień złożenia oferty, te bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tego Produktu przez Zamawiającego.

2.1. Specyfikacja techniczno – eksploatacyjna i cech użytkowych oprogramowania.

W poniżej części przedstawione są wymagania funkcjonalne dotyczące zamawianego oprogramowania i usług.

Z uwagi na to, że art. 30 ust. 5 Ustawy wyraźnie wskazuje na Wykonawcę, jako tego, kto jest zobowiązany wykazać, że oferowane rozwiązania i produkty spełniają wymagania postawione przez Zamawiającego, Zamawiający zastrzega sobie, w przypadku jakichkolwiek wątpliwości, prawo sprawdzenie pełnej zgodności oferowanych produktów z wymogami specyfikacji. Sprawdzenie to, będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych na sprzęcie Zamawiającego, z użyciem urządzeń peryferyjnych Zamawiającego, na arkuszach, bazach danych i plikach Zamawiającego.

W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby Zamawiającego (lub udostępni wymaganą hostowaną usługę standardową) w terminie 5 dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego przedmiotu dostawy. W odniesieniu do oprogramowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne funkcjonalnie z oferowanymi. Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt 2 Ustawy.

Nie przedłożenie oferowanych produktów do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia.

Po wykonaniu testów, dostarczone do testów egzemplarze będą zwrócone oferentowi.

2.1.1. EntCAL ALNG LicSAPk MVL UsrCAL wSrvcs

Pakiet licencji dostępowych na użytkownika do serwerów produkcji Microsoft musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów:

1. Serwerowych systemów operacyjnych,
2. Podstawowej funkcjonalności serwerów portali wielofunkcyjnych intranet,
3. Podstawowej funkcjonalności serwerów poczty e-mail,
4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem,
5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej,
6. Mechanizmów tworzenia dostępu VPN do systemów operacyjnych
7. Licencje dostępowe rozszerzające zakres funkcji dostępnych posiadaczom licencji dostępowych serwera komunikacji wielokanałowej, pozwalające dodatkowo wykorzystać funkcjonalność serwera komunikacji wielokanałowej w zakresie:
    a. Łączności głosowej i video z wieloma (więcej niż dwoma) uczestnikami konferencji,
    b. Zarządzania połączeniami telefonicznymi i głosowymi
    c. Współdzielenia aplikacji.
8. Serwerów zarządzania, monitorowania, składowania danych i zarządzania maszynami wirtualnymi,
9. Serwerów poczty e-mail w zakresie uzupełniającym pakiet podstawowych licencji dostępowych, zapewniających (w zgodzie z wymaganiami licencyjnymi producenta) możliwość wykorzystania przez użytkowników zaawansowanych narzędzi archiwizacyjnych, ochrony informacji oraz narzędzi poczty głosowej.

Licencje umożliwiające użytkownikom wykorzystanie pełnej funkcjonalności serwera portalu wielofunkcyjnego, uwzględniające dostęp do usług serwera formularzy, narzędzi wizualizacji analiz biznesowych, wspólnej infrastruktury wszystkich stron w organizacji.

2.1.2. OfficeProPlus ALNG LicSAPk MVL Pltfrm

Licencja pakietu biurowego z prawem do uaktualniania. Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
2. Wymagania odnośnie interfejsu użytkownika:
    a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu

operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
    a. posiada kompletny i publicznie dostępny opis formatu,
    b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),
    c. umożliwia wykorzystanie schematów XML,
    d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
    a. Edytor tekstów
    b. Arkusz kalkulacyjny
    c. Narzędzie do przygotowywania i prowadzenia prezentacji
    d. Narzędzie do tworzenia i wypełniania formularzy elektronicznych
    e. Narzędzie do tworzenia drukowanych materiałów informacyjnych
    f. Narzędzie do tworzenia i pracy z lokalną bazą danych
    g. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
    h. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
    i. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
11. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.

i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
l. Określenie układu strony (pionowa/pozioma).
m. Wydruk dokumentów.
n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
p. Zapis i edycję plików w formacie PDF.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
r. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
s. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

12. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
    e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
    f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
    g. Wyszukiwanie i zamianę danych
    h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
    i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
    j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
    l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
    m. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
    n. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
    o. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..

p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

13. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
    b. Prezentowanie przy użyciu projektora multimedialnego
    c. Drukowanie w formacie umożliwiającym robienie notatek
    d. Zapisanie jako prezentacja tylko do odczytu.
    e. Nagrywanie narracji i dołączanie jej do prezentacji
    f. Opatrywanie slajdów notatkami dla prezentera
    g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
    h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
    i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
    j. Możliwość tworzenia animacji obiektów i całych slajdów
    k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
    l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.
14. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
    a. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania
    b. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.
    c. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
    d. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
    e. Możliwość pobierania danych z platformy do pracy grupowej.
    f. Przesłanie danych przy użyciu usługi Web (tzw. web service).
    g. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
    h. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.
15. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    a. Tworzenie i edycję drukowanych materiałów informacyjnych
    b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    c. Edycję poszczególnych stron materiałów.
    d. Podział treści na kolumny.
    e. Umieszczanie elementów graficznych.
    f. Wykorzystanie mechanizmu korespondencji seryjnej
    g. Płynne przesuwanie elementów po całej stronie publikacji.
    h. Eksport publikacji do formatu PDF oraz TIFF.
    i. Wydruk publikacji.
    j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
16. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    a. Tworzenie bazy danych przez zdefiniowanie:

b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
c. Relacji pomiędzy tabelami
d. Formularzy do wprowadzania i edycji danych
e. Raportów
f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych
g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.

17. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
    b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
    c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
    d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
    e. Automatyczne grupowanie poczty o tym samym tytule,
    f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
    g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
    h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
    i. Zarządzanie kalendarzem,
    j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
    k. Przeglądanie kalendarza innych użytkowników,
    l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
    m. Zarządzanie listą zadań,
    n. Zlecanie zadań innym użytkownikom,
    o. Zarządzanie listą kontaktów,
    p. Udostępnianie listy kontaktów innym użytkownikom,
    q. Przeglądanie listy kontaktów innych użytkowników,
    r. Możliwość przesyłania kontaktów innym użytkowników,
    s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.
18. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

d. Możliwość obsługi tekstowych wiadomości błyskawicznych.
e. Możliwość komunikacji głosowej i video.
f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.

Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

2.1.3. WinEntforSAwMDOP ALNG UpgrdSAPk MVL Pltfrm

Uaktualnienie systemu operacyjnego klasy PC z prawem do uaktualniania. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.

19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
24. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
25. Mechanizmy logowania do domeny w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
26. Mechanizmy wieloelementowego uwierzytelniania.
27. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
28. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
29. Wsparcie dla algorytmów Suite B (RFC 4869),
30. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
31. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
32. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
33. Wsparcie dla JScript i VBScript, Powershell – możliwość uruchamiania interpretera poleceń,
34. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
35. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
36. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
37. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
38. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
39. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
40. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
41. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
42. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
43. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie maszyn wirtualnych,
44. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
45. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
46. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych

47. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
48. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
49. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
50. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
51. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
52. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
53. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
54. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
55. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
56. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
57. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
58. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
59. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
60. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
61. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
62. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”.
63. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
64. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
65. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
66. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
67. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
68. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
69. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.

70. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym
71. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
72. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet
73. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

2.1.4. EntCAL ALNG LicSAPk MVL Pltfrm UsrCAL wSrvcs

Pakiet licencji dostępowych na użytkownika do serwerów produkcji Microsoft musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów:

10. Serwerowych systemów operacyjnych,
11. Podstawowej funkcjonalności serwerów portali wielofunkcyjnych intranet,
12. Podstawowej funkcjonalności serwerów poczty e-mail,
13. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem,
14. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej,
15. Mechanizmów tworzenia dostępu VPN do systemów operacyjnych
16. Licencje dostępowe rozszerzające zakres funkcji dostępnych posiadaczom licencji dostępowych serwera komunikacji wielokanałowej, pozwalające dodatkowo wykorzystać funkcjonalność serwera komunikacji wielokanałowej w zakresie:
    a. Łączności głosowej i video z wieloma (więcej niż dwoma) uczestnikami konferencji,
    b. Zarządzania połączeniami telefonicznymi i głosowymi
    c. Współdzielenia aplikacji.
17. Serwerów zarządzania, monitorowania, składowania danych i zarządzania maszynami wirtualnymi,
18. Serwerów poczty e-mail w zakresie uzupełniającym pakiet podstawowych licencji dostępowych, zapewniających (w zgodzie z wymaganiami licencyjnymi producenta) możliwość wykorzystania przez użytkowników zaawansowanych narzędzi archiwizacyjnych, ochrony informacji oraz narzędzi poczty głosowej.

Licencje umożliwiające użytkownikom wykorzystanie pełnej funkcjonalności serwera portalu wielofunkcyjnego, uwzględniające dostęp do usług serwera formularzy, narzędzi wizualizacji analiz biznesowych, wspólnej infrastruktury wszystkich stron w organizacji.

2.1.5. EntCloudSuiteAddOn ShrdSvr ALNG SubsVL MVL touserECAL

Produkt zapewniający poniżej opisane funckcjonalności dla użytkowników posiadających pakiet licencji opisanych w punkcie 2.1.2, 2.1.3, 2.1.4.

Licencja subskrypcyjna systemu operacyjnego klasy PC, który musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,

3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Obsługa standardu NFC (near field communication),
23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
26. Mechanizmy logowania do domeny w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

27. Mechanizmy wieloelementowego uwierzytelniania.
28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
30. Wsparcie dla algorytmów Suite B (RFC 4869),
31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
33. Wsparcie dla środowisk Java i.NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
36. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
40. Udostępnianie modemu,
41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
43. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
51. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
52. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku

53. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
54. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
55. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
56. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
57. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
58. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
59. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
60. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
61. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
62. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
63. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
64. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”.
65. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
66. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
67. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
68. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
69. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
70. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
71. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.

72. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym
73. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
74. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet
75. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

Pakiet usług hostowanych

Usługa hostowana (on-line) ma uprawniać użytkowników do wykorzystania usług on-line – portalu wewnętrznego, poczty elektronicznej oraz narzędzi wiadomości błyskawicznych i konferencji głosowych i video. Ponadto musi zawierać 12 miesięczną subskrypcję pakietu biurowego.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

Usługa musi umożliwiać:

a. obsługę poczty elektronicznej,
b. zarządzanie czasem,
c. zarządzania zasobami
d. zarządzanie kontaktami i komunikacją.

Usługa musi dostaczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:

a. Zarządzania użytkownikami poczty,
b. Wsparcia migracji z innych systemów poczty,
c. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
d. Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty.

Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:

a. Posiadanego oprogramowania Outlook (2007 i 2010),
b. Przeglądarki (Web Access),
c. Urządzeń mobilnych.

Wymagane cechy usługi to:

a. Skrzynki pocztowe (do 50GB),
b. Standardowy i łatwy sposób obsługi poczty elektronicznej,
c. Obsługa najnowszych funkcji Outlook 2010 i 2013, takich jak tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari,
d. Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.
e. Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
    a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
    b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
    c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami
    d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia
    e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
2. Funkcjonalność wspierająca pracę grupową:
    a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości
    b. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu
    c. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze
    d. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone
    e. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania
    f. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań
    g. Obsługa list i grup dystrybucyjnych.
    h. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
    i. Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.
    j. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
    k. Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
    l. Funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
    m. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
    n. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
    o. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
    p. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.
3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
    a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja

b. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.
c. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.
d. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.
e. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.
f. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
g. Integracja z usługami zarządzania dostępem do treści (ADRMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania.
h. Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
i. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
j. Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.

4. Wsparcie dla użytkowników mobilnych:
   a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
   b. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
   c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
   d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
   e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
   f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

Usługa portalu on-line musi realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Tworzenie repozytoriów wzorów dokumentów,
6. Tworzenie repozytoriów dokumentów,
7. Wspólną, bezpieczną pracę nad dokumentami,
8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:

1. Interfejs użytkownika:
    a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
    b. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
    c. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
    d. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
    e. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
2. Projektowanie stron
    a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron,
    b. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
    c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
    d. Możliwość osadzania elementów iFrame w polach HTML na stronie.
3. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
    a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili
    b. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów

c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
d. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego
e. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services
f. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
g. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych. Usługa portalu on-line musi mieć wbudowaną funkcjonalność udostępniania użytkownikom komponentów pakietu biurowego on-line dostępnego przez przeglądarkę.

Pakiet biurowy on-line musi spełniać następujące wymagania:

1. Wymagania odnośnie interfejsu użytkownika:
    a. Pełna polska wersja językowa interfejsu użytkownika,
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
2. 2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
    c. a. Posiada kompletny i publicznie dostępny opis formatu,
    d. b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
    e. c. Umożliwia wykorzystanie schematów XML
    f. d. Wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3. Pakiet biurowy on-line musi zawierać:
    a. Edytor tekstów
    b. Arkusz kalkulacyjny
    c. Narzędzie do przygotowywania i prowadzenia prezentacji
    d. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
4. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
    b. Wstawianie oraz formatowanie tabel
    c. Wstawianie oraz formatowanie obiektów graficznych
    d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
    e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
    f. Automatyczne tworzenie spisów treści
    g. Formatowanie nagłówków i stopek stron
    h. Sprawdzanie pisowni w języku polskim

i. Śledzenie zmian wprowadzonych przez użytkowników
j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
k. Określenie układu strony (pionowa/pozioma)
l. Wydruk dokumentów
m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
n. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
p. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
q. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

5. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
   e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
   f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
   g. Wyszukiwanie i zamianę danych
   h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
   i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
   l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
   n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, które będą:
   b. Prezentowanie przy użyciu projektora multimedialnego
   c. Drukowanie w formacie umożliwiającym robienie notatek
   d. Zapisanie jako prezentacja tylko do odczytu.
   e. Nagrywanie narracji i dołączanie jej do prezentacji

f. Opatrywanie slajdów notatkami dla prezentera
g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j. Możliwość tworzenia animacji obiektów i całych slajdów
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

Usługa serwera komunikacji wielokanałowej on-line (SKW) wspomagający wewnętrzną komunikację Zamawiającego ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1. Prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video
2. Przesyłanie wiadomości tekstowych z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę oraz urządzeń mobilnych bazujących na Windows Mobile.
3. Możliwość organizowania telekonferencji

Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty e mail, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać natywną integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu:

1. Ujednolicenie komunikacji biznesowej
    a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
    b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności.
    c. Dostępność aplikacji klienckiej udostepniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc.
    d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością:
        i. Dołączania do telekonferencji
        ii. Szczegółowej listy uczestników
        iii. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
        iv. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli
        v. Głosowania
        vi. Udostępniania plików
        vii. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji
    e. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
    f. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.

g. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym.
h. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
i. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich.

2. W związku z tak postawionymi założeniami SKW ma zapewnić:
   a. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników.
   b. Wykorzystanie statusu obecności i konferencje w czasie rzeczywistym.
   c. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami.
   d. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych.
3. SKW ma zapewnić obsługę następujących funkcjonalności:
   a. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności.
   b. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.
   c. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi,
   d. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych.
   e. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu.
   f. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników.
   g. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.
   h. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.
   i. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów
   j. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów.

Subskrypcja pakietu biurowego

Usługa hostowana on-line musi zawierać 36 miesięczną subskrypcję pakietu biurowego spełniającego następujące wymagania:

1. Wymagania odnośnie interfejsu użytkownika:

   a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
   b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
   c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
2. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
3. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
4. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
   a. Posiada kompletny i publicznie dostępny opis formatu,
   b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),
   c. Umożliwia wykorzystanie schematów XML,
   d. Wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
5. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
6. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
7. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
8. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
9. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   e. Edytor tekstów
   f. Arkusz kalkulacyjny
   g. Narzędzie do przygotowywania i prowadzenia prezentacji
   h. Narzędzie do tworzenia i wypełniania formularzy elektronicznych
   i. Narzędzie do tworzenia drukowanych materiałów informacyjnych
   j. Narzędzie do tworzenia i pracy z lokalną bazą danych
   k. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
   l. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
   m. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
10. Edytor tekstów musi umożliwiać:
   a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
   b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.

c. Wstawianie oraz formatowanie tabel.
d. Wstawianie oraz formatowanie obiektów graficznych.
e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
g. Automatyczne tworzenie spisów treści.
h. Formatowanie nagłówków i stopek stron.
i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
l. Określenie układu strony (pionowa/pozioma).
m. Wydruk dokumentów.
n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
p. Zapis i edycję plików w formacie PDF.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
r. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
s. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

11. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
    e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
    f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
    g. Wyszukiwanie i zamianę danych
    h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
    i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
    j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
    l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

m. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
n. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
o. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
    b. Prezentowanie przy użyciu projektora multimedialnego
    c. Drukowanie w formacie umożliwiającym robienie notatek
    d. Zapisanie, jako prezentacja tylko do odczytu.
    e. Nagrywanie narracji i dołączanie jej do prezentacji
    f. Opatrywanie slajdów notatkami dla prezentera
    g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
    h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
    i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
    j. Możliwość tworzenia animacji obiektów i całych slajdów
    k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
    l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.
13. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
    a. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania
    b. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.
    c. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
    d. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
    e. Możliwość pobierania danych z platformy do pracy grupowej.
    f. Przesłanie danych przy użyciu usługi Web (tzw. web service).
    g. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
    h. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.
14. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    a. Tworzenie i edycję drukowanych materiałów informacyjnych
    b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    c. Edycję poszczególnych stron materiałów.
    d. Podział treści na kolumny.
    e. Umieszczanie elementów graficznych.

f. Wykorzystanie mechanizmu korespondencji seryjnej
g. Płynne przesuwanie elementów po całej stronie publikacji.
h. Eksport publikacji do formatu PDF oraz TIFF.
i. Wydruk publikacji.
j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.

15. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    a. Tworzenie bazy danych przez zdefiniowanie:
    b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
    c. Relacji pomiędzy tabelami
    d. Formularzy do wprowadzania i edycji danych
    e. Raportów
    f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych
    g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
    h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
16. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
    b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
    c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
    d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
    e. Automatyczne grupowanie poczty o tym samym tytule,
    f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
    g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
    h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
    i. Zarządzanie kalendarzem,
    j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
    k. Przeglądanie kalendarza innych użytkowników,
    l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
    m. Zarządzanie listą zadań,
    n. Zlecanie zadań innym użytkownikom,
    o. Zarządzanie listą kontaktów,
    p. Udostępnianie listy kontaktów innym użytkownikom,
    q. Przeglądanie listy kontaktów innych użytkowników,
    r. Możliwość przesyłania kontaktów innym użytkowników.
17. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
d. Możliwość obsługi tekstowych wiadomości błyskawicznych.
e. Możliwość komunikacji głosowej i video.
f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
h. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Usługa zarządzania stacjami i treścią

Subskrypcja usługi zarządzania urządzeniami mobilnymi oraz tożsamością użytkowników musi spełniać następujące wymagania:

1. Pełne zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT),
2. Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych,
3. Portal klasy self-serivce dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej,
4. Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS),
5. Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

Wymagane scenariusze użycia:

1. Automatyczna klasyfikacja treści dokumentów (przechowywanych na zasobach plikowych, bibliotekach lub transportowanych poprzez system pocztowy) i dynamiczne aplikowanie restrykcji związanych z dostępem do informacji wymusza implementację regulacji i zapobiega niekontrolowanemu wyciekowi informacji
2. Bezpieczna wymiana plików wewnątrz organizacji oraz z zewnętrznymi odbiorcami niezależnie od typu pliku, posiadanego urządzenia (PC lub urządzenie mobilne Windows Phone, Android, iOS) lub przynależności do organizacji umożliwia granularną kontrolę dostępu do poufnych informacji i wymuszenie standardów regulacji sektorowej
3. Wykorzystanie telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS podczas dostępu do aplikacji webowych pozwala na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia
4. Możliwość wydajnej pracy przez użytkowników na licznych lubianych przez nich narzędziach, zapewnia im dostęp do potrzebnych aplikacji

5. Jednokrotne logowanie w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika ułatwia pracę użytkownika i redukuje przestoje czasowe
6. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkowstwem w grupach i obsługi kart inteligentnych pozwala na redukcję ilości zgłoszeń działów wsparcia nawet o 30%
7. Automatyczne przepływy pracy i reguł biznesowych pozwalają na zaoszczędzenie czasu i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie reguł biznesowych)
8. Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwala na audyt i kontrolę zgodności z przepisami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.
9. Zarządzanie urządzeniami mobilnymi pozwala na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwia zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:

System zarządzania tożsamością elektroniczną ma zapewniać agregację oraz synchronizacje danych o użytkownikach różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego Centrum certyfikacji.

