Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

OPIS PRZEDMIOTU ZAMÓWIENIA

KONTYNUACJA UMOWY EES ZAWIERAJACEJ USŁUGI MICROSOFT OFFICE365 DLA NAUCZYCIELI AKADEMICKICH WRAZ Z BENAFITOWĄ LICENCJĄ DLA STUDENTÓW, DOKTORANTÓW I SŁUCHACZY UKSW ORAZ Z PAKIETEM BIUROWYM MICROSOFT OFFICE

Ryszard Stasiak, Joanna Antkowiak

Spis treści

1. Wymagania w zakresie dostaw i usług 2

1.1. Specyfikacja ilościowa zamówienia: 2

1.2. Wymagania szczegółowe w zakresie dostaw i usług 2

1.3. Warunki równoważności dla produktów równoważnych - szczegółowa specyfikacja techniczno–eksploatacyjna i cech użytkowych oprogramowania 4

1.3.1. Subskrypcja usług komunikacyjnych, bezpieczeństwa i pakietu biurowego klasy desktop typ I (subskrypcja na użytkownika) (Subskrypcja pakietu M365 EDU A3 Unified ShrdSvr ALNG SubsVL MVL PerUsr (P/N: AAD-38391)) 4

1.3.2. Subskrypcja usług komunikacyjnych, bezpieczeństwa i pakietu biurowego klasy desktop typ II (subskrypcja na użytkownika) (Subskrypcja pakietu M365 EDU A3 Unified ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft (P/N: AAD-38397)) 26

1. Wymagania w zakresie dostaw i usług

Przedmiotem zamówienia jest dostawa subskrypcji oprogramowania biurowego na potrzeby pracowników, studentów i doktorantów wraz z pakietem usług chmurowych (dalej łącznie nazywanych Produktami).
Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off the-shelf - COTS).
Zamawiający wymaga dostawy Produktów na warunkach przewidzianych przez producenta oprogramowania ,dla jednostek edukacyjnych.
Wykonawca powinien posiadać status partnera producenta Oprogramowania z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał status partnera Microsoft LSP (Microsoft Licensing Solution Provider).
Okres realizacji zamówienia to 36 miesięcy. Dniem udostępnienia usługi jest czas do 10 doby od podpisania umowy. W tym czasie Zamawiający zachowuje prawo do aktualizacji ilości zamawianych licencji.
W przypadku zaoferowania produktu równoważnego, Wykonawca zobowiązany jest w ramach wynagrodzenia umownego, do przeprowadzenia szkolenia z obsługi, administracji i zabezpieczania zaoferowanego produktu dla pracowników zamawiającego w wymiarze nie mniejszym niż 5 dni szkoleniowych po 8 godzin w dni robocze w godzinach 7:30-15:30.
W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca zobowiązany jest także do przeprowadzenia migracji użytkowników wraz z przypisywanymi do nich zasobami (pliki, skrzynki pocztowe, zespoły, grupy) z usług Wykorzystywanych przez Zamawiającego opisanych w punkcie 2 OPZ, w terminie nieprzekraczalnym do dnia 31 stycznia 2024 r. w sposób umożliwiający użytkownikom Zamawiającego, bezprzerwowe korzystanie z usług w trakcie migracji.

1.1. Specyfikacja ilościowa zamówienia:

Numer produktu	**Okres**	**Ilość**
Subskrypcja pakietu M365 EDU A3 Unified ShrdSvr ALNG SubsVL MVL PerUsr (P/N: AAD-38391), lub produkt równoważny	36 miesięcy	1 492 szt.
Subskrypcja pakietu M365 EDU A3 Unified ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft (P/N: AAD-38397) lub produkt równoważny	36 miesięcy	59 680 szt.

