**Załącznik nr 1 do SIWZ**

 **OPIS PRZEDMIOTU ZAMÓWIENIA**

**Nazwa nadana zamówieniu: Dostawa subskrypcji oprogramowania dla UJK w Kielcach**

**Przedmiotem zamówienia jest Dostawa subskrypcji oprogramowania w ramach trzyletniej umowy subskrypcyjnej (EES) dla pracowników i studentów Uniwersytetu Jana Kochanowskiego w Kielcach tj:**

**I. Microsoft M365 Edu A3 Shared ALNG sub MVL PU lub produkt równoważny zawierający subskrypcje licencji: systemu operacyjnego, pakietu biurowego, usługi zarządzania urządzeniami i tożsamością użytkowników, spełniające następujące wymagania - 1342 szt.**

1. Interfejs graficzny całości oprogramowania dla użytkownika pozwalający na obsługę:

a. klasyczną przy pomocy klawiatury i myszy,

b. dotykową umożliwiającą 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. Wbudowany system pomocy w języku polskim.

4. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.

5. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne.

6. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizmów zarządzany przez administratora systemu Zamawiającego.

7. Wbudowana zapora Internetowa (firewall) dla ochrony połączeń internetowych.

8. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.

9. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.

10. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.

11. Możliwość zarządzania stacją roboczą poprzez polityki grupowe - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji i dla wskazanych aplikacji.

12. Rozbudowane, definiowalne polityki bezpieczeństwa - polityki dla systemu operacyjnego.

13. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.

14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.

15. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.

16. 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.

17. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); Wsparcie dla IPSEC oparte na politykach - wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.

18. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; Mechanizmy uwierzytelniania w oparciu o:

a. login i hasło,

b. karty z certyfikatami (smartcard),

c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

d. wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.

19. Mechanizmy wieloskładnikowego uwierzytelniania. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5, Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, Wsparcie dla algorytmów Suite B (RFC 4869).

20. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji.

21. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny, (OMA) Device

Management (DM) protocol 2.0.

22. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji.

23. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i

funkcji systemu.

24. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.

25. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.

26. Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

27. Wsparcie dla JScript i VBScript - możliwość uruchamiania interpretera poleceń.

28. Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

29. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning).

30. 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.

31. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.

32. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.

33. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).

34. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.

35. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.

36. 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.

37. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.

38. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

39. Możliwość Instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

40. 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.

41. 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 wparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTIP i SMB.

42. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tych polityk.

43. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC.

44. Mechanizm umożliwiający naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.

45. 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.

46. Pakiet biurowy musi być w pełni kompatybilny (bez konieczności dodatkowego instalowania i używania konwerterów, edytorów, nakładek, itd.) z posiadaną przez Zamawiającego usługą MS Office 365 on-line.

47. Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

a. dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie właściwe ponad 2GB przestrzeni adresowej.

48. 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.

49. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.

50. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych. 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 aktualnymi przepisami prawa w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,

c. umożliwia kreowanie plików w formacie XML.

51. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.

52. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).

53. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.

54. Pakiet zintegrowanych aplikacji biurowych musi zawierać:

a. edytor tekstów,

b. arkusz kalkulacyjny,

c. narzędzie do przygotowywania i prowadzenia prezentacji,

d. narzędzie do tworzenia drukowanych materiałów informacyjnych,

e. narzędzie do tworzenia i pracy z lokalną bazą danych,

f. narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),

g. narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR,

h. narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.

55. Subskrypcja pakietu usług zarządzania urządzeniami oraz tożsamością użytkowników musi spełniać następujące wymagania:

a. pakiet aplikacji biurowych dostępny w wersji instalowanej klasycznych aplikacji dostępny dla pięciu urządzeń pojedynczego użytkownika (5 komputerów PC oraz 5 urządzeń mobilnych),

b. poczta e-mail ze skrzynką pocztową o pojemności min. 100 GB,

c. nieograniczony osobisty magazyn w chmurze,

d. zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy,

e. zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),

f. stałe modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane ISO 27017 i 27018,

g. dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO,

h. możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,

i. możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,

j. dostępność mechanizmów monitorowania zachowania użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych,

k. możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej,

l. możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory,

m. dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione",

n. dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,

o. możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),

p. mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.

56. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.

57. Gwarancja braku dostępu do danych Zamawiającego, przetwarzanych w ramach pakietu usług, z wyłączeniem działań serwisowych wymagających każdorazowo zgody Zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

58. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów 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 ustalonych polityk i procedur).