Wymagania ogólne

1. Bezpieczeństwo
   System zarządzania tożsamością musi umożliwiać zastosowanie przy połączeniu ze źródłami danych mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji). System powinien zapewniać również prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej poprzez zapory firewall oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
   System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
   System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.
2. Skalowalność
   System zarządzania tożsamością dostarczony w ramach zamówienia musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie od 2 500 do 10 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.
3. Interoperacyjność
   System zarządzania tożsamością powinien zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.
   System zarządzania tożsamością powinien zapewniać możliwość realizacji dwukierunkowej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.
4. Rozszerzalność

System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości funkcjonalności o połączenia z innymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu. System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.

5. Wydajność
   System musi umożliwiać generowanie i nagrywanie certyfikatów na kartach w liczbie min. xx na godzinę na stanowisko.

Wymagania w zakresie cech i funkcjonalności rozwiązania

1. Agregacja i synchronizacja danych
   a. System powinien zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
   b. System zarządzania tożsamością, w ramach początkowego wdrożenia powinien zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
      i. Pliki tekstowe CSV, AVP, LDIF
      ii. Bazy danych MS SQL 2000\2005, Oracle
      iii. Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.
   c. System powinien zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
   d. System powinien zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy połączenia poprzez budowę odpowiedniego rozszerzenia systemu.
   e. System powinien zapewniać możliwość tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
   f. System powinien dostarczać mechanizmów pozwalających na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
   g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system powinien umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium. System powinien zapewniać możliwość synchronizacji danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
   h. System powinien oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
   i. System powinien umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.
2. Repozytorium danych teleadresowych
   a. System powinien dostarczać rozwiązania umożliwiającego agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
   b. System powinien dostarczać interfejsu użytkownika zapewniającego możliwość wyszukiwania oraz przeglądania danych dla wszystkich użytkowników systemu.

c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie zarządzania oraz uaktualnienia danych teleadresowych. System powinien zapewniać funkcjonalność synchronizacji uaktualnionych danych do wszystkich zarządzanych systemów.
d. W ramach interfejsu użytkownika system powinien zapewniać możliwość udostępnienia możliwości edycji zakresu danych samodzielnie przez każdego z użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.

3. Zarządzanie kartą elektroniczną
   a. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów)
   b. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników
   c. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów niekwalifikowanych i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnych przechowywanych i wygenerowanym na karcie)
   d. Dostarczany system musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów niekwalifikowanych dla jednego użytkownika)
   e. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania, tylko do logowania, szyfrowanie /podpisywanie poczty itp.
   f. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP.
   g. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI.
   h. System musi wspierać zarządzanie certyfikatami używanymi do logowania w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
   i. Umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
   j. Po wystawieniu certyfikatu, systemu umożliwia włączenie automatycznej publikacji certyfikatu w katalogu LDAP
   k. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP
   l. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej).
   m. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty)
   n. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:

   i. Użytkownik lub administrator wprowadza PIN inicjujący
   ii. PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW
   iii. System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku
   iv. PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API)

o. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego
p. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego)
q. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:
   i. nie mniej niż 6 znaków
   ii. nie mogą być same cyfry (wymagane litery małe i duże)
   iii. PIN może się powtarzać przez N zmian
r. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,
s. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego
t. Wokflow musi umożliwiać, implementacji następujących scenariuszy użycia:
   i. w pełni automatyczne wystawianie certyfikatów dla użytkowników
   ii. wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu
   iii. automatyczne odświeżanie wybranych certyfikatów
   iv. automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia
   v. weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu
   vi. powiadamianie administratorów system o wygasaniu certyfikatów dla serwerów / urządzeń wchodzących w skład infrastruktury teleinformatycznej
u. Workflow musi udostępnić możliwość definiowanie wielu wzorców certyfikatów (w zależności od ich zastosowania) w połączeniu z odpowiednią ścieżką wystawiania/dostarczania certyfikatów do użytkownika, w szczególności:
   i. Certyfikat do szyfrowania poczty wystawiany jest automatycznie o ile użytkownik posiada certyfikat na karcie elektronicznej do podpisu, podpis ten musi być użyty do podpisania wystawianie certyfikatu do szyfrowania
   ii. Certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW

   Definiowanie takich reguł musi być dostępne bezpośrednio dla operatora systemu i nie może wymagać dodatkowych opłat licencyjnych
v. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, ilości zmian PIN'ow, ilość odblokowanych kart
w. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważny

x. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11
y. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania)
z. System musi wspierać graficzną personalizację kart: (nadruk wielokolorowy)
aa. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.

Podsystem zarządzania urządzeniami mobilnymi

1. Architektura Systemu UDM
   Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
   a. Integrację z systemem SCCM 2012 R2 w oparciu o natywne interfejsy komunikacyjne
   b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
   c. Porozumiewania się z użytkownikiem końcowym w języku polskim.
2. Inwentaryzacja sprzętu i zarządzanie zasobami:
   a. Inwentaryzacja zasobów urządzenia mobilnego odbywa się w interwałach czasowych.
   b. Inwentaryzacja sprzętu pozwala na zbieranie następujących informacji
      i. Nazwa urządzenia
      ii. Identyfikator urządzenia
      iii. Nazwa platformy systemu operacyjnego
      iv. Wersja oprogramowania układowego
      v. Typ procesora
      vi. Model urządzenia
      vii. Producent urządzenia
      viii. Architektura procesora
      ix. Język urządzenia
      x. Lista aplikacji zainstalowanych w ramach przedsiębiorstwa
3. Zdalna blokada i wymazanie:
   a. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji.
   b. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
4. Dystrybucja oprogramowania:
   a. Pakiety instalacyjne dla aplikacji mobilnych mogą być przechowywany na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
   b. Systemu UDM umożliwia dystrybucję oprogramowania na prośbę użytkownika, realizowaną poprzez wybór oprogramowania w ramach dostępnego katalogu aplikacji
   c. Katalog aplikacji jest zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
   d. Katalog aplikacji wspiera następujące formaty aplikacji mobilnych:
      i. *.appx (Windows RT)
      ii. *.xap (Windows Phone 8)

iii. *.ipa (iOS)
iv. *.apk (Android)

e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
i. Windows Store
ii. Windows Phone Store
iii. Android Google Play Store
iv. iOS App Store

5. Definiowanie polityk urządzenia mobilnego:
a. Komponenty umożliwiające zdefiniowanie standardu polityk urządzenia mobilnego. W obszarze polityki haseł system zapewni:
i. Zdefiniowanie wymuszenia hasła
ii. Określenia minimalnej długości hasła
iii. Określenia czasu wygasania hasła
iv. Określenia ilości pamiętanych haseł
v. Określenia ilości prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia
vi. Określenia czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła
6. Raportowanie, prezentacja danych:
Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika.

Podsystem ochrony informacji

Usługa bezpieczeństwa informacji musi pozwalać na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem. Usługa musi spełniać następujące wymagania:

1. Usługa musi być dostępna w postaci subskrypcji,
2. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), a nie fizyczne miejsce jej przechowywania,
3. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
4. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
5. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
6. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, np.:
a. Brak uprawnień dostępu do informacji,
b. Informacja tylko do odczytu,
c. Prawo do edycji informacji,
d. Brak możliwości wykonania systemowego zrzutu ekranu,
e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.

7. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
8. Możliwość wyboru restrykcji dostępu w postaci standardowych, łatwych do wyboru szablonów, powstałych na bazie polityk ochrony informacji,
9. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej" instalacji w całej organizacji,
10. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
11. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi katalogowej

Usługa katalogowa musi zapewnić:

1. Możliwość zintegrowania jednokrotnego logowania (SSO) dla ponad 2500 popularnych aplikacji typu SaaS,
2. Możliwość publikacji aplikacji webowych z wewnątrz organizacji,
3. Możliwość połączenia z usługą Active Directory wewnątrz organizacji,
4. Konsolę zarządzania tożsamością i dostępem,
5. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
6. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
7. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
8. Samoobsługowe resetowania hasła,
9. Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników.

2.1.6. OfficeProPlus ALNG LicSAPk MVL Pltfrm

Licencja pakietu biurowego z prawem do uaktualniania. Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
2. Wymagania odnośnie interfejsu użytkownika:
    a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.

5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
    a. posiada kompletny i publicznie dostępny opis formatu,
    b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),
    c. umożliwia wykorzystanie schematów XML,
    d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
    a. Edytor tekstów
    b. Arkusz kalkulacyjny
    c. Narzędzie do przygotowywania i prowadzenia prezentacji
    d. Narzędzie do tworzenia i wypełniania formularzy elektronicznych
    e. Narzędzie do tworzenia drukowanych materiałów informacyjnych
    f. Narzędzie do tworzenia i pracy z lokalną bazą danych
    g. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
    h. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
    i. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
11. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.
    i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
    k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    l. Określenie układu strony (pionowa/pozioma).
    m. Wydruk dokumentów.

n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
p. Zapis i edycję plików w formacie PDF.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
r. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
s. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

12. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
    e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
    f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
    g. Wyszukiwanie i zamianę danych
    h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
    i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
    j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
    l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
    m. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
    n. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
    o. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
    p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
13. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
    b. Prezentowanie przy użyciu projektora multimedialnego
    c. Drukowanie w formacie umożliwiającym robienie notatek
    d. Zapisanie jako prezentacja tylko do odczytu.

e. Nagrywanie narracji i dołączanie jej do prezentacji
f. Opatrywanie slajdów notatkami dla prezentera
g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j. Możliwość tworzenia animacji obiektów i całych slajdów
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

14. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
    a. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania
    b. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.
    c. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
    d. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
    e. Możliwość pobierania danych z platformy do pracy grupowej.
    f. Przesłanie danych przy użyciu usługi Web (tzw. web service).
    g. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
    h. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.
15. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    a. Tworzenie i edycję drukowanych materiałów informacyjnych
    b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    c. Edycję poszczególnych stron materiałów.
    d. Podział treści na kolumny.
    e. Umieszczanie elementów graficznych.
    f. Wykorzystanie mechanizmu korespondencji seryjnej
    g. Płynne przesuwanie elementów po całej stronie publikacji.
    h. Eksport publikacji do formatu PDF oraz TIFF.
    i. Wydruk publikacji.
    j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
16. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    a. Tworzenie bazy danych przez zdefiniowanie:
    b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
    c. Relacji pomiędzy tabelami
    d. Formularzy do wprowadzania i edycji danych
    e. Raportów
    f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych

g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.

17. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
    b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
    c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
    d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
    e. Automatyczne grupowanie poczty o tym samym tytule,
    f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
    g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
    h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
    i. Zarządzanie kalendarzem,
    j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
    k. Przeglądanie kalendarza innych użytkowników,
    l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
    m. Zarządzanie listą zadań,
    n. Zlecanie zadań innym użytkownikom,
    o. Zarządzanie listą kontaktów,
    p. Udostępnianie listy kontaktów innym użytkownikom,
    q. Przeglądanie listy kontaktów innych użytkowników,
    r. Możliwość przesyłania kontaktów innym użytkowników,
    s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.
18. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
    d. Możliwość obsługi tekstowych wiadomości błyskawicznych.
    e. Możliwość komunikacji głosowej i video.
    f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
    g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.

Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

2.1.7. WinEntforSAwMDOP ALNG UpgrdSAPk MVL Pltfrm

Uaktualnienie systemu operacyjnego klasy PC z prawem do uaktualniania. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.

22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
24. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
25. Mechanizmy logowania do domeny w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
26. Mechanizmy wieloelementowego uwierzytelniania.
27. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
28. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
29. Wsparcie dla algorytmów Suite B (RFC 4869),
30. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
31. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
32. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
33. Wsparcie dla JScript i VBScript, Powershell – możliwość uruchamiania interpretera poleceń,
34. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
35. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
36. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
37. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
38. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
39. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
40. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
41. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
42. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
43. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie maszyn wirtualnych,
44. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
45. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
46. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
47. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
48. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
49. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
50. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku

51. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
52. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
53. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
54. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
55. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
56. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
57. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
58. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
59. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
60. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
61. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
62. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
63. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
64. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
65. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
66. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
67. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
68. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
69. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
70. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym
71. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
72. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet
73. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

2.1.8. CoreCAL ALNG LicSAPk MVL Pltfrm UsrCAL

Pakiet licencji dostępowych musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów producenta oferowanego oprogramowania:

1. Serwerowych systemów operacyjnych (z wyłączeniem dostępu terminalowego),
2. Serwerów portali intranet,
3. Serwerów poczty elektronicznej,
4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem,
5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej,
6. Klienta systemu antywirusowego.

2.1.9. EntCloudSuiteAddOn ShrdSvr ALNG SubsVL MVL touserCoreCal

Produkt zapewniający poniżej opisane funckcjonalności dla użytkowników posiadających pakiet licencji opisanych w punkcie 2.1.6, 2.1.7, 2.1.8.

Licencja subskrypcyjna systemu operacyjnego klasy PC, który musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

76. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    c. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    d. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
77. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
78. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
79. Wbudowany system pomocy w języku polskim;
80. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
81. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
82. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
83. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
84. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
85. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
86. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
87. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
88. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),

89. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
90. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
91. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
92. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
93. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
94. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
95. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
96. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
97. Obsługa standardu NFC (near field communication),
98. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
99. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
100. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
101. Mechanizmy logowania do domeny w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
102. Mechanizmy wieloelementowego uwierzytelniania.
103. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
104. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
105. Wsparcie dla algorytmów Suite B (RFC 4869),
106. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
107. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
108. Wsparcie dla środowisk Java i.NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
109. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
110. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
111. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
112. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
113. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,

114. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
115. Udostępnianie modemu,
116. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
117. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
118. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
119. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
120. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
121. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
122. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
123. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
124. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
125. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
126. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
127. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
128. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
129. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
130. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
131. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
132. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC

133. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
134. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
135. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
136. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
137. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
138. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
139. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
140. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
141. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
142. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
143. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
144. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
145. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
146. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
147. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym
148. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
149. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet
150. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

Pakiet usług hostowanych

Usługa hostowana (on-line) ma uprawniać użytkowników do wykorzystania usług on-line – portalu wewnętrznego, poczty elektronicznej oraz narzędzi wiadomości błyskawicznych i konferencji głosowych i video. Ponadto musi zawierać 12 miesięczną subskrypcję pakietu biurowego.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

Usługa musi umożliwiać:

e. obsługę poczty elektronicznej,
f. zarządzanie czasem,
g. zarządzania zasobami
h. zarządzanie kontaktami i komunikacją.

Usługa musi dostaczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:

e. Zarządzania użytkownikami poczty,
f. Wsparcia migracji z innych systemów poczty,
g. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
h. Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty.

Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:

d. Posiadanego oprogramowania Outlook (2007 i 2010),
e. Przeglądarki (Web Access),
f. Urządzeń mobilnych.

Wymagane cechy usługi to:

f. Skrzynki pocztowe (do 50GB),
g. Standardowy i łatwy sposób obsługi poczty elektronicznej,
h. Obsługa najnowszych funkcji Outlook 2010 i 2013, takich jak tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari,
i. Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.
j. Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

5. Funkcjonalność podstawowa:
    a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
    b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
    c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami
    d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia
    e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
6. Funkcjonalność wspierająca pracę grupową:
    a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości
    b. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu
    c. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze
    d. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone

e. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania
f. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań
g. Obsługa list i grup dystrybucyjnych.
h. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
i. Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.
j. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
k. Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
l. Funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
m. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
n. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
o. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
p. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.

7. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
   a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja
   b. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.
   c. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.
   d. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.
   e. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.
   f. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
   g. Integracja z usługami zarządzania dostępem do treści (ADRMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania.

h. Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
i. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
j. Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.

8. Wsparcie dla użytkowników mobilnych:
   a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
   b. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
   c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
   d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
   e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
   f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

Usługa portalu on-line musi realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

14. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
15. Zarządzanie strukturą portalu i treściami www,
16. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
17. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
18. Tworzenie repozytoriów wzorów dokumentów,
19. Tworzenie repozytoriów dokumentów,
20. Wspólną, bezpieczną pracę nad dokumentami,
21. Wersjonowanie dokumentów (dla wersji roboczych),
22. Organizację pracy grupowej,
23. Wyszukiwanie treści,
24. Dostęp do danych w relacyjnych bazach danych,
25. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
26. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:

4. Interfejs użytkownika:
    a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
    b. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
    c. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
    d. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
    e. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
5. Projektowanie stron
    a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron,
    b. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
    c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
    d. Możliwość osadzania elementów iFrame w polach HTML na stronie.
6. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
    a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili
    b. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów
    c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
    d. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego
    e. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services
    f. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
    g. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych. Usługa portalu on-line musi mieć wbudowaną funkcjonalność udostępniania użytkownikom komponentów pakietu biurowego on-line dostępnego przez przeglądarkę.

Pakiet biurowy on-line musi spełniać następujące wymagania:

7. Wymagania odnośnie interfejsu użytkownika:
    g. Pełna polska wersja językowa interfejsu użytkownika,

h. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych

8. 2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   i. a. Posiada kompletny i publicznie dostępny opis formatu,
   j. b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   k. c. Umożliwia wykorzystanie schematów XML
   l. d. Wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
9. Pakiet biurowy on-line musi zawierać:
   e. Edytor tekstów
   f. Arkusz kalkulacyjny
   g. Narzędzie do przygotowywania i prowadzenia prezentacji
   h. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
10. Edytor tekstów musi umożliwiać:
    r. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
    s. Wstawianie oraz formatowanie tabel
    t. Wstawianie oraz formatowanie obiektów graficznych
    u. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
    v. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
    w. Automatyczne tworzenie spisów treści
    x. Formatowanie nagłówków i stopek stron
    y. Sprawdzanie pisowni w języku polskim
    z. Śledzenie zmian wprowadzonych przez użytkowników
    aa. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    bb. Określenie układu strony (pionowa/pozioma)
    cc. Wydruk dokumentów
    dd. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
    ee. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
    ff. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
    gg. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
    hh. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
11. Arkusz kalkulacyjny musi umożliwiać:

o. Tworzenie raportów tabelarycznych
p. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
q. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
r. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
s. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
t. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
u. Wyszukiwanie i zamianę danych
v. Wykonywanie analiz danych przy użyciu formatowania warunkowego
w. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
x. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
y. Formatowanie czasu, daty i wartości finansowych z polskim formatem
z. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
aa. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
bb. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    m. Przygotowywanie prezentacji multimedialnych, które będą:
    n. Prezentowanie przy użyciu projektora multimedialnego
    o. Drukowanie w formacie umożliwiającym robienie notatek
    p. Zapisanie jako prezentacja tylko do odczytu.
    q. Nagrywanie narracji i dołączanie jej do prezentacji
    r. Opatrywanie slajdów notatkami dla prezentera
    s. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
    t. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
    u. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
    v. Możliwość tworzenia animacji obiektów i całych slajdów
    w. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
    x. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

Usługa serwera komunikacji wielokanałowej on-line (SKW) wspomagający wewnętrzną komunikację Zamawiającego ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

4. Prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video
5. Przesyłanie wiadomości tekstowych z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę oraz urządzeń mobilnych bazujących na Windows Mobile.
6. Możliwość organizowania telekonferencji

Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty e mail, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać natywną integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu:

4. Ujednolicenie komunikacji biznesowej
    a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
    b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności.
    c. Dostępność aplikacji klienckiej udostepniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc.
    d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością:
        i. Dołączania do telekonferencji
        ii. Szczegółowej listy uczestników
        iii. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
        iv. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli
        v. Głosowania
        vi. Udostępniania plików
        vii. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji
    e. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
    f. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.
    g. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym.
    h. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
    i. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich.
5. W związku z tak postawionymi założeniami SKW ma zapewnić:
    e. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników.
    f. Wykorzystanie statusu obecności i konferencje w czasie rzeczywistym.
    g. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami.
    h. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych.
6. SKW ma zapewnić obsługę następujących funkcjonalności:
    k. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu

wielofunkcyjnego. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności.

l. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.
m. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi,
n. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych.
o. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu.
p. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników.
q. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.
r. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.
s. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów
t. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów.