1.2. Wymagania szczegółowe w zakresie dostaw i usług

1.2.1 Zamawiający wymaga od Wykonawcy dedykowania do obsługi umowy co najmniej 2 osób, posiadających wiedzę, potwierdzoną egzaminem z zakresu pól eksploatacji Produktów.
1.2.2 Warunki użytkowania oprogramowania muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi lub serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu).
1.2.3 Oferowane produkty i usługi. muszą zapewniać posiadanie powszechnie uznanych i rozpowszechnionych standardów i normatywów potwierdzonych aktualnymi wynikami niezależnych audytów, w szczególności:

1) ISO 27001, ISO 27002, ISO 27017, ISO 27018 lub równoważne

2) SOC 1, SOC 2 lub równoważne
3) Open Authentication Standard – OAuth lub równoważne

1.2.4 Oferowane subskrypcje usług hostowanych muszą zapewniać:

1) Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym), w trybie 24/7,
2) Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.
3) 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 lub równoważnymi.
4) Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
5) Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
6) Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
7) Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single signon) na bazie własnej usługi katalogowej Active Directory.
8) Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
9) 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".
10) Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN)
11) Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
12) Przynajmniej dwa niezależne od siebie, równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 150 km,
13) Zapisy umowne zawierające tzw. Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych,
14) Zobowiązania umowne potwierdzające zgodność z rozporządzeniem RODO i potwierdzające rolę operatora usługi jako współprzetwarzającego dane,
15) Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
16) Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
17) Gwarancję usunięcia danych Zamawiającego z Platformy po zakończeniu umowy.
18) Gwarancję braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy.

5. Dostarczane subskrypcje oprogramowania będące przedmiotem niniejszego zamówienia, muszą gwarantować prawo instalacji najnowszej wersji oprogramowania, dostępnych w trakcie trwania umowy.
6. Oprogramowanie musi pozwalać na udzielenie licencji oprogramowania dla jednostek stowarzyszonych.
7. Zamawiający dopuszcza oferowanie Produktów o szerszej niż opisana funkcjonalności.
8. 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, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej.
9. W związku z możliwością zwiększenia liczby użytkowników systemów w trakcie trwania umowy,

Zamawiający wymaga zaoferowania licencjonowania gwarantowanego przez Producenta Produktów, umożliwiającego w okresie trwania umowy instalację dodatkowych licencji (w ramach prawa opcji) z zamawianego zakresu Produktów z rozliczaniem się post factum.

10. Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym osobom ze strony Zamawiającego na:

    a. Pobieranie zakupionego oprogramowania,
    b. Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,
    c. Sprawdzanie liczby zakupionych Produktów w wykazie zakupionych Produktów.

11. Zamawiający wymaga udzielenia uprawnień na stronie Producenta oraz dostępu do kluczy licencyjnych w terminie do 10 dni od podpisania umowy.
12. Po dziewięćdziesięciu (90) dniach od zakończenia okresu trwania umowy Wykonawca zapewni możliwość wyłączenia konta Zamawiającego na spersonalizowanej stronie Producenta i usunięcie jego danych.
13. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
14. Jeżeli nowa wersja Produktu zawierać będzie bardziej restrykcyjne prawa do używania 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.

1.3. Warunki równoważności dla produktów równoważnych - szczegółowa specyfikacja techniczno–eksploatacyjna i cech użytkowych oprogramowania

W poniżej części przedstawione są wymagania funkcjonalne dotyczące zamawianego oprogramowania i usług.
Z uwagi na to, że ustawa prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę, jako tego, kto jest zobowiązany wykazać, że oferowane rozwiązania i produkty spełniają wymagania postawione przez Zamawiającego, Wykonawca zobowiązany jest udowodnić w ofercie, że oferowane przez niego dostawy oraz normy równoważne do wskazanych w OPZ spełniają wymagania określone przez Zamawiającego.

Zamawiający zastrzega sobie, na etapie realizacji umowy, 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 z dołączeniem do usługi katalogowej Zamawiającego – Active Directory.

W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby zamawiającego 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 z oferowanymi.
Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty.

1.3.1. Subskrypcja usług komunikacyjnych, bezpieczeństwa i pakietu biurowego klasy desktop typ I (subskrypcja na użytkownika) (Subskrypcja pakietu M365 EDU A3 Unified ShrdSvr ALNG SubsVL MVL PerUsr (P/N: AAD-38391))

1.3.1.1. Subskrypcja usługi hostowanej

Subskrypcja powszechnie dostępnej, standardowej usługi hostowanej (on-line) typu COTS (Commercial Of The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi katalogowej typu LDAP, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, usług bezpieczeństwa, usług analizy danych, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi). Ponadto musi zawierać subskrypcję pakietu biurowego. Wymagania dotyczące usługi hostowanej:

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę LDAP.
2. Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. Możliwość dodawania do 500 własnych nazw domenowych do usługi LDAP.
4. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
5. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
6. Ochrona danych w systemie poczty elektronicznej przed złośliwym oprogramowaniem i wirusami oraz atakami typu zero-day.
7. W okresie obowiązywania subskrypcji Usługa będzie przechowywać dane i umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu subskrypcji, w przypadku podjęcia decyzji o baraku jej kontynuacji, Usługa będzie przechowywać dane Zamawiającego, które zostały w niej zapisane, na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia subskrypcji w celu umożliwienia ich odzyskania. Po upływie tego 90-dniowego okresu przechowywania konto związane z subskrypcją Usługi zostanie wyłączone a dane Zamawiającego zostaną usunięte.
8. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows, Mac OS , iOS oraz Android
9. Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego jednocześnie na 5 komputerach PC lub Mac, 5 tabletach (iPad, z systemem Windows lub Android) oraz 5 telefonach.
10. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
11. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych przez Zamawiającego w Usłudze jako własność Zamawiającego.
12. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
13. Usługa musi odpowiadać wymaganiom prawa Europejskiego w zakresie ochrony danych osobowych w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych.
14. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
15. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji w terminie 90 dni.
16. Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:
    - 16.1. Usługa musi umożliwiać:
        - 16.1.1. Obsługę poczty elektronicznej.
        - 16.1.2. Zarządzanie czasem (kalendarz).
        - 16.1.3. Zarządzania zasobami.
        - 16.1.4. Zarządzanie kontaktami i komunikacją.
    - 16.2. Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:

16.2.1. Zarządzania użytkownikami poczty.
16.2.2. Wsparcia migracji z innych systemów poczty.
16.2.3. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych.
16.2.4. Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty.

17. Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:
    17.1. Posiadanego oprogramowania Outlook (2016 i nowsze).
    17.2. Przeglądarki (Web Access).
    17.3. Urządzeń mobilnych.
18. Wymagane cechy usługi to:
    18.1. Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 100 GB.
    18.2. Standardowy i łatwy sposób obsługi poczty elektronicznej.
19. Obsługa najnowszych funkcji Outlook 2016 i nowszego wykorzystywanego przez Zamawiającego, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Microsoft Edge, Apple Safari i Mozilla Firefox, Google Chrome, Opera.
20. 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.
21. Możliwość dostosowania strony logowania do usługi do potrzeb Zamawiającego.
22. Bezpieczny dostęp z każdego miejsca z wykorzystaniem protokołu HTTPS.

1.3.1.2. Usługa poczty elektronicznej

Wymagania dotyczące usługi poczty elektronicznej:

1. Funkcjonalność podstawowa:

    1.1 Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.
    1.2. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
    1.3. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
    1.4. 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.
    1.5. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.

2. Funkcjonalność wspierająca pracę grupową:

    2.1 Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości.
    2.2 Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
    2.3 Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.
    2.4 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.

2.5 Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania.
2.6 Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.
2.7 Obsługa list i grup dystrybucyjnych.
2.8 Dostęp ze skrzynki do poczty elektronicznej i wiadomości błyskawicznych.
2.9 Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.
2.10 Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
2.11 Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
2.12 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.
2.13 Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie ustalenie priorytetów wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
2.14 Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
2.15 Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów.
2.16 Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.

3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:

3.1 Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym czasie, archiwizacja.
3.2 Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.
3.3 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.
3.4 Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.
3.5 Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.
3.6 Możliwość wyszukiwania/filtrowania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanego filtrowania przez osoby odpowiedzialne za zgodność z uregulowaniami.
3.7 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.
3.8 Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
3.9 Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.

3.10 Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.

4. Wsparcie dla użytkowników mobilnych:

4.1. 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.
4.2. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.).
4.3. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych.
4.4. 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.
4.5. 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.
5. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Microsoft Edge, Apple Safari i Mozilla Firefox.

1.3.1.3. Usługa repozytorium dokumentów

1. Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 1TB dla każdego użytkownika. Repozytorium musi umożliwiać użytkownikom pakietów biurowych na:
   1.1. Traktowanie go jako własnego dysku użytkownika.
   1.2. Synchronizację zawartości wybranego folderu ze stacji roboczej do repozytorium przypisanego danemu użytkownikowi na bazie niezaprzeczalnego uwierzytelnienia.
   1.3. Synchronizację zawartości repozytorium z wieloma urządzeniami w ramach uprawnień użytkownika –właściciela repozytorium.