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

a. integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy,

b. wykorzystanie bazy użytkowników znajdujących się w Active Directory,

c. inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,

d. inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji: nazwa urządzenia, identyfikator urządzenia, nazwa platformy systemu operacyjnego, wersja oprogramowania układowego, typ procesora, model urządzenia, producent urządzenia, lista aplikacji zainstalowanych w ramach przedsiębiorstwa.

60. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych.

61. Usługa ma umożliwiać dystrybucji oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji.

62. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).

63. Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji.

64. System i pakiet aplikacji musi być w pełni kompatybilny z wdrożonymi i użytkowanymi przez Zamawiającego aplikacjami zainstalowanymi i użytkowanymi na współpracujących zasobach: Simple.ERP, Uczelnia.XP firmy PCG Academia, ALEPH, Płatnik firmy Asseco Poland, Systemy Informacji Prawnej Legalis/LEX, System Elektronicznej Legitymacji Studenckiej firmy Opteam S.A. W przypadku zaoferowania systemu równoważnego oferent winien skonfigurować każdy z komputerów do pracy z wszystkimi wyżej wymienionymi programami oraz w okresie gwarancji zapewnić wsparcie przy konfiguracji w przypadku aktualizacji wszystkich wyżej wymienionych programów.

65. System musi umożliwiać hosting spotkań dla ok. 10000 osób dla aplikacji Skype.

66. System planowania spotkań z wykładowcami przy użyciu usługi MS Booking lub równoważnej z jej wszystkimi właściwościami.

67. Udostępnienie w subskrypcji Profesjonalnych Grup Learningowych.

**II. Windows Server STD Core ALNG Lic SAP k MVL 2 CoreLic – 40 szt. lub równoważny spełniający następujące wymagania:**

1. System musi być w pełni kompatybilny z wdrożonymi i użytkowanymi przez Zamawiającego aplikacjami zainstalowanymi i użytkowanymi na współpracujących zasobach: Simple.ERP, Uczelnia.XP firmy PCG Academia, ALEPH, Płatnik firmy Asseco Poland, Systemy Informacji Prawnej Legalis/LEX, System Elektronicznej Legitymacji Studenckiej firmy Opteam S.A. W przypadku zaoferowania systemu równoważnego oferent winien skonfigurować każdy z komputerów do pracy z wszystkimi wyżej wymienionymi programami oraz w okresie gwarancji zapewnić wsparcie przy konfiguracji w przypadku aktualizacji wszystkich wyżej wymienionych programów.

2. Systemy muszą, bez potrzeby dodatkowej edycji, formatowania, konwertowania i modyfikowania przejąć role kontrolerów domeny usługi Microsoft Active Directory (GroupPolicy, DNS, DHCP, centrum certyfikacji);

a. umożliwić zarządzanie kontami użytkowników komputerów zaimportowanych z infrastruktury Zamawiającego;

b. pozwolić na uruchomienie oprogramowania Azure AD Connect niezbędnego do synchronizacji z wdrożoną usługą Microsoft Office365;

c. pozwolić na uruchomienie hybrydowej konfiguracji Microsoft Exchange 2013;

d. pozwolić na uruchomienie oprogramowania Windows Server Update Service (WSUS) niezbędnej do aktualizacji systemów operacyjnych;

e. pozwolić na uruchomienie oprogramowania Microsoft System Center Configuration Manager (SCCM);

3. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4TB pamięci RAM w środowisku fizycznym.

4. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

5. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

6. 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.

7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

8. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

9. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego .

10. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

11. 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 (AGL).

12. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

13. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

14. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

15. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

16. Wbudowana zapora sieciowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

17. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

18. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

19. Możliwość zmiany języka interfejsu po zainstalowani u systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

20. 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).

21. 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.

22. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 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:

b.1. podłączenie do domeny w trybie offline - bez dostępnego połączenia sieciowego z domeną,

b.2. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania,

b.3. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

b.4. bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows.

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:

e.1. dystrybucję certyfikatów poprzez http,

e.2. konsolidację CA dla wielu lasów domeny,

e.3. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

e.4. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

e.5. szyfrowanie plików i folderów,

e.6. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami stacjami roboczymi (IPSec).

f. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

g. serwis udostępniania stron WWW.

h. wsparcie dla protokołu IP w wersji 6 (1Pv6).

i. wsparcie dla algorytmów Suite B (RFC 4869).

j. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

k. 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:

k.1. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

k.2. obsługi ramek typu jumbo frames dla maszyn wirtualnych,

k.3. obsługi 4-KB sektorów dysków,

k.4. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra.

k.5. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,

k.6. 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.