Subskrypcja pakietu biurowego

Usługa hostowana on-line musi zawierać 36 miesięczną subskrypcję pakietu biurowego spełniającego następujące wymagania:

18. Wymagania odnośnie interfejsu użytkownika:
    d. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
    e. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    f. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
19. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
20. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
21. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
    n. Posiada kompletny i publicznie dostępny opis formatu,
    o. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci

elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),

p. Umożliwia wykorzystanie schematów XML,
q. Wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,

22. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
23. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
24. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
25. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
26. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
    r. Edytor tekstów
    s. Arkusz kalkulacyjny
    t. Narzędzie do przygotowywania i prowadzenia prezentacji
    u. Narzędzie do tworzenia i wypełniania formularzy elektronicznych
    v. Narzędzie do tworzenia drukowanych materiałów informacyjnych
    w. Narzędzie do tworzenia i pracy z lokalną bazą danych
    x. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
    y. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
    z. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
27. Edytor tekstów musi umożliwiać:
    t. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    u. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    v. Wstawianie oraz formatowanie tabel.
    w. Wstawianie oraz formatowanie obiektów graficznych.
    x. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    y. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    z. Automatyczne tworzenie spisów treści.
    aa. Formatowanie nagłówków i stopek stron.
    bb. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    cc. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
    dd. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    ee. Określenie układu strony (pionowa/pozioma).
    ff. Wydruk dokumentów.
    gg. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
    hh. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    ii. Zapis i edycję plików w formacie PDF.

jj. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
kk. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
ll. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

28. Arkusz kalkulacyjny musi umożliwiać:
    q. Tworzenie raportów tabelarycznych
    r. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
    s. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    t. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
    u. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
    v. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
    w. Wyszukiwanie i zamianę danych
    x. Wykonywanie analiz danych przy użyciu formatowania warunkowego
    y. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
    z. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    aa. Formatowanie czasu, daty i wartości finansowych z polskim formatem
    bb. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
    cc. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
    dd. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
    ee. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
    ff. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
29. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    m. Przygotowywanie prezentacji multimedialnych, które będą:
    n. Prezentowanie przy użyciu projektora multimedialnego
    o. Drukowanie w formacie umożliwiającym robienie notatek
    p. Zapisanie, jako prezentacja tylko do odczytu.
    q. Nagrywanie narracji i dołączanie jej do prezentacji
    r. Opatrywanie slajdów notatkami dla prezentera
    s. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
    t. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego

u. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
v. Możliwość tworzenia animacji obiektów i całych slajdów
w. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
x. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

30. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
    i. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania
    j. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.
    k. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
    l. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
    m. Możliwość pobierania danych z platformy do pracy grupowej.
    n. Przesłanie danych przy użyciu usługi Web (tzw. web service).
    o. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
    p. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.
31. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    k. Tworzenie i edycję drukowanych materiałów informacyjnych
    l. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    m. Edycję poszczególnych stron materiałów.
    n. Podział treści na kolumny.
    o. Umieszczanie elementów graficznych.
    p. Wykorzystanie mechanizmu korespondencji seryjnej
    q. Płynne przesuwanie elementów po całej stronie publikacji.
    r. Eksport publikacji do formatu PDF oraz TIFF.
    s. Wydruk publikacji.
    t. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
32. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    i. Tworzenie bazy danych przez zdefiniowanie:
    j. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
    k. Relacji pomiędzy tabelami
    l. Formularzy do wprowadzania i edycji danych
    m. Raportów
    n. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych
    o. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
    p. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
33. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

s. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
t. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
u. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
v. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
w. Automatyczne grupowanie poczty o tym samym tytule,
x. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
y. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
z. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
aa. Zarządzanie kalendarzem,
bb. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
cc. Przeglądanie kalendarza innych użytkowników,
dd. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
ee. Zarządzanie listą zadań,
ff. Zlecanie zadań innym użytkownikom,
gg. Zarządzanie listą kontaktów,
hh. Udostępnianie listy kontaktów innym użytkownikom,
ii. Przeglądanie listy kontaktów innych użytkowników,
jj. Możliwość przesyłania kontaktów innym użytkowników.

34. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    i. Pełna polska wersja językowa interfejsu użytkownika.
    j. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    k. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
    l. Możliwość obsługi tekstowych wiadomości błyskawicznych.
    m. Możliwość komunikacji głosowej i video.
    n. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
    o. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
    p. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Usługa zarządzania stacjami i treścią

Subskrypcja usługi zarządzania urządzeniami mobilnymi oraz tożsamością użytkowników musi spełniać następujące wymagania:

6. Pełne zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT),
7. Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych,
8. Portal klasy self-serivce dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej,
9. Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS),
10. Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

Wymagane scenariusze użycia:

10. Automatyczna klasyfikacja treści dokumentów (przechowywanych na zasobach plikowych, bibliotekach lub transportowanych poprzez system pocztowy) i dynamiczne aplikowanie restrykcji związanych z dostępem do informacji wymusza implementację regulacji i zapobiega niekontrolowanemu wyciekowi informacji
11. Bezpieczna wymiana plików wewnątrz organizacji oraz z zewnętrznymi odbiorcami niezależnie od typu pliku, posiadanego urządzenia (PC lub urządzenie mobilne Windows Phone, Android, iOS) lub przynależności do organizacji umożliwia granularną kontrolę dostępu do poufnych informacji i wymuszenie standardów regulacji sektorowej
12. Wykorzystanie telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS podczas dostępu do aplikacji webowych pozwala na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia
13. Możliwość wydajnej pracy przez użytkowników na licznych lubianych przez nich narzędziach, zapewnia im dostęp do potrzebnych aplikacji
14. Jednokrotne logowanie w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika ułatwia pracę użytkownika i redukuje przestoje czasowe
15. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkowstwem w grupach i obsługi kart inteligentnych pozwala na redukcję ilości zgłoszeń działów wsparcia nawet o 30%
16. Automatyczne przepływy pracy i reguł biznesowych pozwalają na zaoszczędzenie czasu i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie reguł biznesowych)
17. Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwala na audyt i kontrolę zgodności z przepisami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.
18. Zarządzanie urządzeniami mobilnymi pozwala na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwia zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:

System zarządzania tożsamością elektroniczną ma zapewniać agregację oraz synchronizacje danych o użytkownikach różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego Centrum certyfikacji.

Wymagania ogólne

6. Bezpieczeństwo
   System zarządzania tożsamością musi umożliwiać zastosowanie przy połączeniu ze źródłami danych mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji). System powinien zapewniać również prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej poprzez zapory firewall oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
   System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
   System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.
7. Skalowalność
   System zarządzania tożsamością dostarczony w ramach zamówienia musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie od 2 500 do 10 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.
8. Interoperacyjność
   System zarządzania tożsamością powinien zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.
   System zarządzania tożsamością powinien zapewniać możliwość realizacji dwukierunkowej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.
9. Rozszerzalność
   System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości funkcjonalności o połączenia z innymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu. System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.
10. Wydajność
    System musi umożliwiać generowanie i nagrywanie certyfikatów na kartach w liczbie min. xx na godzinę na stanowisko.

Wymagania w zakresie cech i funkcjonalności rozwiązania

4. Agregacja i synchronizacja danych
   a. System powinien zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
   b. System zarządzania tożsamością, w ramach początkowego wdrożenia powinien zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
      i. Pliki tekstowe CSV, AVP, LDIF
      ii. Bazy danych MS SQL 2000\2005, Oracle
      iii. Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.

c. System powinien zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
d. System powinien zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy połączenia poprzez budowę odpowiedniego rozszerzenia systemu.
e. System powinien zapewniać możliwość tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
f. System powinien dostarczać mechanizmów pozwalających na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system powinien umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium. System powinien zapewniać możliwość synchronizacji danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
h. System powinien oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
i. System powinien umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.

5. Repozytorium danych teleadresowych
   e. System powinien dostarczać rozwiązania umożliwiającego agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
   f. System powinien dostarczać interfejsu użytkownika zapewniającego możliwość wyszukiwania oraz przeglądania danych dla wszystkich użytkowników systemu.
   g. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie zarządzania oraz uaktualnienia danych teleadresowych. System powinien zapewniać funkcjonalność synchronizacji uaktualnionych danych do wszystkich zarządzanych systemów.
   h. W ramach interfejsu użytkownika system powinien zapewniać możliwość udostępnienia możliwości edycji zakresu danych samodzielnie przez każdego z użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.
6. Zarządzanie kartą elektroniczną
   bb. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów)
   cc. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników
   dd. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów niekwalifikowanych i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnych przechowywanych i wygenerowanym na karcie)

ee. Dostarczany system musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów niekwalifikowanych dla jednego użytkownika)
ff. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania, tylko do logowania, szyfrowanie /podpisywanie poczty itp.
gg. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP.
hh. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI.
ii. System musi wspierać zarządzanie certyfikatami używanymi do logowania w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
jj. Umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
kk. Po wystawieniu certyfikatu, systemu umożliwia włączenie automatycznej publikacji certyfikatu w katalogu LDAP
ll. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP
mm. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej).
nn. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty)
oo. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:
    i. Użytkownik lub administrator wprowadza PIN inicjujący
    ii. PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW
    iii. System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku
    iv. PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API)
pp. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego
qq. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego)
rr. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:
    iv. nie mniej niż 6 znaków
    v. nie mogą być same cyfry (wymagane litery małe i duże)
    vi. PIN może się powtarzać przez N zmian
ss. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,

tt. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego

uu. Wokflow musi umożliwiać, implementacji następujących scenariuszy użycia:
   vii. w pełni automatyczne wystawianie certyfikatów dla użytkowników
   viii. wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu
   ix. automatyczne odświeżanie wybranych certyfikatów
   x. automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia
   xi. weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu
   xii. powiadamianie administratorów system o wygasaniu certyfikatów dla serwerów / urządzeń wchodzących w skład infrastruktury teleinformatycznej

vv. Workflow musi udostępnić możliwość definiowanie wielu wzorców certyfikatów (w zależności od ich zastosowania) w połączeniu z odpowiednią ścieżką wystawiania/dostarczania certyfikatów do użytkownika, w szczególności:
   iii. Certyfikat do szyfrowania poczty wystawiany jest automatycznie o ile użytkownik posiada certyfikat na karcie elektronicznej do podpisu, podpis ten musi być użyty do podpisania wystawianie certyfikatu do szyfrowania
   iv. Certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW

   Definiowanie takich reguł musi być dostępne bezpośrednio dla operatora systemu i nie może wymagać dodatkowych opłat licencyjnych

ww. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, ilości zmian PIN'ow, ilość odblokowanych kart

xx. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważny

yy. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11

zz. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania)

aaa. System musi wspierać graficzną personalizację kart: (nadruk wielokolorowy)

bbb. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.

Podsystem zarządzania urządzeniami mobilnymi

7. Architektura Systemu UDM

   Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
   d. Integrację z systemem SCCM 2012 R2 w oparciu o natywne interfejsy komunikacyjne
   e. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
   f. Porozumiewania się z użytkownikiem końcowym w języku polskim.

8. Inwentaryzacja sprzętu i zarządzanie zasobami:
    c. Inwentaryzacja zasobów urządzenia mobilnego odbywa się w interwałach czasowych.
    d. Inwentaryzacja sprzętu pozwala na zbieranie następujących informacji
        i. Nazwa urządzenia
        ii. Identyfikator urządzenia
        iii. Nazwa platformy systemu operacyjnego
        iv. Wersja oprogramowania układowego
        v. Typ procesora
        vi. Model urządzenia
        vii. Producent urządzenia
        viii. Architektura procesora
        ix. Język urządzenia
        x. Lista aplikacji zainstalowanych w ramach przedsiębiorstwa
9. Zdalna blokada i wymazanie:
    c. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji.
    d. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
10. Dystrybucja oprogramowania:
    f. Pakiety instalacyjne dla aplikacji mobilnych mogą być przechowywany na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
    g. Systemu UDM umożliwia dystrybucję oprogramowania na prośbę użytkownika, realizowaną poprzez wybór oprogramowania w ramach dostępnego katalogu aplikacji
    h. Katalog aplikacji jest zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
    i. Katalog aplikacji wspiera następujące formaty aplikacji mobilnych:
        i. *.appx (Windows RT)
        ii. *.xap (Windows Phone 8)
        iii. *.ipa (iOS)
        iv. *.apk (Android)
    j. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
        i. Windows Store
        ii. Windows Phone Store
        iii. Android Google Play Store
        iv. iOS App Store
11. Definiowanie polityk urządzenia mobilnego:
    b. Komponenty umożliwiające zdefiniowanie standardu polityk urządzenia mobilnego. W obszarze polityki haseł system zapewni:
        vii. Zdefiniowanie wymuszenia hasła
        viii. Określenia minimalnej długości hasła
        ix. Określenia czasu wygasania hasła
        x. Określenia ilości pamiętanych haseł

xi. Określenia ilości prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia
xii. Określenia czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła

12. Raportowanie, prezentacja danych:
    Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika.

Podsystem ochrony informacji

Usługa bezpieczeństwa informacji musi pozwalać na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem. Usługa musi spełniać następujące wymagania:

12. Usługa musi być dostępna w postaci subskrypcji,
13. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), a nie fizyczne miejsce jej przechowywania,
14. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
15. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
16. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
17. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, np.:
    a. Brak uprawnień dostępu do informacji,
    b. Informacja tylko do odczytu,
    c. Prawo do edycji informacji,
    d. Brak możliwości wykonania systemowego zrzutu ekranu,
    e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
    f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
    g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
18. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
19. Możliwość wyboru restrykcji dostępu w postaci standardowych, łatwych do wyboru szablonów, powstałych na bazie polityk ochrony informacji,
20. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
21. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
22. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi katalogowej

Usługa katalogowa musi zapewnić:

10. Możliwość zintegrowania jednokrotnego logowania (SSO) dla ponad 2500 popularnych aplikacji typu SaaS,
11. Możliwość publikacji aplikacji webowych z wewnątrz organizacji,
12. Możliwość połączenia z usługą Active Directory wewnątrz organizacji,
13. Konsolę zarządzania tożsamością i dostępem,
14. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
15. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
16. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
17. Samoobsługowe resetowania hasła,
18. Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników.

2.1.10. EntCloudSuite ShrdSvr ALNG SubsVL MVL PerUsr

Oferowana subskrypcja musi zawierać następujące składniki.

Licencja subskrypcyjna systemu operacyjnego klasy PC, który musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,

17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Obsługa standardu NFC (near field communication),
23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
26. Mechanizmy logowania do domeny w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
27. Mechanizmy wieloelementowego uwierzytelniania.
28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
30. Wsparcie dla algorytmów Suite B (RFC 4869),
31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
33. Wsparcie dla środowisk Java i.NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
36. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
40. Udostępnianie modemu,
41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
43. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,

46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
51. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
52. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
53. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
54. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
55. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
56. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
57. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
58. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
59. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
60. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
61. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
62. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
63. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
64. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
65. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
66. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
67. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji

68. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
69. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
70. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
71. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
72. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym
73. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
74. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet
75. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

Pakiet usług hostowanych

Usługa hostowana (on-line) ma uprawniać użytkowników do wykorzystania usług on-line – portalu wewnętrznego, poczty elektronicznej oraz narzędzi wiadomości błyskawicznych i konferencji głosowych i video. Ponadto musi zawierać 12 miesięczną subskrypcję pakietu biurowego.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

Usługa musi umożliwiać:
a. obsługę poczty elektronicznej,
b. zarządzanie czasem,
c. zarządzania zasobami
d. zarządzanie kontaktami i komunikacją.

Usługa musi dostaczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:
a. Zarządzania użytkownikami poczty,
b. Wsparcia migracji z innych systemów poczty,
c. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
d. Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty.

Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:
- Posiadanego oprogramowania Outlook (2007 i 2010),
- Przeglądarki (Web Access),
- Urządzeń mobilnych.

Wymagane cechy usługi to:
- Skrzynki pocztowe (do 50GB),
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych funkcji Outlook 2010 i 2013, takich jak tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari,
- Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.
- Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:
1. Funkcjonalność podstawowa:
    a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
    b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
    c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami

   d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia
   e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
2. Funkcjonalność wspierająca pracę grupową:
   a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości
   b. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu
   c. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze
   d. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone
   e. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania
   f. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań
   g. Obsługa list i grup dystrybucyjnych.
   h. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
   i. Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.
   j. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
   k. Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
   l. Funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
   m. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
   n. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
   o. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
   p. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.
3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
   a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja
   b. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.
   c. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.
   d. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.
   e. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.

f. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
g. Integracja z usługami zarządzania dostępem do treści (ADRMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania.
h. Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
i. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
j. Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.