1.3.1.4. Usługa portalu on-line - funkcjonalności

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.
14. Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio jako wbudowane właściwości produktu:
    14.1. Interfejs użytkownika:
        14.1.1. 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).
        14.1.2. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0.
        14.1.3. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów.
        14.1.4. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego.
        14.1.5. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
    14.2. Projektowanie stron:
        14.2.1. Wbudowane intuicyjne narzędzia projektowania wyglądu stron.
        14.2.2. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML.
        14.2.3. Wsparcie dla ASP.NET, Apache, C#, Java i PHP.
        14.2.4. Możliwość osadzania elementów iFrame w polach HTML na stronie.
    14.3. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
        14.3.1. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili.
        14.3.2. 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.
        14.3.3. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili.
        14.3.4. 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.
        14.3.5. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services.
        14.3.6. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.
        14.3.7. Wbudowane samoobsługowe narzędzia wyszukiwania, analizy i wizualizacji danych Typu BI wraz z raportowaniem.

1.3.1.5. Usługa portalu on-line – udostępnienie komponentów pakietu biurowego

Usługa portalu on-line musi mieć wbudowaną funkcjonalność Udostępniania użytkownikom komponentów pakietu Biurowego on-line dostępnego przez przeglądarkę:

1. Pakiet biurowy on-line musi spełniać następujące wymagania:

1.1. Wymagania dotyczące interfejsu użytkownika:

1.1.1. Pełna polska wersja językowa interfejsu użytkownika.

1.1.2. 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:

2.1. Posiada kompletny i publicznie dostępny opis formatu.

2.2. Ma zdefiniowany układ informacji w postaci XML zgodnie z załącznikiem nr 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. (tj. Dz.U. 2017, poz. 2247) w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

3. Pakiet biurowy on-line musi zawierać:

3.1. Edytor tekstów.

3.2. Arkusz kalkulacyjny.

3.3. Narzędzie do przygotowywania i prowadzenia prezentacji.

3.4. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.

4. Edytor tekstów musi umożliwiać:

4.1. 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.

4.2 Wstawianie oraz formatowanie tabel.

4.3 Wstawianie oraz formatowanie obiektów graficznych.

4.4 Wstawianie wykresów i tabel z arkusza kalkulacyjnego.

4.5 Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.

4.6 Automatyczne tworzenie spisów treści.

4.7 Formatowanie nagłówków i stopek stron.

4.8 Sprawdzanie pisowni w języku polskim.

4.9 Śledzenie zmian wprowadzonych przez użytkowników.

4.10 Określenie układu strony (pionowa/pozioma).

4.11 Wydruk dokumentów.

4.12 Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2013 i nowszym z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu.

4.13 Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

5. Arkusz kalkulacyjny musi umożliwiać:

5.1. Tworzenie raportów tabelarycznych.

5.2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.

5.3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

5.4. Wyszukiwanie i zamianę danych.

5.5. Wykonywanie analiz danych przy użyciu formatowania warunkowego.

5.6. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.

5.7. Formatowanie czasu, daty i wartości finansowych z polskim formatem.

5.8. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

5.9. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2013 i nowszych wykorzystywanych przez Zamawiającego, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

5.10. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

6. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

6.1. Przygotowywanie prezentacji multimedialnych, które będą:

6.1.1. Prezentowanie przy użyciu projektora multimedialnego.

6.1.2. Drukowanie w formacie umożliwiającym robienie notatek.

6.1.3. Zapisanie jako prezentacja tylko do odczytu.

6.1.4. Nagrywanie narracji i dołączanie jej do prezentacji.

6.1.5. Opatrywanie slajdów notatkami dla prezentera.

6.1.6. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.

6.1.7. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.

6.1.8. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.

6.1.9. Możliwość tworzenia animacji obiektów i całych slajdów.

6.1.10. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.

6.1.11. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2013 i nowszym wykorzystywanego przez Zamawiającego.

1.3.1.6. Usługa komunikacji wielokanałowej On-Line (SKW)

Wymagania dotyczące usługi SKW:
Usługa serwera komunikacji wielokanałowej on-line ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1. Bezpieczną komunikację głosową oraz video,
2. Przesyłanie wiadomości błyskawicznych (tekstowych),
3. Możliwość organizowania telekonferencji,
4. Możliwość współdzielenia dokumentów w trakcie spotkań on-line (zdalnych).

5. W połączeniu z funkcjami aplikacji klienckich usługa ma zapewnić uprawnionym użytkownikom:

5.1. Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.