4. Wsparcie dla użytkowników mobilnych:
   a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
   b. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
   c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
   d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
   e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
   f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

Usługa portalu on-line musi realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Tworzenie repozytoriów wzorów dokumentów,
6. Tworzenie repozytoriów dokumentów,
7. Wspólną, bezpieczną pracę nad dokumentami,
8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:

1. Interfejs użytkownika:
    a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
    b. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
    a. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
    b. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
    c. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
2. Projektowanie stron
    a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron,
    b. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
    c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
    d. Możliwość osadzania elementów iFrame w polach HTML na stronie.
3. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
    a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili
    b. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów
    c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
    d. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego
    e. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services
    f. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
    g. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

Usługa portalu on-line musi mieć wbudowaną funkcjonalność udostępniania użytkownikom komponentów pakietu biurowego on-line dostępnego przez przeglądarkę.
Pakiet biurowy on-line musi spełniać następujące wymagania:

1. Wymagania odnośnie interfejsu użytkownika:
    a. Pełna polska wersja językowa interfejsu użytkownika,
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
    a. Posiada kompletny i publicznie dostępny opis formatu,
    b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
    c. Umożliwia wykorzystanie schematów XML

d. Wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)

3. Pakiet biurowy on-line musi zawierać:
   a. Edytor tekstów
   b. Arkusz kalkulacyjny
   c. Narzędzie do przygotowywania i prowadzenia prezentacji
   d. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
4. Edytor tekstów musi umożliwiać:
   a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b. Wstawianie oraz formatowanie tabel
   c. Wstawianie oraz formatowanie obiektów graficznych
   d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
   e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   f. Automatyczne tworzenie spisów treści
   g. Formatowanie nagłówków i stopek stron
   h. Sprawdzanie pisowni w języku polskim
   i. Śledzenie zmian wprowadzonych przez użytkowników
   j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   k. Określenie układu strony (pionowa/pozioma)
   l. Wydruk dokumentów
   m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
   n. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
   o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
   p. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
   q. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
5. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
   e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
   f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
   g. Wyszukiwanie i zamianę danych
   h. Wykonywanie analiz danych przy użyciu formatowania warunkowego

i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, które będą:
   b. Prezentowanie przy użyciu projektora multimedialnego
   c. Drukowanie w formacie umożliwiającym robienie notatek
   d. Zapisanie jako prezentacja tylko do odczytu.
   e. Nagrywanie narracji i dołączanie jej do prezentacji
   f. Opatrywanie slajdów notatkami dla prezentera
   g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
   h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
   i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
   j. Możliwość tworzenia animacji obiektów i całych slajdów
   k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
   l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

Usługa serwera komunikacji wielokanałowej on-line (SKW) wspomagający wewnętrzną komunikację Zamawiającego ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1. Prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video
2. Przesyłanie wiadomości tekstowych z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę oraz urządzeń mobilnych bazujących na Windows Mobile.
3. Możliwość organizowania telekonferencji

Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty e-mail, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać natywną integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu:

1. Ujednolicenie komunikacji biznesowej
   a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
   b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności.
   c. Dostępność aplikacji klienckiej udostepniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc.
   d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością:
      - Dołączania do telekonferencji
      - Szczegółowej listy uczestników
      - Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
      - Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli
      - Głosowania

- Udostępniania plików
- Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji

e. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
f. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.
g. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym.
h. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
i. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich.

2. W związku z tak postawionymi założeniami SKW ma zapewnić:
   a. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników.
   b. Wykorzystanie statusu obecności i konferencje w czasie rzeczywistym.
   c. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami.
   d. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych.
3. SKW ma zapewnić obsługę następujących funkcjonalności:
   a. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności.
   b. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.
   c. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi,
   d. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych.
   e. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu.
   f. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników.
   g. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.
   h. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.
   i. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów
   j. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów.

Subskrypcja pakietu biurowego

Usługa hostowana on-line musi zawierać 36 miesięczną subskrypcję pakietu biurowego spełniającego następujące wymagania:

1. Wymagania odnośnie interfejsu użytkownika:
   a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.

b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

2. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
3. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
4. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
   a. Posiada kompletny i publicznie dostępny opis formatu,
   b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),
   c. Umożliwia wykorzystanie schematów XML,
   d. Wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
5. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
6. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
7. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
8. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
9. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a. Edytor tekstów
   b. Arkusz kalkulacyjny
   c. Narzędzie do przygotowywania i prowadzenia prezentacji
   d. Narzędzie do tworzenia i wypełniania formularzy elektronicznych
   e. Narzędzie do tworzenia drukowanych materiałów informacyjnych
   f. Narzędzie do tworzenia i pracy z lokalną bazą danych
   g. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
   h. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
   i. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
10. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.
    i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.

j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
l. Określenie układu strony (pionowa/pozioma).
m. Wydruk dokumentów.
n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
p. Zapis i edycję plików w formacie PDF.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
r. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
s. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

11. Arkusz kalkulacyjny musi umożliwiać:
a. Tworzenie raportów tabelarycznych
b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
g. Wyszukiwanie i zamianę danych
h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
n. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
o. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a. Przygotowywanie prezentacji multimedialnych, które będą:
b. Prezentowanie przy użyciu projektora multimedialnego
c. Drukowanie w formacie umożliwiającym robienie notatek
d. Zapisanie, jako prezentacja tylko do odczytu.
e. Nagrywanie narracji i dołączanie jej do prezentacji

f. Opatrywanie slajdów notatkami dla prezentera
g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j. Możliwość tworzenia animacji obiektów i całych slajdów
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

13. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
    a. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania
    b. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.
    c. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
    d. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
    e. Możliwość pobierania danych z platformy do pracy grupowej.
    f. Przesłanie danych przy użyciu usługi Web (tzw. web service).
    g. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
    h. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.
14. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    a. Tworzenie i edycję drukowanych materiałów informacyjnych
    b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    c. Edycję poszczególnych stron materiałów.
    d. Podział treści na kolumny.
    e. Umieszczanie elementów graficznych.
    f. Wykorzystanie mechanizmu korespondencji seryjnej
    g. Płynne przesuwanie elementów po całej stronie publikacji.
    h. Eksport publikacji do formatu PDF oraz TIFF.
    i. Wydruk publikacji.
    j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
15. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    a. Tworzenie bazy danych przez zdefiniowanie:
    b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
    c. Relacji pomiędzy tabelami
    d. Formularzy do wprowadzania i edycji danych
    e. Raportów
    f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych
    g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
    h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
16. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,

b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
e. Automatyczne grupowanie poczty o tym samym tytule,
f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
i. Zarządzanie kalendarzem,
j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
k. Przeglądanie kalendarza innych użytkowników,
l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
m. Zarządzanie listą zadań,
n. Zlecanie zadań innym użytkownikom,
o. Zarządzanie listą kontaktów,
p. Udostępnianie listy kontaktów innym użytkownikom,
q. Przeglądanie listy kontaktów innych użytkowników,
r. Możliwość przesyłania kontaktów innym użytkowników.

17. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
    d. Możliwość obsługi tekstowych wiadomości błyskawicznych.
    e. Możliwość komunikacji głosowej i video.
    f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
    g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
    h. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Usługa zarządzania stacjami i treścią

Subskrypcja usługi zarządzania urządzeniami mobilnymi oraz tożsamością użytkowników musi spełniać następujące wymagania:

1. Pełne zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT),
2. Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych,
3. Portal klasy self-serivce dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej,

4. Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS),
5. Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

Wymagane scenariusze użycia:

1. Automatyczna klasyfikacja treści dokumentów (przechowywanych na zasobach plikowych, bibliotekach lub transportowanych poprzez system pocztowy) i dynamiczne aplikowanie restrykcji związanych z dostępem do informacji wymusza implementację regulacji i zapobiega niekontrolowanemu wyciekowi informacji
2. Bezpieczna wymiana plików wewnątrz organizacji oraz z zewnętrznymi odbiorcami niezależnie od typu pliku, posiadanego urządzenia (PC lub urządzenie mobilne Windows Phone, Android, iOS) lub przynależności do organizacji umożliwia granularną kontrolę dostępu do poufnych informacji i wymuszenie standardów regulacji sektorowej
3. Wykorzystanie telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS podczas dostępu do aplikacji webowych pozwala na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia
4. Możliwość wydajnej pracy przez użytkowników na licznych lubianych przez nich narzędziach, zapewnia im dostęp do potrzebnych aplikacji
5. Jednokrotne logowanie w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika ułatwia pracę użytkownika i redukuje przestoje czasowe
6. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkowstwem w grupach i obsługi kart inteligentnych pozwala na redukcję ilości zgłoszeń działów wsparcia nawet o 30%
7. Automatyczne przepływy pracy i reguł biznesowych pozwalają na zaoszczędzenie czasu i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie reguł biznesowych)
8. Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwala na audyt i kontrolę zgodności z przepisami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.
9. Zarządzanie urządzeniami mobilnymi pozwala na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwia zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:

System zarządzania tożsamością elektroniczną ma zapewniać agregację oraz synchronizacje danych o użytkownikach różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego Centrum certyfikacji.

Wymagania ogólne

1. Bezpieczeństwo
   System zarządzania tożsamością musi umożliwiać zastosowanie przy połączeniu ze źródłami danych mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji). System powinien zapewniać również prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej poprzez zapory *firewall* oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
   System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
   System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.
2. Skalowalność
   System zarządzania tożsamością dostarczony w ramach zamówienia musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie od 2 500 do 10 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.

3. Interoperacyjność
   System zarządzania tożsamością powinien zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.
   System zarządzania tożsamością powinien zapewniać możliwość realizacji dwukierunkowej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.
4. Rozszerzalność
   System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości funkcjonalności o połączenia z innymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu. System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.
5. Wydajność
   System musi umożliwiać generowanie i nagrywanie certyfikatów na kartach w liczbie min. xx na godzinę na stanowisko.

Wymagania w zakresie cech i funkcjonalności rozwiązania

1. Agregacja i synchronizacja danych
   a. System powinien zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
   b. System zarządzania tożsamością, w ramach początkowego wdrożenia powinien zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
      - Pliki tekstowe CSV, AVP, LDIF
      - Bazy danych MS SQL 2000\2005, Oracle
      - Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.
   c. System powinien zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
   d. System powinien zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy połączenia poprzez budowę odpowiedniego rozszerzenia systemu.
   e. System powinien zapewniać możliwość tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
   f. System powinien dostarczać mechanizmów pozwalających na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
   g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system powinien umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium. System powinien zapewniać możliwość synchronizacji danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
   h. System powinien oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
   i. System powinien umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.
2. Repozytorium danych teleadresowych
   a. System powinien dostarczać rozwiązania umożliwiającego agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.

b. System powinien dostarczać interfejsu użytkownika zapewniającego możliwość wyszukiwania oraz przeglądania danych dla wszystkich użytkowników systemu.
c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie zarządzania oraz uaktualnienia danych teleadresowych. System powinien zapewniać funkcjonalność synchronizacji uaktualnionych danych do wszystkich zarządzanych systemów.
d. W ramach interfejsu użytkownika system powinien zapewniać możliwość udostępnienia możliwości edycji zakresu danych samodzielnie przez każdego z użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.

3. Zarządzanie kartą elektroniczną
   a. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów)
   b. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników
   c. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów niekwalifikowanych i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnych przechowywanych i wygenerowanym na karcie)
   d. Dostarczany system musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów niekwalifikowanych dla jednego użytkownika)
   e. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania, tylko do logowania, szyfrowanie /podpisywanie poczty itp.
   f. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP.
   g. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI.
   h. System musi wspierać zarządzanie certyfikatami używanymi do logowania w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
   i. Umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
   j. Po wystawieniu certyfikatu, systemu umożliwia włączenie automatycznej publikacji certyfikatu w katalogu LDAP
   k. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP
   l. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej).
   m. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty)
   n. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:
      - Użytkownik lub administrator wprowadza PIN inicjujący
      - PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW
      - System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku

- PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API)

o. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego
p. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego)
q. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:
   - nie mniej niż 6 znaków
   - nie mogą być same cyfry (wymagane litery małe i duże)
   - PIN może się powtarzać przez N zmian
r. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,
s. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego
t. Wokflow musi umożliwiać, implementacji następujących scenariuszy użycia:
   - w pełni automatyczne wystawianie certyfikatów dla użytkowników
   - wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu
   - automatyczne odświeżanie wybranych certyfikatów
   - automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia
   - weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu
   - powiadamianie administratorów system o wygasaniu certyfikatów dla serwerów / urządzeń wchodzących w skład infrastruktury teleinformatycznej
u. Workflow musi udostępnić możliwość definiowanie wielu wzorców certyfikatów (w zależności od ich zastosowania) w połączeniu z odpowiednią ścieżką wystawiania/dostarczania certyfikatów do użytkownika, w szczególności:
   - Certyfikat do szyfrowania poczty wystawiany jest automatycznie o ile użytkownik posiada certyfikat na karcie elektronicznej do podpisu, podpis ten musi być użyty do podpisania wystawianie certyfikatu do szyfrowania
   - Certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW

   Definiowanie takich reguł musi być dostępne bezpośrednio dla operatora systemu i nie może wymagać dodatkowych opłat licencyjnych
v. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, ilości zmian PIN'ow, ilość odblokowanych kart
w. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważny
x. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11
y. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania)
z. System musi wspierać graficzną personalizację kart: (nadruk wielokolorowy)
aa. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.

Podsystem zarządzania urządzeniami mobilnymi

1. Architektura Systemu UDM

   Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:

a. Integrację z systemem SCCM 2012 R2 w oparciu o natywne interfejsy komunikacyjne
b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
c. Porozumiewania się z użytkownikiem końcowym w języku polskim.

2. Inwentaryzacja sprzętu i zarządzanie zasobami:
   a. Inwentaryzacja zasobów urządzenia mobilnego odbywa się w interwałach czasowych.
   b. Inwentaryzacja sprzętu pozwala na zbieranie następujących informacji
      - Nazwa urządzenia
      - Identyfikator urządzenia
      - Nazwa platformy systemu operacyjnego
      - Wersja oprogramowania układowego
      - Typ procesora
      - Model urządzenia
      - Producent urządzenia
      - Architektura procesora
      - Język urządzenia
      - Lista aplikacji zainstalowanych w ramach przedsiębiorstwa
3. Zdalna blokada i wymazanie:
   a. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji.
   b. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
4. Dystrybucja oprogramowania:
   a. Pakiety instalacyjne dla aplikacji mobilnych mogą być przechowywany na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
   b. Systemu UDM umożliwia dystrybucję oprogramowania na prośbę użytkownika, realizowaną poprzez wybór oprogramowania w ramach dostępnego katalogu aplikacji
   c. Katalog aplikacji jest zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
   d. Katalog aplikacji wspiera następujące formaty aplikacji mobilnych:
      - *.appx (Windows RT)
      - *.xap (Windows Phone 8)
      - *.ipa (iOS)
      - *.apk (Android)
   e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
      - Windows Store
      - Windows Phone Store
      - Android Google Play Store
      - iOS App Store
5. Definiowanie polityk urządzenia mobilnego:
   a. Komponenty umożliwiające zdefiniowanie standardu polityk urządzenia mobilnego. W obszarze polityki haseł system zapewni:
      - Zdefiniowanie wymuszenia hasła
      - Określenia minimalnej długości hasła
      - Określenia czasu wygasania hasła
      - Określenia ilości pamiętanych haseł
      - Określenia ilości prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia
      - Określenia czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła
6. Raportowanie, prezentacja danych:
   Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest

możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika.

Podsystem ochrony informacji
Usługa bezpieczeństwa informacji musi pozwalać na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem. Usługa musi spełniać następujące wymagania:

1. Usługa musi być dostępna w postaci subskrypcji,
2. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), a nie fizyczne miejsce jej przechowywania,
3. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
4. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
5. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
6. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, np.:
    a. Brak uprawnień dostępu do informacji,
    b. Informacja tylko do odczytu,
    c. Prawo do edycji informacji,
    d. Brak możliwości wykonania systemowego zrzutu ekranu,
    e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
    f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
    g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
7. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
8. Możliwość wyboru restrykcji dostępu w postaci standardowych, łatwych do wyboru szablonów, powstałych na bazie polityk ochrony informacji,
9. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
10. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
11. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi katalogowej
Usługa katalogowa musi zapewnić:

1. Możliwość zintegrowania jednokrotnego logowania (SSO) dla ponad 2500 popularnych aplikacji typu SaaS,
2. Możliwość publikacji aplikacji webowych z wewnątrz organizacji,
3. Możliwość połączenia z usługą Active Directory wewnątrz organizacji,
4. Konsolę zarządzania tożsamością i dostępem,
5. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
6. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
7. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
8. Samoobsługowe resetowania hasła,
9. Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników.

2.1.11. WinEntforSAwMDOP ALNG UpgrdSAPk MVL

Uaktualnienie systemu operacyjnego klasy PC z prawem do uaktualniania. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
24. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
25. Mechanizmy logowania do domeny w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

26. Mechanizmy wieloelementowego uwierzytelniania.
27. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
28. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
29. Wsparcie dla algorytmów Suite B (RFC 4869),
30. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
31. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
32. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
33. Wsparcie dla JScript i VBScript, Powershell – możliwość uruchamiania interpretera poleceń,
34. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
35. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
36. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
37. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
38. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
39. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
40. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
41. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
42. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
43. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie maszyn wirtualnych,
44. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
45. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
46. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
47. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
48. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
49. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
50. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
51. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
52. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.

53. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
54. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
55. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
56. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
57. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
58. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
59. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
60. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
61. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
62. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
63. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
64. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
65. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
66. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
67. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
68. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
69. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
70. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym
71. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
72. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet
73. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

2.1.12. EntCAL ALNG LicSAPk MVL UsrCAL wSrvcs

Pakiet licencji dostępowych na użytkownika do serwerów produkcji Microsoft musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów:

1. Serwerowych systemów operacyjnych,
2. Podstawowej funkcjonalności serwerów portali wielofunkcyjnych intranet,
3. Podstawowej funkcjonalności serwerów poczty e-mail,

4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem,
5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej,
6. Mechanizmów tworzenia dostępu VPN do systemów operacyjnych
7. Licencje dostępowe rozszerzające zakres funkcji dostępnych posiadaczom licencji dostępowych serwera komunikacji wielokanałowej, pozwalające dodatkowo wykorzystać funkcjonalność serwera komunikacji wielokanałowej w zakresie:
    a. Łączności głosowej i video z wieloma (więcej niż dwoma) uczestnikami konferencji,
    b. Zarządzania połączeniami telefonicznymi i głosowymi
    c. Współdzielenia aplikacji.
8. Serwerów zarządzania, monitorowania, składowania danych i zarządzania maszynami wirtualnymi,
9. Serwerów poczty e-mail w zakresie uzupełniającym pakiet podstawowych licencji dostępowych, zapewniających (w zgodzie z wymaganiami licencyjnymi producenta) możliwość wykorzystania przez użytkowników zaawansowanych narzędzi archiwizacyjnych, ochrony informacji oraz narzędzi poczty głosowej.

Licencje umożliwiające użytkownikom wykorzystanie pełnej funkcjonalności serwera portalu wielofunkcyjnego, uwzględniające dostęp do usług serwera formularzy, narzędzi wizualizacji analiz biznesowych, wspólnej infrastruktury wszystkich stron w organizacji.

2.1.13. OfficeProPlus ALNG LicSAPk MVL

Licencja pakietu biurowego z prawem do uaktualniania. Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
2. Wymagania odnośnie interfejsu użytkownika:
    a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
    a. posiada kompletny i publicznie dostępny opis formatu,
    b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),

   c. umożliwia wykorzystanie schematów XML,
   d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
    a. Edytor tekstów
    b. Arkusz kalkulacyjny
    c. Narzędzie do przygotowywania i prowadzenia prezentacji
    d. Narzędzie do tworzenia i wypełniania formularzy elektronicznych
    e. Narzędzie do tworzenia drukowanych materiałów informacyjnych
    f. Narzędzie do tworzenia i pracy z lokalną bazą danych
    g. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
    h. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
    i. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
11. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.
    i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
    k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    l. Określenie układu strony (pionowa/pozioma).
    m. Wydruk dokumentów.
    n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
    o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    p. Zapis i edycję plików w formacie PDF.
    q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

r. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
s. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

12. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
    d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
    e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
    f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
    g. Wyszukiwanie i zamianę danych
    h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
    i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
    j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
    k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
    l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
    m. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
    n. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
    o. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
    p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
13. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
    b. Prezentowanie przy użyciu projektora multimedialnego
    c. Drukowanie w formacie umożliwiającym robienie notatek
    d. Zapisanie jako prezentacja tylko do odczytu.
    e. Nagrywanie narracji i dołączanie jej do prezentacji
    f. Opatrywanie slajdów notatkami dla prezentera
    g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
    h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
    i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
    j. Możliwość tworzenia animacji obiektów i całych slajdów

k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

14. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
    a. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania
    b. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.
    c. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.
    d. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.
    e. Możliwość pobierania danych z platformy do pracy grupowej.
    f. Przesłanie danych przy użyciu usługi Web (tzw. web service).
    g. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.
    h. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.
15. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    a. Tworzenie i edycję drukowanych materiałów informacyjnych
    b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    c. Edycję poszczególnych stron materiałów.
    d. Podział treści na kolumny.
    e. Umieszczanie elementów graficznych.
    f. Wykorzystanie mechanizmu korespondencji seryjnej
    g. Płynne przesuwanie elementów po całej stronie publikacji.
    h. Eksport publikacji do formatu PDF oraz TIFF.
    i. Wydruk publikacji.
    j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
16. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    a. Tworzenie bazy danych przez zdefiniowanie:
    b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
    c. Relacji pomiędzy tabelami
    d. Formularzy do wprowadzania i edycji danych
    e. Raportów
    f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych
    g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
    h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
17. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
    b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,

c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
e. Automatyczne grupowanie poczty o tym samym tytule,
f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
i. Zarządzanie kalendarzem,
j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
k. Przeglądanie kalendarza innych użytkowników,
l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
m. Zarządzanie listą zadań,
n. Zlecanie zadań innym użytkownikom,
o. Zarządzanie listą kontaktów,
p. Udostępnianie listy kontaktów innym użytkownikom,
q. Przeglądanie listy kontaktów innych użytkowników,
r. Możliwość przesyłania kontaktów innym użytkowników,
s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

18. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
    a. Pełna polska wersja językowa interfejsu użytkownika.
    b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
    d. Możliwość obsługi tekstowych wiadomości błyskawicznych.
    e. Możliwość komunikacji głosowej i video.
    f. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
    g. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.

Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

2.1.14. EntCAL ALNG LicSAPk MVL UsrCAL wSrvcs

Pakiet licencji dostępowych na użytkownika do serwerów produkcji Microsoft musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów:

1. Serwerowych systemów operacyjnych,
2. Podstawowej funkcjonalności serwerów portali wielofunkcyjnych intranet,
3. Podstawowej funkcjonalności serwerów poczty e-mail,
4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem,
5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej,
6. Mechanizmów tworzenia dostępu VPN do systemów operacyjnych
7. Licencje dostępowe rozszerzające zakres funkcji dostępnych posiadaczom licencji dostępowych serwera komunikacji wielokanałowej, pozwalające dodatkowo wykorzystać funkcjonalność serwera komunikacji wielokanałowej w zakresie:
    a. Łączności głosowej i video z wieloma (więcej niż dwoma) uczestnikami konferencji,
    b. Zarządzania połączeniami telefonicznymi i głosowymi
    c. Współdzielenia aplikacji.
8. Serwerów zarządzania, monitorowania, składowania danych i zarządzania maszynami wirtualnymi,
9. Serwerów poczty e-mail w zakresie uzupełniającym pakiet podstawowych licencji dostępowych, zapewniających (w zgodzie z wymaganiami licencyjnymi producenta) możliwość wykorzystania przez użytkowników zaawansowanych narzędzi archiwizacyjnych, ochrony informacji oraz narzędzi poczty głosowej.

Licencje umożliwiające użytkownikom wykorzystanie pełnej funkcjonalności serwera portalu wielofunkcyjnego, uwzględniające dostęp do usług serwera formularzy, narzędzi wizualizacji analiz biznesowych, wspólnej infrastruktury wszystkich stron w organizacji.

2.1.15. CoreCAL ALNG LicSAPk MVL UsrCAL

Pakiet licencji dostępowych musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów producenta oferowanego oprogramowania:

1. Serwerowych systemów operacyjnych (z wyłączeniem dostępu terminalowego),
2. Serwerów portali intranet,
3. Serwerów poczty elektronicznej,
4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem,
5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej,
6. Klienta systemu antywirusowego.

2.1.16. Prjct ALNG LicSAPk MVL

Pakiet zarządzania projektami ma zapewnić możliwość wspomagania dla prowadzenia projektów, między innymi w zakresie tworzenia, oraz wdrażania szablonów planów projektów. Ma zapewnić rozwiązania umożliwiające elastyczne zarządzanie pracą oraz narzędzia do współpracy potrzebne kierownikom projektów. Wraz z rozwojem potrzeb ma umożliwić korzystanie z bardziej zaawansowanych narzędzi do zespołowego zarządzania projektami i portfelem projektów. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.
Pakiet musi umożliwiać planowanie i udostępnianie wymaganych informacji o projekcie, takich jak:

2. Definiowanie projektów,
3. Przygotowanie harmonogramów,
    a. Opis listy zadań do wykonania

   b. Określenie struktury hierarchicznej zadań (WBS)
   c. Określenie zależności między zadaniami – relacje,
4. Tworzenie planów bazowych
5. Zapisywanie projektów,
6. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
7. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,
8. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
9. Opcje automatycznego planowania terminów zadań, wyliczające daty i okresy trwania.
10. Wizualizacja osi czasu przedstawiającej harmonogram i plan projektu.
11. Wsparcie dla planowania kroczącego i tworzenia prognoz, wykorzystujących ręcznie wprowadzone do harmonogramu zadania sumaryczne Top Down.
12. Identyfikacja braków zasobów poprzez porównanie zaplanowanych ręcznie zadań sumarycznych z informacjami spływającymi z podzadań.
13. Definicja aktywnych i nieaktywnych zadań, umożliwiająca przeprowadzenie analizy wielowariantowej.
14. Bilansowanie nadmiernie przydzielonych zasobów – zarówno automatycznie dla całego harmonogramu, jak i ręcznie dla poszczególnych zadań.
15. Grupowanie projektów według zadanych kryteriów,
    a. Etap projektu,
    b. Lokalizacja projektu,
    c. Kierownik projektu,
    d. Itp.
16. Sygnalizacja graficzna opóźnienia zadania względem planu bazowego
    a. Informacja czy jest plan bazowy,
    b. Informacja o odchyleniu względem czasu,
    c. Informacja o odchylenia względem kosztu,
    d. Informacja o odchyleniach względem pracy,
17. Śledzenie postępu realizacji projektu
    a. Analiza czasu,
    b. Analiza kosztu,
    c. Analiza godzin przepracowanych,
18. Zmiana właściciela projektu,
19. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,
20. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów.
21. Łatwą analizę danych poprzez definiowanie filtrów dla kolumn.
22. Szeroki zakres formatowania tekstu.
23. Natywna integracja z składnikami pakietu biurowego między innymi poprzez możliwość przenoszenia informacji do aplikacji pakietu biurowego przy zachowaniu formatowania dzięki funkcjom kopiowania i wklejania.

2.1.17. PrjctPro ALNG LicSAPk MVL w1PrjctSvrCAL

Pakiet zarządzania projektami wraz z licencją dostępową do serwera projektów z prawem do uaktualniania (licencja na użytkownika). Pakiet zarządzania projektami ma zapewnić możliwość wspomagania dla prowadzenia projektów, między innymi w zakresie tworzenia, oraz wdrażania szablonów planów projektów. Ma zapewnić rozwiązania umożliwiające elastyczne zarządzanie pracą oraz narzędzia do współpracy potrzebne kierownikom projektów. Wraz z rozwojem potrzeb ma umożliwić korzystanie z bardziej zaawansowanych narzędzi do zespołowego zarządzania projektami i portfelem projektów. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.

Pakiet musi umożliwiać planowanie i udostępnianie wymaganych informacji o projekcie, takich jak:

1. Definiowanie projektów,
2. Przygotowanie harmonogramów,
    a. Opis listy zadań do wykonania
    b. Określenie struktury hierarchicznej zadań (WBS)
    c. Określenie zależności między zadaniami – relacje,
3. Tworzenie planów bazowych
4. Zapisywanie projektów,
5. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
6. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,
7. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
8. Opcje automatycznego planowania terminów zadań, wyliczające daty i okresy trwania.
9. Wizualizacja osi czasu przedstawiającej harmonogram i plan projektu.
10. Wsparcie dla planowania kroczącego i tworzenia prognoz, wykorzystujących ręcznie wprowadzone do harmonogramu zadania sumaryczne Top Down.
11. Identyfikacja braków zasobów poprzez porównanie zaplanowanych ręcznie zadań sumarycznych z informacjami spływającymi z podzadań.
12. Definicja aktywnych i nieaktywnych zadań, umożliwiająca przeprowadzenie analizy wielowariantowej.
13. Bilansowanie nadmiernie przydzielonych zasobów – zarówno automatycznie dla całego harmonogramu, jak i ręcznie dla poszczególnych zadań.
14. Grupowanie projektów według zadanych kryteriów,
    a. Etap projektu,
    b. Lokalizacja projektu,
    c. Kierownik projektu,
    d. Itp.
15. Sygnalizacja graficzna opóźnienia zadania względem planu bazowego
    a. Informacja czy jest plan bazowy,
    b. Informacja o odchyleniu względem czasu,
    c. Informacja o odchylenia względem kosztu,
    d. Informacja o odchyleniach względem pracy,
16. Śledzenie postępu realizacji projektu
    a. Analiza czasu,
    b. Analiza kosztu,
    c. Analiza godzin przepracowanych,
17. Zmiana właściciela projektu,
18. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,
19. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów.
20. Łatwą analizę danych poprzez definiowanie filtrów dla kolumn.
21. Szeroki zakres formatowania tekstu.
22. Natywna integracja z składnikami pakietu biurowego między innymi poprzez możliwość przenoszenia informacji do aplikacji pakietu biurowego przy zachowaniu formatowania dzięki funkcjom kopiowania i wklejania.
23. Integracja ze środowiskiem serwera zarządzania projektami – pełna, dwukierunkowa synchronizacja danych.
24. Możliwość przypisywania zasobów z Active Directory.

2.1.18. VisioPro ALNG LicSAPk MVL

Zintegrowane środowisko programistyczne powinno:

1. Umożliwiać tworzenie aplikacji dla Windows, aplikacji internetowych, aplikacji opartych na Microsoft Office system, platformie .NET Framework, SQL Server, Windows Azure za pomocą zintegrowanych kreatorów obsługiwanych metodą przeciągnij i upuść,

2. Umożliwiać zintegrowaną obsługę języków Visual Basic, Visual C# i Visual C++ , która pozwala na stosowanie różnych stylów programowania,
3. Obsługiwać funkcje edytora, takie jak zmień i kontynuuj, które upraszczają cykl projektowania, tworzenia kodu i debugowania aplikacji,
4. Obsługiwać wdrażanie aplikacji klienckich z wykorzystaniem ClickOnce, dzięki której programiści i specjaliści IT mogą wdrażać aplikacje i wymagane przez nie komponenty w sposób gwarantujący stałą aktualność aplikacji,
5. Obsługiwać tworzenie aplikacji opartych na .NET Framework, pozwalające na skrócenie czasu opracowywania aplikacji ze względu na mniejszą ilość niezbędnego kodu infrastrukturalnego i podniesienie bezpieczeństwa aplikacji,
6. Wykorzystywać ASP.NET do przyspieszenia tworzenia interaktywnych, atrakcyjnych aplikacji internetowych oraz usług sieciowych. Strony wzorcowe (master pages) umożliwiają utworzenie spójnego wyglądu witryny i zarządzanie wyglądem wielu stron z jednego miejsca
7. Umożliwiać dokonywanie aktualizacji i poprawek systemu przez Internet
8. Umożliwiać pobieranie darmowych aktualizacji w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bezpłatnie) – wymagane podanie nazwy strony www
9. Posiadać graficzny interfejs użytkownika
10. Posiadać zintegorwane graficzne narzędzie do projektowania interfejsu użytkownika
11. Posiadać zintegrowane funkcjonalności umożliwiające współdzielenie zadań i zarządzenie projektem
12. Posiadać narzędzia do refaktoringu bazy danych
13. Posiadać narzędzia do kontroli jakości kodu
14. Posiadać zorganizowany system szkoleń i materiały edukacyjne w języku polskim
15. Umożliwiać dokonywanie zmian kodu podczas sesji debugowania na platformie x86
16. Zawierać szablony projektowe dostosowane do MSF Agile i MSF CMMI
17. Umożliwiać bezpieczną pracę zdalną i lokalną z repozytorium kodu źródłowego
18. Wspierać w zintegrowanym środowisku pracę z zadaniami, zapewniać miechanizmy powiązania zadań z kodem oddawanym przez programistów
19. Zapewniać mechanizmy automatycznej kompilacji rozwiązań .Net oraz automatycznie uruchamiać testy jednostkowe i generować raporty pokazujące listę błędów
20. Możliwość tworzenia testów jednostkowych interfejsu użytkownika poprzez nagrywanie interakcji użytkownika z aplikacją.
21. Posiadać narzędzia pozwalające na tworzenie rozwiązań dla SharePoint Portal Server
22. Posiadać możliwość budowania rozwiązań Silverlight
23. Dawać dostęp do bazy oprogramowania wspomagającego proces wytwórczy.

2.1.19. VSPremwMSDN ALNG LicSAPk MVL

Pakiet programistyczny z usługą wsparcia programistycznego typ 1 z prawem do uaktualniania. Zintegrowane środowisko programistyczne musi zapewniać:

1. Umożliwiać tworzenie aplikacji dla Windows, aplikacji internetowych, aplikacji dla systemu Windows Phone, aplikacji opartych na Microsoft Office system, platformie .NET Framework, SQL Server, Windows Azure za pomocą zintegrowanych kreatorów obsługiwanych metodą przeciągnij i upuść,
2. Umożliwiać zintegrowaną obsługę języków Visual Basic, Visual C# i Visual C++ , która pozwala na stosowanie różnych stylów programowania,
3. Obsługiwać funkcje edytora, takie jak zmień i kontynuuj, które upraszczają cykl projektowania, tworzenia kodu i debugowania aplikacji,
4. Obsługiwać wdrażanie aplikacji klienckich z wykorzystaniem ClickOnce, dzięki której programiści i specjaliści IT mogą wdrażać aplikacje i wymagane przez nie komponenty w sposób gwarantujący stałą aktualność aplikacji,

5. Obsługiwać tworzenie aplikacji opartych na .NET Framework, pozwalające na skrócenie czasu opracowywania aplikacji ze względu na mniejszą ilość niezbędnego kodu infrastrukturalnego i podniesienie bezpieczeństwa aplikacji,
6. Wykorzystywać ASP.NET do przyspieszenia tworzenia interaktywnych, atrakcyjnych aplikacji internetowych oraz usług sieciowych. Strony wzorcowe (master pages) umożliwiają utworzenie spójnego wyglądu witryny i zarządzanie wyglądem wielu stron z jednego miejsca
7. Umożliwiać dokonywanie aktualizacji i poprawek systemu przez Internet
8. Umożliwiać pobieranie darmowych aktualizacji w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bezpłatnie) – wymagane podanie nazwy strony www
9. Posiadać graficzny interfejs użytkownika
10. Posiadać zintegrowane graficzne narzędzie do projektowania interfejsu użytkownika
11. Posiadać zintegrowane funkcjonalności umożliwiające współdzielenie zadań i zarządzenie projektem
12. Posiadać narzędzia do refaktoringu bazy danych
13. Posiadać narzędzia do kontroli jakości kodu
14. Umożliwiać wykrywanie wielokrotnie powielanych fragmentów kodu, poprzez analizę semantyczną
15. Posiadać zorganizowany system szkoleń i materiały edukacyjne w języku polskim
16. Umożliwiać dokonywanie zmian kodu podczas sesji debugowania na platformach x86 i x64
17. Zawierać szablony projektowe dostosowane do MSF Agile, MSF CMMI i SCRUM
18. Umożliwiać bezpieczną pracę zdalną i lokalną z repozytorium kodu źródłowego
19. Wspierać w zintegrowanym środowisku pracę z zadaniami, zapewniać mechanizmy powiązania zadań z kodem oddawanym przez programistów
20. Zapewniać mechanizmy automatycznej kompilacji rozwiązań .Net oraz automatycznie uruchamiać testy jednostkowe i generować raporty pokazujące listę błędów
21. Możliwość tworzenia testów jednostkowych interfejsu użytkownika poprzez nagrywanie interakcji użytkownika z aplikacją.
22. Posiadać narzędzia pozwalające na tworzenie rozwiązań dla SharePoint Portal Server
23. Posiadać możliwość budowania rozwiązań Silverlight
24. Dawać dostęp do bazy oprogramowania wspomagającego proces wytwórczy
25. Zapewniać integrację z przeglądarkami internetowymi, umożliwiającą dwukierunkową komunikację ze środowiskiem programistycznym (m.in. analiza SEO po wygenerowaniu przez serwer strony internetowej, automatyczne odświeżanie wszystkich instancji przeglądarek po dokonaniu zmian w środowisku, itp.)
26. Umożliwiać automatyczną synchronizację ustawień środowiska pomiędzy różnymi stacjami roboczymi
27. Umożliwiać zgłaszanie oraz zarządzanie żądaniami dokonania oceny kodu przez innych członków zespołu

2.1.20. VSUltwMSDN ALNG LicSAPk MVL

Pakiet programistyczny z usługą wsparcia programistycznego typ 2 z prawem do uaktualniania.
Zintegrowane środowisko programistyczne powinno:

1. Umożliwiać tworzenie aplikacji dla Windows, aplikacji internetowych, aplikacji dla systemu Windows Phone, aplikacji opartych na Microsoft Office system, platformie .NET Framework, SQL Server, Windows Azure za pomocą zintegrowanych kreatorów obsługiwanych metodą przeciągnij i upuść,
2. Umożliwiać zintegrowaną obsługę języków Visual Basic, Visual C# i Visual C++ , która pozwala na stosowanie różnych stylów programowania,
3. Obsługiwać funkcje edytora, takie jak zmień i kontynuuj, które upraszczają cykl projektowania, tworzenia kodu i debugowania aplikacji,
4. Obsługiwać wdrażanie aplikacji klienckich z wykorzystaniem ClickOnce, dzięki której programiści i specjaliści IT mogą wdrażać aplikacje i wymagane przez nie komponenty w sposób gwarantujący stałą aktualność aplikacji,
5. Obsługiwać tworzenie aplikacji opartych na .NET Framework, pozwalające na skrócenie czasu opracowywania aplikacji ze względu na mniejszą ilość niezbędnego kodu infrastrukturalnego i podniesienie bezpieczeństwa aplikacji,

6. Wykorzystywać ASP.NET do przyspieszenia tworzenia interaktywnych, atrakcyjnych aplikacji internetowych oraz usług sieciowych. Strony wzorcowe (master pages) umożliwiają utworzenie spójnego wyglądu witryny i zarządzanie wyglądem wielu stron z jednego miejsca
7. Umożliwiać dokonywanie aktualizacji i poprawek systemu przez Internet
8. Umożliwiać pobieranie darmowych aktualizacji w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bezpłatnie) – wymagane podanie nazwy strony www
9. Posiadać graficzny interfejs użytkownika
10. Posiadać zintegorwane graficzne narzędzie do projektowania interfejsu użytkownika
11. Posiadać zintegrowane funkcjonalności umożliwiające współdzielenie zadań i zarządzenie projektem
12. Posiadać zintegrowane narzędzia do automatyzacji i nagrywania testów webowych
13. Umożliwiać generowanie i uruchamianie testów obciążeniowych
14. Posiadać narzędzia do refaktoringu bazy danych
15. Posiadać narzędzia do kontroli jakości kodu
16. Umożliwiać wykrywanie wielokrotnie powielanych fragmentów kodu, poprzez analizę semantyczną
17. Umożliwiać monitorowanie wskaźnków wydajności serwera podczas testów obciążeniowych
18. Posiadać zorganizowany system szkoleń i materiały edukacyjne w języku polskim
19. Umożliwiać dokonywanie zmian kodu podczas sesji debugowania na platformach x86 i x64
20. Zawierać szablony projektowe dostosowane do MSF Agile, MSF CMMI i SCRUM
21. Umożliwiać bezpieczną pracę zdalną i lokalną z repozytorium kodu źródłowego
22. Wspierać z zintegorwanym środowisku pracę z zadaniami, zapewniać miechanizmy powiązania zadań z kodem oddawanym przez programistów
23. Zapewniać mechanizmy automatycznej kompilacji rozwiązań .Net oraz automatycznie uruchamiać testy jednostkowe i generować raporty pokazujące listę błędów
24. Możliwość tworzenia testów jednostkowych interfejsu użytkownika poprzez nagrywanie interakcji użytkownika z aplikacją.
25. Posiadać narzędzia pozwalające na tworzenie rozwiązań dla SharePoint Portal Server
26. Posiadać możliwość budowania rozwiązań Silverlight
27. Wspierać tworzenie diagramów UML
28. Mieć możliwość nagrywania stanu aplikacji w celu historycznego debugowania aplikacji
29. Dostęp do bazy oprogramowania wspomagającego proces wytwórczy
30. Posiadać narzędzia do analizy zrzutów pamięci aplikacji .NET
31. Zapewniać integrację z przeglądarkami internetowymi, umożliwiającą dwukierunkową komunikację ze środowiskiem programistycznym (m.in. analiza SEO po wygenerowaniu przez serwer strony internetowej, automatyczne odświeżanie wszystkich instancji przeglądarek po dokonaniu zmian w środowisku, itp.)
32. Umożliwiać automatyczną synchronizację ustawień środowiska pomiędzy różnymi stacjami roboczymi
33. Umożliwiać zgłaszanie oraz zarządzanie żądaniami dokonania oceny kodu przez innych członków zespołu
34. Posiadać mechanizm, dostarczający bezpośrednio nad deklaracjami metod w kodzie źródłowym informacji na temat rezultatu weryfikujących ją testów jednostkowych, historycznych zmian oraz innych miejsc w kodzie posiadających referencje do danej metody
35. Zapewniać integrację debugera z mapą struktury kodu

2.1.21. CISDataCtr ALNG LicSAPk MVL 2Proc

Zestaw oprogramowania z prawem do uaktualniania składającego się z opisanych w specyfikacji oprogramowania zarządzania środowiskami serwerowymi typ II oraz serwerowego systemu operacyjnego typ II.
Serwerowy system operacyjny z narzędziami zarządzania i monitorowania typ II licencjonowany na 2 procesory fizyczne.
Licencja na serwerowy system operacyjny musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi

uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f. Szyfrowanie plików i folderów.
    g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i. Serwis udostępniania stron WWW.
    j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k. Wsparcie dla algorytmów Suite B (RFC 4869),
    l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
        i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
        ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
        iii. Obsługi 4-KB sektorów dysków
        iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
        v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
        vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego

umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na minimum 2 fizyczne procesory serwera zarządzanego. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do zarządzania dowolną liczbą środowisk systemu operacyjnego na tym serwerze.

Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

- System zarządzania infrastrukturą i oprogramowaniem
- System zarządzania komponentami
- System zarządzania środowiskami wirtualnym
- System tworzenia kopii zapasowych
- System automatyzacji zarządzania środowisk IT
- System zarządzania incydentami i problemami
- Ochrona antymalware

System zarządzania infrastrukturą i oprogramowaniem

System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.

7. Inwentaryzacja i zarządzanie zasobami:
    d. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania
    e. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu
    f. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp…)
    g. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta
    h. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera
8. Użytkowane oprogramowanie – pomiar wykorzystania
    a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania
    b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.
9. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.
10. Definiowanie i sprawdzanie standardu serwera:
    b. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej,
    c. Reguły powinny sprawdzać następujące elementy systemy komputerowego:

- stan usługi (Windows Service)
- obecność poprawek (Hotfix)
- WMI
- rejestr systemowy
- system plików
- Active Directory
- SQL (query)
- Metabase

11. Raportowanie, prezentacja danych:
    a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub
    b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services
    c. System powinien posiadać predefiniowane raport w następujących kategoriach:
        - Sprzęt (inwentaryzacja)
        - Oprogramowanie (inwentaryzacja)
        - Oprogramowanie (wykorzystanie)
        - Oprogramowanie (aktualizacje, w tym system operacyjny)
    d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport
    e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu
12. Analiza działania systemu, logi, komponenty
    a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy
    b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

System zarządzania komponentami

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania:

1. Architektura
    a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.
    b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.
    c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.
    d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.
    e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.
    f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.
    g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).
    h. Wsparcie dla protokołu IPv6.
    i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.
2. Audyt zdarzeń bezpieczeństwa

System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:

a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).
b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.
c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.

3. Konfiguracja i monitorowanie

System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:

a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:
   - rejestru
   - WMI
   - OLEDB
   - LDAP
   - skrypty (uruchamiane w celu wykrycia atrybutów obiektu),

W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.

b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp…
c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:
   - Windows Server 2003/2008/2008R2
   - Active Directory 2003/2008
   - Exchange 2003/2007/2010
   - Microsoft SharePoint 2003/2007/2010
   - Microsoft SharePoint Services 3.0
   - Microsoft SharePoint Foundation 2010
   - SQL 2005/2008/2008R2 (x86/x64/ia64)
   - Windows Client OS (XP/Vista/7)
   - Information Worker (Office, IExplorer, Outlook, itp…)
   - IIS 6.0/7.0/7.5
   - HP-UX 11i v2/v3
   - Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86)
   - Red Hat Enterprise Linux 4/5/6 (x86/x64) Server
   - Novell SUSE Linux Enterprise Server 9/10SP1/11
   - IBM AIX v5.3 i v6.1/v7.1 (POWER)
d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.
e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:
   - interfejsy sieciowe
   - porty
   - sieci wirtualne (VLAN)
   - grupy Hot Standby Router Protocol (HSRP)
f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:
   - SNMP (trap, probe)
   - WMI Performance Counters
   - Log Files (text, text CSV)
   - Windows Events (logi systemowe)
   - Windows Services

- Windows Performance Counters (perflib)
- WMI Events
- Scripts (wyniki skryptów, np.: WSH, JSH)
- Unix/Linux Service
- Unix/Linux Log

g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów

4. Tworzenie reguł
   a. w systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:
      - Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event)
      - Performance based (SNMP performance, WMI performance, Windows performance)
      - Probe based (scripts: event, performance)
   b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.
   c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:
      - na ilość takich samych próbek o takiej samej wartości
      - na procentową zmianę od ostatniej wartości próbki.
   d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia" się monitorowanego parametru w zakresie przebiegu bazowego „baseline" w zadanym okresie czasu.
   e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.
   f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:
      - ASP .Net Application
      - ASP .Net Web Service
      - OLE DB
      - TCP Port
      - Web Application
      - Windows Service
      - Unix/Linux Service
      - Process Monitoring

Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji

   g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.
   h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp…) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).
   i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.
   j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostępność), i licznika wydajności (z agregacją dla wartości – min, max, avg).

5. Przechowywanie i dostęp do informacji:
   a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp.) powinny być przechowywane w bazie danych operacyjnych.
   b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.

c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).
d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.
e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.
f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:
   - XML
   - CSV
   - TIFF
   - PDF
   - XLS
   - Web archive

6. Konsola systemu zarządzania
   a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.
   b. System powinien udostępniać dwa rodzaje konsoli:
      - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna)
      - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).
   c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:
      - Alerts
      - Events
      - State
      - Performance
      - Diagram
      - Task Status
      - Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).
   d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.
   e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp…), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych".
   f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.
   g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
      - opcji definiowania ról użytkowników
      - opcji definiowania widoków
      - opcji definiowania i generowania raportów
      - opcji definiowania powiadomień
      - opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących
      - opcji instalacji/deinstalacji klienta
   h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostepu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).
7. Wymagania dodatkowe

a. System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na:
   - Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
   - Wykonywanie operacji w systemie z poziomu linii poleceń,
   - Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
   - Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie,

System zarządzania środowiskami wirtualnym

System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1. Architektura
   a. System zarządzania środowiskiem wirtualnym powinien składać się z:
      - serwera zarządzającego,
      - relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
      - konsoli, instalowanej na komputerach operatorów,
      - portalu self-service (konsoli webowej) dla operatorów „departamentowych”,
      - biblioteki, przechowującej komponenenty niezbędne do budowy maszyn wirtualnych,
      - agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
      - „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.
   b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
   c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.
2. Interfejs użytkownika
   a. Konsola musi umożliwiać wykonywanie codziennych zadań związnych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.
   b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień posczególnym operatorom do grup hostów.
   c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp...
   d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.
   e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.
3. Scenariusze i zadania
   a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:
      1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,
      2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:
         - profilu sprzętowego
         - profilu systemu operacyjnego,
         - przygotowanych dysków twardych,
   b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.
   c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:
      - w trybie migracji „on-line” – bez przerywania pracy,
      - w trybie migracji „off-line – z zapisem stanu maszyny
   d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.
   e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.

f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance" w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.
g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.
h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.

4. Wymagania dodatkowe
   a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.
   b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.
   c. System musi kreować raporty z działania zarządzanego środowiska, w tym:
      - utylizacja poszczególnych hostów,
      - trend w utylizacji hostów,
      - alokacja zasobów na centra kosztów,
      - utylizacja poszczególnych maszyn wirtualnych,
      - komputery-kandydaci do wirtualizacji
   d. System musi umożliwiać skorzystanie z szablonów:
      - wirtualnych maszyn
      - usług

oraz profili dla:

      - aplikacji
      - serwera SQL
      - hosta
      - sprzętu
      - systemu operacyjnego gościa
   e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).
   f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.
   g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją)

System tworzenia kopii zapasowych

System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania:

1. System musi składać się z:
   a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
   b. agentów kopii zapasowych instalowanych na komputerach zdalnych
   c. konsoli zarządzającej
   d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach
   e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną
   f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
2. System kopii zapasowych musi umożliwiać:
   a. zapis danych na puli magazynowej złożonej z dysków twardych
   b. zapis danych na bibliotekach taśmowych
3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej.
4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe.
5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej.
6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania.

7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii.
8. System kopii zapasowych powinien umożliwiać przywrócenie:
   a. danych plikowych
   b. danych aplikacyjnych
   c. stanu systemu (Systemstate)
   d. obrazu systemu operacyjnego (tzw. Bare Metal Restore)
9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych
10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości
11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy
12. System kopii zapasowych musi rozpoznawać aplikacje:
    a. ze względu na tworzone logi transakcyjne:
    - Microsoft Exchange Server
    - Microsoft Office Sharepoint Server
    - Microsoft SQL Server
    b. ze względu na zapewnienie nieprzerwalności pracy
    - Microsoft Virtual Server 2005
    - Microsoft Hyper-V server
13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach
14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach
15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów
16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń
17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje”
18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych
19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych
20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).
21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku
22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat
23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe.
25. System kopii zapasowych musi umożliwiać odtworzenie danych do:
    a. lokalizacji oryginalnej
    b. lokalizacji alternatywnej
    c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk.

1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie.
2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT.
3. System musi wspomagać planowanie i automatyzację wdrażania poprawek.
4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych.
5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania worklow.
6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, IBM Tivoli i BMC Patrol do zarządzania oprogramowaniem i sprzętem.
7. Wbudowane (gotowe) workflow, takie jak:
   - Active Directory Password Reset
   - Microsoft Cluster Patching
   - Microsoft SQL Server Cluster Patching
   - Microsoft SQL: Server Dump Copy Load
   - Operations Manager Event Remediation
   - Operations Manager Event Remediation and Enrichment
   - Operations Manager Service Alert Testing
   - VM Provisioning
   - Working with FTP
   - Operations Manager Tool Integration
   - Operations Manager: Manager of Managers
   - Operations Manager: Maintenance Windows
   - Active Directory: New Employee Onboarding
   - Operations Manager: Multi-Service Desk Integration

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi spełniać następujące wymagania:

1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna)
2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:
   - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,
   - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,
   - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,
   - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
   - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,
   - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,
   - Tworzenie baz wiedzy na temat rozwiązywania problemów,
   - Automatyzację działań w przypadku znanych i opisanych problemów,
   - Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.

Ochrona antymalware

Oprogramowanie antymalware musi spełniać następujące wymagania:

1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem
3. Centralne zarządzanie politykami ochrony.
4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5. Mechanizmy wspomagające masową instalację.
6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów", skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.
7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.).
10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.

System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

2.1.22. ExchgSvrEnt ALNG LicSAPk MVL

Serwer systemu poczty elektronicznej z prawem do uaktualniania musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
    a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.
    b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
    c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
    d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.
    e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
    f. Pełne wsparcie dla klienta poczty elektronicznej MS Outlook 2007 i nowszych wersji.
2. Funkcjonalność wspierająca pracę grupową:
    a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie.
    b. Możliwość określenia terminu wygaśnięcia wiadomości.
    c. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
    d. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.

e. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone.
f. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania.
g. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.
h. Mechanizm udostępniania współdzielonych skrzynek pocztowych.
i. Obsługa list i grup dystrybucyjnych.
j. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
k. Możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności.
l. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
m. Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami.
n. Konfigurowalna funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
o. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
p. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
q. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów.
r. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby wsparcia ze strony informatyków.
s. Mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący priorytetyzacją wyników wyszukiwania.
t. Możliwość wyszukiwania i łączenia danych (zgodnie z nadanymi uprawnieniami) z systemu poczty elektronicznej oraz innych systemów w organizacji (portali wielofunkcyjnych, komunikacji wielokanałowej i serwerów plików).
u. Możliwość dostępu do poczty elektronicznej i dokumentów przechowywanych w portalu wielofunkcyjnym z poziomu jednego interfejsu zarządzanego przez serwer poczty elektronicznej.

3. Funkcjonalność wspierająca zarządzanie systemem poczty:
   a. Oparcie się o profile użytkowników usługi katalogowej Active Directory.
   b. Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk i logów użytkowników.
   c. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu.
   d. Możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników.
   e. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer.
   f. Możliwość korzystania interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.
   g. Narzędzia kreowania, wdrażania i zarządzania politykami nazewnictwa grup dystrybucyjnych.
4. Utrzymanie bezpieczeństwa informacji
   a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym: śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, oraz archiwizacja danych.
   b. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym

za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.

c. Mechanizm zapobiegania wycieku danych ograniczający możliwość wysyłania danych poufnych do nieuprawnionych osób poprzez konfigurowalne funkcje monitoringu i analizy treści, bazujący na ustalonych politykach bezpieczeństwa.
d. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości.
e. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
f. Integracja z usługami zarządzania dostępem do treści pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania. Wymagana jest możliwość użycia 2048-bitowych kluczy RSA, 256-bitowych kluczy SHA-1 oraz algorytmu SHA-2.
g. Odbieranie wiadomości zabezpieczonych funkcją IRM przez zewnętrznych użytkowników oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
h. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
i. Wbudowane filtrowanie oprogramowania złośliwego, wirusów i oprogramowania szpiegującego zawartego w wiadomościach wraz z konfigurowalnymi mechanizmami powiadamiania o wykryciu i usunięciu takiego oprogramowania.
j. Mechanizm audytu dostępu do skrzynek pocztowych z kreowaniem raportów audytowych.

5. Wsparcie dla użytkowników mobilnych:
   a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
   b. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
   c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone.
   d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.
   e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
   f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.
6. Funkcje związane z niezawodnością systemu:
   a. Zapewnienie pełnej redundancji serwerów poczty elektronicznej bez konieczności wdrażania klastrów oraz niezależnych produktów do replikacji danych.
   b. Automatyzacja replikacji bazy danych i przełączania awaryjnego już dla dwóch serwerów poczty, a także w wypadku centrów danych rozproszonych geograficznie.
   c. Utrzymanie dostępności i uzyskanie możliwości szybkiego odzyskiwania po awarii dzięki możliwości konfiguracji wielu replik każdej bazy danych skrzynki pocztowej.
   d. Automatyczne odtwarzanie redundancji poprzez tworzenie kopii zapasowych w miejsce kopii na uszkodzonych dyskach według zadanego schematu.
   e. Ograniczenie zakłócenia pracy użytkowników podczas przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie – nawet w godzinach pracy biurowej.

f. Zapewnienie ochrony przed utratą e-maili spowodowaną uaktualnianiem lub awarią roli serwera transportu poprzez zapewnienie redundancji i inteligentne przekierowywanie poczty na inną dostępną ścieżkę.
g. Obsługa ponad pięciu baz danych.

2.1.23. ExchgSvrStd ALNG LicSAPk MVL

Serwer systemu poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
    a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.
    b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
    c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
    d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.
    e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
    f. Pełne wsparcie dla klienta poczty elektronicznej MS Outlook 2007 i nowszych wersji.
2. Funkcjonalność wspierająca pracę grupową:
    a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie.
    b. Możliwość określenia terminu wygaśnięcia wiadomości.
    c. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
    d. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.
    e. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone.
    f. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania.
    g. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.
    h. Mechanizm udostępniania współdzielonych skrzynek pocztowych.
    i. Obsługa list i grup dystrybucyjnych.
    j. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
    k. Możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności.
    l. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
    m. Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami.
    n. Konfigurowalna funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
    o. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
    p. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
    q. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów.
    r. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby wsparcia ze strony informatyków.

s. Mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący priorytetyzacją wyników wyszukiwania.
t. Możliwość wyszukiwania i łączenia danych (zgodnie z nadanycmi uprawnieniami) z systemu poczty elektronicznej oraz innych systemów w organizacji (portali wielofunkcyjnych, komunikacji wielokanałowej i serwerów plików).
u. Mozliwość dostępu do poczty elektronicznej i dokumentów przechowywanych w portalu wielofunkcyjnym z poziomu jednego interfejsu zarządzanego przez serwer poczty elektronicznej.

3. Funkcjonalność wspierająca zarządzanie systemem poczty:
   a. Oparcie się o profile użytkowników usługi katalogowej Active Directory.
   b. Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk i logów uzytkowników.
   c. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu.
   d. Możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników.
   e. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer.
   f. Możliwość korzystania interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.
   g. Narzędzia kreowania, wdrażania i zarządzania politykami nazewnictwa grup dystrybucyjnych.
4. Utrzymanie bezpieczeństwa informacji
   a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym: śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, oraz archiwizacja danych.
   b. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.
   c. Mechanizm zapobiegania wycieku danych ograniaczający możliwość wysyłania danych poufnych do nieuprawnionych osób poprzez konfigurowalne funkcje monitoringu i analizy treści, bazujący na ustalonych politykach bezpieczeństwa.
   d. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości.
   e. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
   f. Integracja z usługami zarządzania dostępem do treści pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania. Wymagana jest możliwość użycia 2048-bitowych kluczy RSA, 256-bitowych kluczy SHA-1 oraz algorytmu SHA-2.
   g. Odbieranie wiadomości zabezpieczonych funkcją IRM przez zewnętrznych użytkowników oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
   h. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
   i. Wbudowane filtrowanie oprogramowania złośliwego, wirusów i oprogramowania szpiegującego zawartego w wiadomościach wraz z konfigurowalnymi mechanizmami powiadamiania o wykryciu i usunięciu takiego oprogramowania.
   j. Mechanizm audytu dostępu do skrzynek pocztowych z kreowaniem raportów audytowych.
5. Wsparcie dla użytkowników mobilnych:
   a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem

podstawowej funkcjonalności systemu. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem

b. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone.
d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.
e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

6. Funkcje związane z niezawodnością systemu:
    a. Zapewnienie pełnej redundancji serwerów poczty elektronicznej bez konieczności wdrażania klastrów oraz niezależnych produktów do replikacji danych.
    b. Automatyzacja replikacji bazy danych i przełączania awaryjnego już dla dwóch serwerów poczty, a także w wypadku centrów danych rozproszonych geograficznie.
    c. Utrzymanie dostępności i uzyskanie możliwości szybkiego odzyskiwania po awarii dzięki możliwości konfiguracji wielu replik każdej bazy danych skrzynki pocztowej.
    d. Automatyczne odtwarzanie redundancji poprzez tworzenie kopii zapasowych w miejsce kopii na uszkodzonych dyskach według zadanego schematu.
    e. Ograniczenie zakłócenia pracy użytkowników podczas przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie – nawet w godzinach pracy biurowej.
    f. Zapewnienie ochrony przed utratą e-maili spowodowaną uaktualnianiem lub awarią roli serwera transportu poprzez zapewnienie redundancji i inteligentne przekierowywanie poczty na inną dostępną ścieżkę.

2.1.24. FrfrntIdnttyMgrCAL ALNG LicSAPk MVL UsrCAL

Licencje dostępowe pozwalające użytkownikom na wykorzystanie funkcji posiadanego przez Zamawiającego serwera Microsoft Forefront Identity Manager – licencja na użytkownika.

2.1.25. PrjctSvr ALNG LicSAPk MVL

Serwer zarządzania projektami ma być oparty na platformie portalu wielofunkcyjnego i musi spełniać następujące wymagania i funkcje:

1. Zarządzania projektami i portfelami projektów.
2. Wykorzystanie środowiska portalu wielofunkcyjnego, jako interfejsu użytkownika.
3. Implementacja przyjętych w skali organizacji procedur zarządzania projektami. Planowanie, śledzenie i kontrola realizacji projektów muszą odbywać się w oparciu o procedury przyjęte w ramach własnych doświadczeń projektowych. Wymagana jest implementacja rozwiązania umożliwiającego śledzenie realizowanych projektów, postępów prac, obciążenia zasobów, kontrolę kosztów etc.
4. Współdziałanie z kalendarzami systemu Exchange w zakresie przepływu informacji o zadaniach i ich aktualizacji.
5. Wykorzystanie otwartego standardu OData do wyszukiwania danych i ich analizy.

6. Dane dotyczące realizowanych projektów i dokumentacja projektowa muszą być przechowywane w sposób bezpieczny z ochroną dostępu dla uprawnionych osób. System ma umożliwić dostęp do aktualnego statusu prowadzonych projektów.
7. Możliwość wykorzystania profili użytkowników lub ich grup z usługi katalogowej przy udzielaniu uprawnień dostępu.
8. Kontrola, rozpatrywanie i zatwierdzanie dokumentów za pomocą definiowalnego przepływu pracy (workflow),
9. Możliwość definiowania przepływu pracy przy pomocy oprogramowania Visio.
10. System zarządzania projektami:
    a. szybki wgląd w aktualny status realizowanych projektów,
    b. określenie kosztów ponoszonych w poszczególnych projektach,
    c. ocenę prac w zakresie zgodności z harmonogramem i przyjętym budżetem,
    d. określenie zasobów zaangażowanych w realizację poszczególnych projektów i poziomu ich zaangażowania,
    e. określenie odpowiedzialności za realizację poszczególnych zadań i projektów,
    f. aktualną ocenę stanu dostępności zasobów w organizacji.
11. Dostęp do funkcji systemu poprzez przeglądarkę Internet Explorer, Firefox, Safari i Chrome.
12. Możliwość definiowania projektów za pomocą pakietu zarządzania projektami (niezależnego narzędzia instalowanego na stacjach klienckich).

Ze względu na to, że Zamawiający realizuje dużą liczbę równoczesnych projektów, a każdy kierownik projektu ma różne potrzeby, charakterystyczne dla pełnionych przez niego ról, wybrane rozwiązanie ma udostępniać poszczególnym grupom odbiorców różne cechy i funkcjonalność.

1. Zarządzanie projektami

System zarządzania projektami ma zapewnić sprawną koordynację i zarządzanie projektami. Dzięki Centralnemu Repozytorium Projektów (CRP), kierownictwo ma utrzymywać oraz wdrażać szablony planów projektów. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.

Wymagane informacje o Projekcie

a. Definiowanie inicjatyw projektowych,
b. Definiowanie typów projektów dla wszystkich żądań i możliwość powiązania ich z cyklami pracy, planem projektu i zindywidualizowanymi szablonami miejsca pracy.
c. Przygotowanie harmonogramów,
    - Opis listy zadań do wykonania
    - Określenie struktury hierarchicznej zadań (WBS)
    - Określenie zależności między zadaniami – relacje,
d. Zapisywanie projektów do centralnego repozytorium,
e. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
f. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,
g. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
h. Przeglądanie informacji o projektach za pomocą przeglądarki internetowej,
i. Grupowanie projektów według zadanych kryteriów,
    - Etap projektu,
    - Lokalizacja projektu,
    - Kierownik projektu,
    - Itp.
j. Sygnalizacja graficzna opóźnienia zadania względem planu bazowego
    - Informacja czy jest plan bazowy,
    - Informacja o odchyleniu względem czasu,
    - Informacja o odchylenia względem kosztu,

- Informacja o odchyleniach względem pracy,

k. Śledzenie postępu realizacji projektu
   - Analiza czasu,
   - Analiza kosztu,
   - Analiza godzin przepracowanych,

l. Raportowanie
   - Informacja o zadaniach opóźnionych,
   - Informacja o kosztach zadań,
   - Informacja o pracy w zadaniach,

m. Delegowanie uprawnień do projektu,
n. Zmiana właściciela projektu,
o. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,
p. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów,

2. Zarządzanie portfelami projektów

System zarządzania projektami ma zapewnić sprawną koordynację i zarządzanie wszystkimi prowadzonymi projektami poprzez ustalenie zależności między projektami i używanymi do nich zasobami. W związku z tym system musi posiadać następujące cechy:

a. Narzędzia pozwalające na wybór optymalnego portfela projektów dostosowany do różnych ograniczeń, w tym budżetowych.
b. Analizy pozwalające określić priorytetowe projekty ze względu na wiele czynników – wartość strategiczną, wartość finansową i ryzyko.
c. Narzędzia pozwalające porównywać scenariusze optymalizacji projektów za pomocą kart wyników.

Narzędzia pozwalające na zmianę terminów projektów wewnątrz horyzontu czasowego planowania, w celu zoptymalizowania wykorzystania zasobów przy zachowaniu współzależności projektów.

2.1.26. SfBSvr ALNG LicSAPk MVL

Serwer komunikacji wielokanałowej z prawem do uaktualniania (SKW) wspomagający wewnętrzną komunikację Zamawiającego ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1. Prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video
2. Przesyłanie wiadomości błyskawicznych (tekstowych) z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę.
3. Możliwość organizowania telekonferencji

Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty elektronicznej, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu:

1. Ujednolicenie komunikacji biznesowej
   a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
   b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności.
   c. Dostępność aplikacji klienckiej udostepniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc.
   d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością:
      - Dołączania do telekonferencji
      - Szczegółowej listy uczestników

- Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
- Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli
- Głosowania
- Udostępniania plików
- Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji

e. Dostępność funkcjonalności text-to-speech w języku polskim
f. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
g. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.
h. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym.
i. Usługi bezpieczeństwa umożliwiające chronioną komunikację wewnątrz organizacji.
j. Aplikacje biznesowe dostępne bezpośrednio na urządzeniach mobilnych.
k. Mobilny dostęp do ludzi i danych firmowych.
l. Obniżone koszty dzięki zdalnej administracji i zarządzaniu urządzeniami.
m. Niższe koszty usług telefonicznych i komunikacji między odległymi lokalizacjami.
n. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
o. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich.

2. W związku z tak postawionymi założeniami SKW ma zapewnić:
   a. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników.
   b. Ulepszoną komunikację poprzez wykorzystanie statusu obecności i konferencje w czasie rzeczywistym.
   c. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami.
   d. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych.
3. SKW ma zapewnić obsługę następujących funkcjonalności:
   a. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności.
   b. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.
   c. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi, możliwość realizacji połączeń głosowych do i z sieci PSTN (publicznej sieci telefonicznej). Możliwość realizacji funkcjonalności RCC (Remote Call Controll) tj. zarządzania telefonem stacjonarnym firm trzecich z poziomu komunikatora.
   d. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych.
   e. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu.
   f. Możliwość dostępu do telekonferencji użytkownikom wykorzystujących urządzenia z systemami Android, Apple iOS, Windows, Windows Phone.
   g. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników.

h. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie z poziomu serwera WWW.
i. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.
j. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.
k. Wbudowane funkcjonalności: SIP Proxy
l. Wbudowana funkcjonalność mostka konferencyjnego MCU
m. Obsługa standardów: CSTA, TLS, SIP over TCP
n. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
o. Kodowanie video H.264,
p. Wsparcie dla adresacji IPv6,
q. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
r. Wykorzystanie wyłącznie 64 bitowej platformy serwerowego systemu operacyjnego
s. Możliwość instalacji w układzie klastra niezawodnościowego.
t. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów.

4. Wymagania w zakresie administracji i zarządzania serwerem:
   a. Mechanizm pozwalający na przełączenie serwera w tryb off-line (np. w celach dokonania czynności administracyjnych) bez utraty usług serwera dla zalogowanych użytkowników, a jednocześnie blokujący dostęp nowych użytkowników
   b. Możliwość administrowania z wiersza poleceń
   c. Możliwość administrowania za pomocą interfejsu Web
   d. Mechanizm gotowych kreatorów (wizard) umożliwiających planowanie i zmiany topologii serwerów SKW
   e. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
5. Dodatkowe wymagania
   a. Możliwość instalacji w układzie klastra typu load-balancing,
   b. DNS load balancing balansujący ruch sieciowy dla serwerów SKW, na przykład w zakresie ruchu SIP lub mediów,
   c. Możliwość instalacji bazy danych serwera komunikacji wielokanałowej na oddzielnym serwerze,
   d. Możliwość wydzielenia na niezależnym serwerze roli serwera konferencji audio i video.

2.1.27. SharePointSvr ALNG LicSAPk MVL

Serwery portali intranet i internet z prawem do uaktualniania muszą realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych i zewnętrznych,
2. Zarządzanie strukturą portalu i treściami www,
3. Uczestnictwo Internautów w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
4. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej,
5. Udostępnienie formularzy elektronicznych,
6. Tworzenie repozytoriów wzorów dokumentów,
7. Tworzenie repozytoriów dokumentów,
8. Wspólną, bezpieczną pracę nad dokumentami,
9. Wersjonowanie dokumentów (dla wersji roboczych),
10. Organizację pracy grupowej,
11. Wyszukiwanie treści,

12. Dostęp do danych w relacyjnych bazach danych,
13. Analizy danych wraz z graficzną prezentacją danych,
14. Możliwość wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning).
15. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
16. PW muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery PW muszą posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:

4. Interfejs użytkownika:
    c. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
    d. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
    a. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
    b. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
    c. Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu
    d. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
5. Uwierzytelnianie – wbudowane mechanizmy wspierające uwierzytelnianie na bazie:
    a. Oświadczeń (claim-based authentication) z wykorzystaniem:
        - Open Authorization 2.0 dla uwierzytelniania aplikacji,
        - Uwierzytelniania w trybie server-to-server,
        - SAML
        - Windows claims
    b. Pojedynczego logowania domenowego (single-sign on),
    c. Na bazie formularzy (Form-based).
6. Projektowanie stron
    a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron,
    b. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
    c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
    d. Możliwość osadzania elementów iFrame w polach HTML na stronie.
7. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
    a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili
    b. Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów
    c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
    d. Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony)
    e. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego

f. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services
g. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
h. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

8. Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:
    a. Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.
    b. Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML)
    c. Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego
    d. Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów
    e. Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte
    f. Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana
    g. Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny).
    h. Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo,
9. Organizacja i publikacja treści:
    a. Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.
    b. Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu.
    c. Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.
    d. Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię.
    e. Automatyczne generowanie mapy stron portalu.
    f. Możliwość definiowania nawigacji w oparciu o centralne zarządzanie metadanymi.
    g. Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.
    h. Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do

odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.

i. Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.
j. Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.
k. Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu oraz zapewnienie automatycznego tłumaczenia na wybrane języki.

10. Repozytoria dokumentów:
    a. Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów.
    b. Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa.
    c. Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu.
    d. Możliwość publikacji plików w strukturze katalogów.
    e. Możliwość publikacji materiałów wideo oraz audio.
    f. Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku.
    g. Możliwość nawigacji po repozytorium dokumentów (lub całym portalu) w oparciu o metadane z metryk dokumentów.
    h. Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania.
    i. Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x… 2.0), automatyczna kontrola wersji przy publikacji dokumentów.
    j. Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu.
    k. Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.
    l. Możliwość definiowania polityk cyklu życia dokumentu oraz retencji dokumentów.
    m. Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich.
    n. Możliwość automatyzacji usuwania duplikatów dokumentów.
11. Wyszukiwanie treści:
    a. Pełnotekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice.
    b. Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu
    c. Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, oraz zakresów dat publikacji
    d. Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów
    e. Możliwość definiowania słownika słów wykluczonych (często używanych)

f. Możliwość tworzenia „linków sponsorowanych", prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu
g. Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu.
h. Przedstawianie w wynikach duplikatów plików
i. Statystyki wyszukiwanych fraz

12. Administracja intranetem i inne funkcje:
    a. Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych
    b. Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu
    c. Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści
    d. Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu oraz centralnie zarządzanego zbioru metadanych z wyznaczonym administratorem merytorycznym.
    e. Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów,
    f. Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu
    g. Statystyki odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy
    h. Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie intranetu do celów pracy działów i zespołów zadaniowych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń
    i. Funkcjonalność publikowania na portalu formularzy elektronicznych XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.
    j. Mechanizmy wspierające przepływy pracy (workflow) wraz z funkcjonalnością definiowania procesów obiegu dokumentów, integracji przepływów z web-services, wywoływania web-services z poziomu workflow bez konieczności kodowania przy wykorzystaniu prostych w obsłudze narzędzi portalu.

2.1.28. WinSvrDataCtr ALNG LicSAPk MVL 2Proc

Licencja na serwerowy system operacyjny typ II z prawem do uaktualniania musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

32. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
33. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

34. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
35. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
36. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
37. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
38. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
39. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
40. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
41. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
42. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
43. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
44. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
45. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
46. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
47. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
48. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
49. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
50. Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników.
51. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
52. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
53. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
54. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
55. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
56. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    n. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    o. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

   i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
   ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
   iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
   iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
p. Zdalna dystrybucja oprogramowania na stacje robocze.
q. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
r. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   i. Dystrybucję certyfikatów poprzez http
   ii. Konsolidację CA dla wielu lasów domeny,
   iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
s. Szyfrowanie plików i folderów.
t. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
u. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
v. Serwis udostępniania stron WWW.
w. Wsparcie dla protokołu IP w wersji 6 (IPv6),
x. Wsparcie dla algorytmów Suite B (RFC 4869),
y. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
z. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   iii. Obsługi 4-KB sektorów dysków
   iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

57. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
58. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
59. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
60. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
61. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
62. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

2.1.29. WinSvrStd ALNG LicSAPk MVL 2Proc

Licencja na serwerowy system operacyjny typ I z prawem do uaktualniania musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f. Szyfrowanie plików i folderów.
    g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i. Serwis udostępniania stron WWW.
    j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k. Wsparcie dla algorytmów Suite B (RFC 4869),
    l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
        i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
        ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
        iii. Obsługi 4-KB sektorów dysków
        iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

2.1.30. DsktpOptmztnPkforSA ALNG SubsVL MVL PerDvc forWinSA

Pakiet wspomagania zarządzania i instalacji posiadanych systemów operacyjnych Windows w wersji 7, 8 i 10 musi zawierać:

1. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
2. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
3. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
4. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
5. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
6. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
7. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
8. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
9. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
10. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
11. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
12. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
13. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
14. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek aplikacji.
15. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.

16. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
17. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym
18. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
19. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
20. Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

2.1.31. AzureMonetaryCommit ShrdSvr ALNG SubsVL MVL Commit

Platforma Infrastruktury Niezawodnościowej, która musi być osadzona na standardowej, powszechnie dostępnej poprzez sieć Internet, skalowalnej i bezpiecznej usłudze polegającej na udostępnieniu serwerowej platformy umożliwiającej przechowywanie danych i uruchamianie własnych serwerów oraz aplikacji w środowisku zwirtualizowanym.

Usługa powinna spełniać następujące wymagania:

1. Usługa musi być dostępna na zasadzie subskrypcji przez okres minimum 35 miesięcy od jej uruchomienia z możliwością dalszego przedłużenia.
2. Minimum 9831 godzin czasu obliczeniowego w ciągu miesiąca dla znormalizowanej jednostki obliczeniowej: 1 rdzeń procesora min. 1.5GHz, min. 1.5 GB pamięci operacyjnej.
3. Dostęp do przestrzeni dyskowej o sumarycznej pojemności 3,5 TB.
4. Minimum 700 GB transferu danych miesięcznie.
5. Wsparcie techniczne z gwarantowanym czasem reakcji.
6. Dostępność usługi na poziomie 99,9%.
7. Możliwość skalowania usługi.
8. Możliwość dynamicznego zwiększania i zmniejszania zasobów sprzętowych bez przestoju pracy aplikacji.
9. Wdrażanie nowych wersji aplikacji bez przestoju działających wersji.
10. Automatyczna, niewpływającą na ciągłość pracy systemu instalacja poprawek udostępnianych przez dostawcę systemu operacyjnego.
11. Możliwość gromadzenia i przetwarzania danych w udostępnianej przez platformę bazie relacyjnej, w oparciu o składnię SQL.
12. Łatwa integracja z wdrożonymi lokalnie usługami katalogowymi, zgodnie ze Specyfikacją WS-Federation.
13. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP.
14. Możliwość uruchomienia aplikacji internetowych wykorzystujących technologię ASP.NET z automatyczną dystrybucją ruchu sieciowego HTTP pomiędzy kilka pracujących serwerów.
15. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów z możliwością zdalnego dostępu.
16. Platforma ma korzystać z serwerowych systemów operacyjnych *[Windows Server i Linux / zgodnych z opisanymi w specyfikacji].*
17. Usługa powinna być bezpieczna, oferowane funkcje musi potwierdzać certyfikat zgodności z normą ISO/IEC 27001.
18. Usługa musi mieć możliwość zapewnienia bezpieczeństwa i wysokiej dostępności danych w przypadku katastrofy poprzez replikację danych między dwoma lokalizacjami oddalonymi od siebie o minimum 500 kilometrów i zachowaniu minimum dwóch replik w każdej lokalizacji.

2.1.32. DynCRMOnlnPro ShrdSvr ALNG SubsVL MVL Restricted PerUsr

Usługa pozwalająca wykorzystać hostowany system zarządzania relacjami z klientami (dalej ZRK) bez możliwości:

1. Tworzenia i aktualizowania raportów i aplikacji do analizy biznesowej w programach klienckich systemu CRM,
2. Tworzenia i aktualizowania danych wszystkich standardowych i niestandardowych obiektów poprzez programy klienckie systemu CRM,
3. Tworzenia i aktualizowania procesów biznesowych raportów i asystowanych okien dialogowych za pomocą programów klienckich systemu CRM,
4. Administrowanie systemem Microsoft Dynamics CRM i dostosowywania go.

Hostowany System Zarządzania Relacjami z Klientami musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

1. Oferowane rozwiązanie ZRK ma bazować na wbudowanych, konfigurowalnych funkcjach standardowej aplikacji klasy CRM.
2. Rozwiązanie ma umożliwić wydzielenie na jednej platformie ZRK wielu instancji obsługujących różne jednostki lub funkcje.
3. Celem implementacji systemu ZRK jest możliwość efektywnej obsługi klientów wewnętrznych i zewnętrznych oraz fizycznego wsparcia dla następujących funkcji:
   a. Stworzenie zespołu narzędzi dla struktur działu obsługi klientów, reprezentującego sprawy interesantów wobec różnych jednostek,
   b. Stworzenie zestandaryzowanych i jednolicie obsługiwanych procedur obsługi sprawy, niezależnie od sposobu jej wniesienia,
   c. Umożliwienie sprawnego przekazywania spraw do działów merytorycznych i wykonawczych z możliwością śledzenia ich statusu i raportowania wykonania niezbędnych działań,
   d. Wspomaganie sprzedaży z opisem i monitorowaniem jej etapów,
   e. Prognozowanie sprzedaży,
   f. Możliwość monitorowania statusu sprawy przez interesanta,
4. ZRK będzie wspierać obsługę kontaktów z klientami.
5. W systemie zaimplementowany będzie mechanizm tworzenia i udostępniania baz wiedzy.
6. ZRK zawierać będzie kartotekę klienta.
7. ZRK umożliwi rejestrację spraw klientów.
8. ZRK umożliwi samoobsługę w Internecie poprzez portal wielofunkcyjny.
9. W systemie zaimplementowane będą kalendarze użytkowników oraz wybranych zasobów (np. sale).
10. ZRK udostępni raportowanie statystyki obsługiwanych spraw.
11. ZRK umożliwi zaprezentowanie raportu efektywności działania na portalu wielofunkcyjny.
12. ZRK umożliwi przechowywanie dokumentów.
13. ZRK umożliwi obsługę korespondencji seryjnej.
14. ZRK umożliwi badanie satysfakcji klienta.
15. ZRK umożliwi tworzenie bazy danych klientów i ich spraw. System będzie udostępniał możliwość importowania danych klientów ad-hoc z wykorzystaniem kreatora importu oraz kreatora mapowania pliku źródłowego na strukturę danych w C
16. Docelowym rozwiązaniem jest rejestrowanie wszystkich spraw procesowanych w systemach za pośrednictwem CRM. System będzie pozwalał na wiązanie danych każdej sprawy, korespondencji, dokumentu z kartoteką klienta z jednoczesnym wskazaniem statusu sprawy, dokumentu, korespondencji.
17. Wymagana jest możliwość monitorowania poprzez CRM statusu spraw z udzielaniem informacji o jej statusie.
18. Wymagana jest możliwość wprowadzania do systemu CRM informacji o:
    a. sposobie załatwiania spraw (opis oraz implementacja procedury realizacji sprawy)
    b. kompetencjach poszczególnych jednostek czy działów
    c. danych teleadresowych
19. Wymagana jest analiza danych zawartych w CRM pod kątem wydajności i efektywności obsługi klientów
20. Wymagane jest tworzenie listy zgłoszeń priorytetowych lub przewlekłych, eskalacja spraw na poziom kierownictwa zgodnie ze zdefiniowanym przebiegiem eskalacji.

21. Wymagana jest integracja CRM z system obiegu dokumentów, archiwum elektronicznym, portalem wielofunkcyjny i systemem komunikacji wielokanałowej z wykorzystaniem Web Services lub mechanizmów osadzania zewnętrznych formularzy w interfejsie użytkownika systemu CRM (iFrame).
22. System CRM będzie wspierał szkolenie zdalne personelu poprzez budowanie zaawansowanej bazy wiedzy zintegrowanej z systemem portalowym pozwalającym przechowywać pliki procedur, webcasty oraz inne materiały w formie dostępnej dla personelu.
23. System CRM będzie umożliwiał po pierwszej migracji danych o obywatelach na segmentacje i przygotowanie selektywnego przekazu informacyjnego dostosowanego do grupy docelowej.
24. ZRK pozwoli na:
    a. Tworzenie bazy danych klientów i ich spraw,
    b. Możliwość monitorowania poprzez CRM statusu spraw klientów z udzielaniem informacji o statusie
        - przez pracownika
        - poprzez portal
    c. Możliwość wprowadzenia do systemu CRM informacji (baz wiedzy) o:
        - sposobie załatwiania spra
        - kompetencjach poszczególnych jednostek
        - danych teleadresowych
        - podłączenia do funkcji bazy wiedzy danych, artykułów, opisów zarchiwizowanych w rozwiązaniu portalowym w sposób natywny (tak, aby urzędnik nie musiał zmieniać środowiska pracy, aby uzyskać dostęp do powiązanych danych)
        - prowadzonych działaniach informacyjnych na wybranych grupach klientów.
    d. prowadzonych działaniach na wybranych grupach klientów. Procesowanie zgłoszeń/spraw w następujący sposób:
        - przejęcie i zarejestrowanie danych klienta (lub ich potwierdzenie)
        - zarejestrowanie sprawy
        - przekazanie informacji o sposobie załatwienia sprawy lub uruchomienie „ręczne" sprawy poprzez przekazanie do odpowiedniej jednostki (mail, dokument papierowy, lub poprzez końcówkę systemu)
        - informowanie o statusie sprawy
    e. Badanie poziomu satysfakcji klientów z wykorzystaniem dostępnych kanałów komunikacji – użycie systemu CRM w centrum kontaktu telefonicznego, wysłanie ankiety mailem, wykonanie ankiety podczas wizyty klienta (kontakt 1:1)
    f. Analiza danych zawartych w CRM pod kątem wydajności i efektywności obsługi klientów z poziomu systemu CRM.
        - System posiada wbudowany mechanizm analizy danych poprzez zestaw raportów dostępnych natywnie w interfejsie użytkownika systemu.
        - System będzie współpracował z platformą raportową z wykorzystaniem matrycy uprawnień użytkowników oraz profilem użytkownika dostępnym w usłudze katalogowej.
        - System będzie eksponował dane do platformy analitycznej z wykorzystaniem matrycy uprawnień użytkowników oraz profilem użytkownika dostępnym w usłudze katalogowej pozwalając na integrację danych analitycznych z innymi systemami wchodzącymi w skład Systemu.
    g. Tworzenie listy zgłoszeń priorytetowych lub przewlekłych, eskalacja spraw na wyższy poziom decyzyjny zgodnie z zdefiniowanymi procesami eskalacji.
        - System będzie implementował strukturę organizacyjną urzędu i jego jednostek organizacyjnych pozwalając na budowanie reguł podległości i zależności miedzy personelem.
        - Urzędnicy na poszczególnych poziomach organizacyjnych będą mieli dostęp do spraw realizowanych przez podległy im personel.
        - Personel będzie miał możliwość przekazania (współdzielenia) danych w systemie CRM poza ustalonymi procedurami w przypadku dłuższej nieobecności w pracy. Współdzielenie musi pozwalać na udostępnienie danych pojedynczemu pracownikowi lub zespołowi.

h. Możliwość budowania zestawów danych w CRM na podstawie, których Zamawiający będzie optymalizował obsługę swoich celów nadrzędnych. Listy będą budowane przez personel wg ich własnego uznania z założeniem zapisania i wykorzystania takiej listy w czasie późniejszym. Poniżej przykłady.
   - Lista zadań przeterminowanych lub zapadających w zdefiniowanym terminie
   - Lista kartotek klientów wymagających uzupełnienia
   - Lista korespondencji wysłanej w sprawie...

i. Integracja CRM z Systemem z wykorzystaniem Web Services lub systemu osadzania stron i formularzy w interfejsie użytkownika CRM. Integracja będzie również oferować wystawianie poszczególnych funkcji systemu CRM w systemie portalowym jak również będzie umożliwiać przepływ pracy pomiędzy ZRK i portalem wielofunkcyjny w zakresie technologii workflow.

25. Wymagana jest możliwość monitorowania poprzez CRM statusu spraw z udzielaniem informacji o jej statusie.
26. Wymagana jest analiza danych zawartych w CRM pod kątem wydajności i efektywności obsługi klientów
27. Wymagane jest tworzenie listy zgłoszeń priorytetowych lub przewlekłych, eskalacja spraw na poziom kierownictwa zgodnie ze zdefiniowanym przebiegiem eskalacji.
28. Wymagana jest integracja CRM z system obiegu dokumentów, archiwum elektronicznym, portalem wielofunkcyjny i systemem komunikacji wielokanałowej z wykorzystaniem Web Services lub mechanizmów osadzania zewnętrznych formularzy w interfejsie użytkownika systemu CRM (iFrame).
29. System CRM będzie wspierał szkolenie zdalne personelu poprzez budowanie zaawansowanej bazy wiedzy zintegrowanej z systemem portalowym pozwalającym przechowywać pliki procedur, webcasty oraz inne materiały w formie dostępnej dla personelu.
30. System CRM będzie umożliwiał po pierwszej migracji danych o klientach na segmentacje i przygotowanie selektywnego przekazu informacyjnego dostosowanego do grupy docelowej.
31. ZRK pozwoli na budowę jednolitego systemu informacyjnego dla klientów pozwalającego na uzyskanie informacji o:
    a. Informacji o sposobie i miejscu realizacji usług
    b. Ewidencji spraw z przypisaniem do klienta
    c. Liście usług świadczonych przez Zamawiającego
    d. Sposobie realizacji tych usług
    e. Działaniach i kampaniach poszczególnych komórek Zamawiającego

2.1.33. EntVoiceAddOntoECS ShrdSvr ALNG SubsVL MVL AddOn toEntCloudSte

Subskrypcja uzupełniająca do usługi opisanej w punkcie 2.1.10 pozwalająca dodatkowo wykorzystać funkcjonalność serwera komunikacji wielokanałowej w zakresie:

- Łączności głosowej i video z wieloma (więcej niż dwoma) uczestnikami konferencji,
- Zarządzania połączeniami telefonicznymi i głosowymi
- Współdzielenia aplikacji.

2.1.34. PowerBI ShrdSvr ALNG SubsVL MVL PerUsr forSPOP2/E3/E4

System analizy danych musi być oparty na usługach obliczeniowych świadczonych z użyciem chmury publicznej spełniającej wymogi polskiego prawa. Opublikowane raporty i analizy powinny wykorzystywać moc obliczeniową chmury publicznej i w minimalnym stopniu obciążać komputery użytkowników końcowych.

1. System musi umożliwiać użytkownikom:
   a. Import i łączenie danych z wielu różnych systemów źródłowych
   b. Ładowanie danych do jednego spójnego modelu danych
   c. Wzbogacanie modelu danych o dodatkowe pola obliczeniowe
   d. Tworzenie raportów i wizualizacji danych w postaci tabel i wykresów przestawnych, interaktywnych raportów z możliwością dynamicznego i kontekstowego filtrowania danych,
   e. Tworzenie animowanych wykresów pozwalających na śledzenie zmian i trendów w czasie,

f. Tworzenie wizualizacji z użyciem interaktywnych map geograficznych z nałożonymi warstwami analitycznymi (mapy powinni być wizualizowane w 2D oraz 3D z możliwością drążenia i powiększania w dowolnie wybranym punkcie mapy),
g. Tworzenie animowanych filmów prezentujących dane analityczne nałożone na na mapie geograficznej z możliwością dodawania do animacji komentarzy, opisów, wykresów oraz zdjęć,
h. Wszystkie wyżej wymienione funkcje muszą być dostępne z poziomu jednej aplikacji raportowej z graficznym interfejsem użytkownika, bez konieczności dodatkowego programowania.

2. W celu zwiększenia wydajności przetwarzania system musi posiadać wbudowany mechanizm przetwarzania danych in-memory (w pamięci RAM komputera) oraz mechanizm kolumnowej kompresji danych. Wymienione mechanizmy in-memory muszą działać zarówno po stronie serwerowej (po opublikowaniu raportów na serwerze i udostępnieniu przez przeglądarkę WWW), jak również w narzędziu raportowym na komputerze użytkownika (podczas przygotowywania modeli danych i raportów).
3. Narzędzie raportowe musi umożliwiać użytkownikowi pobieranie i łączenie danych z wielu źródeł w jednym modelu semantycznym. Proces pobierania danych w narzędziu raportowym musi umożliwiać użytkownikowi przekształcenie danych wejściowych i dostosowanie ich do postaci wymaganej w modelu semantycznym i raportach. Narzędzie raportowe musi mieć wbudowane gotowe funkcje i graficzne kreatory transformacji danych pozwalające na:
   i. Usuwanie i kopiowanie kolumn wejściowych
   j. Filtrowanie wierszy wejściowych na podstawie wartości z wybranych kolumn
   k. Łączenie i rozdzielanie wartości w kolumnach (na podstawie wskazanego znaku separatora lub określonej liczby znaków)
   l. Konwersję typów danych (tekstowy, liczbowy, daty)
   m. Automatyczną zamianę wielkości liter w danych wejściowych
   n. Automatyczne usuwanie duplikatów wartości we wskazanej kolumnie
   o. Automatyczne zastępowanie wartości w kolumnach inną wskazaną przez użytkownika
   p. Automatyczną konwersję danych z formatu JSON
   q. Automatyczne wyliczanie agregacji (grupowanie danych według danej kolumny)
   r. Automatyczne wykonywanie operacji przekształcenia wierszy w kolumny i kolumn w wiersze (pivot/unpivot)
   s. Automatyczne łączenie wielu tabel o takiej samej strukturze kolumn w jedną tabelę (UNION)
   t. Automatyczne złączenie dwóch różnych tabel w jedną na podstawie wskazanych wspólnych kolumn dla obu tabel (kluczy złączenia)
4. Zastosowane przez użytkownika transformacje danych (zapytanie) muszą być pamiętane w narzędziu, jako sekwencja kolejno następujących po sobie czynności (etapów). Użytkownik musi mieć możliwość przejścia do dowolnego z kroków procesu transformacji danych i obejrzenia danych sprzed zastosowania danego kroku.
5. Zdefiniowane kroki transformacji danych powinny być zapamiętywane w postaci automatycznie generowanego skryptu, który zaawansowani użytkownicy mogą modyfikować i powielać.
6. System musi udostępniać funkcję katalogu zapytań, w którym autorzy zapytań (transformacji danych) udostępniają efekty swojej pracy dla innych użytkowników. Użytkownicy katalogu zapytań, z poziomu narzędzia raportowego, muszą mieć możliwość wyszukania i wykorzystania interesującego ich zapytania na potrzeby zasilania danymi własnych analiz i raportów. W katalogu zapytań musi istnieć:
   g. Możliwość nadawania uprawnień dostępu do zapytania dla poszczególnych użytkowników lub grup użytkowników
   h. Możliwość podglądu w wyszukiwarce zapytań wyniku zwracanego przez określone zapytanie (zanim jeszcze wynik zapytania zostanie załadowany do narzędzia raportowego i modelu danych).
   i. Możliwość wprowadzenia nazwy i opisu biznesowego określonego zapytania w celu łatwiejszego wyszukiwania
   j. Możliwość dołączenia adresu URL do dokumentacji opisującej zawartość merytoryczną zapytania i wyników, które ono zwraca
   k. Dostęp do statystyk i monitoringu częstości wyszukiwania i wykorzystania przez użytkowników opublikowanych zapytań.
7. Narzędzie raportowe musi mieć wbudowane sterowniki do pobierania danych, co najmniej z następujących źródeł: pliki tekstowe, pliki CSV, pliki XML, pliki Excel, strony internetowe (podając adres

URL takiej strony), bazy relacyjne (Microsoft SQL Server, Oracle, IBM DB2, MySQL, PostgreSQL, Sybase, Teradata), listy Sharepoint, Facebook, Active Directory, SAP Business Objects, Microsoft Azure, OData Feed, klastry Hadoop, ODBC. Dodatkowo system musi umożliwiać bezpośrednio w narzędziu raportowym wyszukiwanie i importowanie zbiorów danych dostępnych w internecie (wyszukiwanie na podstawie słów kluczowych i zwrotów podawanych przez użytkownika).

8. System musi umożliwiać dostęp do danych oraz wykonywanie analiz z wykorzystaniem zapytań w języku naturalnym. Użytkownik musi mieć możliwość wpisywania pytania w języku naturalnym bezpośrednio na portalu, a jako odpowiedź system powinien zwracać wyniki w formie tabel, wykresów lub map geograficznych. Sposób wizualizacji danych powinien być automatycznie dobierany przez system w celu optymalnej i czytelnej prezentacji wyników (np. w przypadku zapytań o dane związane z położeniem geograficznym system powinien automatycznie prezentować wyniki nałożone na mapie geograficznej). Jednocześnie użytkownik musi mieć możliwość dalszej zmiany sposobu wizualizacji otrzymanych wyników tak, aby dostosować je do własnych preferencji (np. zamiana danych prezentowanych w formie mapy geograficznej na tabelę, wykres kołowy, liniowy itp) . Użytkownik musi mieć możliwość wyboru modelu danych, w kontekście którego uruchamiane są zapytania w języku naturalnym.
9. System musi zapewniać użytkownikom możliwość umieszczenia/przypięcia na portalu często wykorzystywanych zapytań zdefiniowanych w języku naturalnym. Musi istnieć możliwość umieszczania tych zapytań w postaci graficznego interfejsu obiektowego, tzn. pod każdym obiektem graficznym powinno być podpięte pytanie, które po kliknięciu na dany obiekt jest automatycznie uruchamiane, a jego wyniki prezentowane są w oknie przeglądarki w formie interaktywnego raportu. Użytkownik (bezpośrednio w przeglądarce) musi mieć możliwość wprowadzenia zmiany koloru obiektów graficznych, dodania na obiektach własnej grafiki (np. poprzez wstawienie źródłowego adresu URL do grafiki dostępnej w sieci) oraz zmiany rozmiaru obiektów.
10. System musi umożliwiać publikację modeli danych oraz raportów bezpośrednio na portalu. Po udostępnieniu raportu na portalu dla użytkowników powinny być dostępne takie informacje, jak: tytuł raportu, data i czas opublikowania raportu, nazwa użytkownika publikującego raport oraz graficzny podgląd zawartości raportu.
11. Użytkownicy muszą mieć możliwość wyboru i oznaczenia wybranych raportów, jako swoich ulubionych. Ulubione raporty użytkownika są automatycznie oznaczane gwiazdką, a jednocześnie prezentowane w osobnej części portalu, dedykowanej do prezentacji jedynie ulubionych raportów bieżącego użytkownika.
12. System musi udostępniać dedykowany język do tworzenia logiki biznesowej w modelu semantycznym. Język ten musi m.in. obsługiwać relacje utworzone między tabelami, mechanizmy operacji na datach i okresach (time intelligence), agregacje danych, wyrażenia warunkowe, hierarchie, filtrowanie danych, funkcje matematyczne i statystyczne. Narzędzia muszą mieć wbudowany mechanizm podpowiadania składni wyrażeń i funkcji w tym języku.
13. System musi umożliwiać automatyczną synchronizację i odświeżanie opublikowanych raportów, zarówno zasilanych ze źródeł internetowych (w tym z chmury publicznej), jak również ze źródeł i baz danych przechowywanych we własnym centrum przetwarzania danych.
14. System musi udostępniać aplikację dedykowaną dla urządzeń mobilnych przystosowaną do prezentacji raportów z użyciem interfejsu dotykowego.
15. Raporty oznaczone, jako ulubione na portalu raportowym powinny być również prezentowane w sekcji raportów ulubionych w aplikacji.