5.2. Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub Internet.

5.3. Możliwość oceny jakości komunikacji głosowej i wideo.

5.4. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.

5.5. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką SKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub

specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory.

5.6. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.

5.7. Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.

5.8. Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.

5.9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.

5.10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.

5.11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).

5.12. Możliwość nagrywania telekonferencji przez uczestników.

5.13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.

5.14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.

5.15. Wbudowane funkcjonalności: SIP Proxy.

5.16. Wbudowana funkcjonalność mostka konferencyjnego MCU.

5.17. Obsługa standardów: CSTA, TLS, SIP over TCP, NDI.

5.18. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów.

5.19. Kodowanie video H.264.

5.20. Wsparcie dla adresacji IPv4 i IPv6.

5.21. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności.

5.22. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników.

5.23. Możliwość szyfrowania połączeń.

5.24. Możliwość tworzenia zespołów i przydzielania zadań.

6. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników spoza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:

6.1. Dołączania do telekonferencji.

6.2. Szczegółowej listy uczestników.

6.3. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.

6.4. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.

6.5. Dostępu do udostępnianych plików.

6.6. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji.

7. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:

7.1. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.

7.2. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień.

8. Wsparcia telekonferencji:

8.1. Dołączania do telekonferencji.

8.2. Szczegółowej listy uczestników.

8.3. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
8.4. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
8.5. Głosowania.
8.6. Udostępniania plików i pulpitów.
8.7. Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji.
8.8. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
8.9. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

9. Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/Internet oraz usługą katalogową Active Directory.
10. Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów:
    10.1. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
    10.2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
11. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
    11.1. Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu.
    11.2. Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
    11.3. Możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

1.3.1.7. Usługi bezpieczeństwa

Usługi bezpieczeństwa wbudowane w produkt muszą pozwalać na:

1. Zarządzanie prawami dostępu do dokumentów i poczty elektronicznej tworzonych w Usłudze poprzez ich szyfrowanie i nadawanie praw odczytu, edycji, wydruku dla konkretnych użytkowników Usługi lub grup użytkowników Usługi.
2. Wykrywanie słów kluczowych w przesyłanych wiadomościach i sygnalizowanie potencjalnego wycieku informacji.
3. Możliwość ograniczania przedziału czasowego uprawnionego dostępu użytkowników do informacji.
4. Możliwość stosowania wymogu wieloskładnikowego uwierzytelniania.
5. Możliwość kontroli przepływu danych w ramach usługi repozytorium dokumentów/SKW oraz usługi poczty elektronicznej w oparciu o mechanizmy DLP (Data Loss Prevention)
6. Możliwość zaawansowanej analizy zagrożeń w usłudze w czasie rzeczywistym
7. Możliwość wykorzystania uwierzytelniania wieloskładnikowego (MFA) przy logowaniu do usługi będącej przedmiotem zamówienia oraz aplikacji internetowych Zamawiającego wykorzystujących SSO/SAML.
8. Możliwość tworzenia zasad dostępu warunkowego dla usług i dynamiczne przydzielanie polityk bezpieczeństwa zależnie od przypisanej do użytkownika roli.

9. Możliwość samodzielnej zmiany hasła przez użytkowników z wykorzystaniem witryny internetowej.
10. Możliwość przypisywania licencji poszczególnym użytkownikom.
11. Możliwość logowania się użytkowników i zarządzania stacjami roboczymi bez konieczności bezpośredniego podłączenia do lokalnego kontrolera domeny Zamawiającego. Zarządzanie stacjami roboczymi musi obejmować między innymi:
    a. Zarządzanie ochroną antywirusową.
    b. Zarządzanie aktualizacjami.
    c. Zarządzanie licencjami posiadanego oprogramowania firmy Microsoft.
    d. Konfigurowanie polityk zabezpieczeń .

1.3.1.8. Usługi analizy danych

Usługi analizy danych wbudowane w produkt muszą umożliwiać:

1. Konfigurowanie on-line kokpitów informacyjnych wizualizujących wyniki analiz danych.
2. Gotowe mechanizmy podłączania różnego rodzaju danych strukturalnych, semi-strukturalnych i niestrukturalnych.
3. Korzystanie z gotowych algorytmów i modeli analizy oraz budowa własnych modeli w języku R.
4. Możliwość instalacji bramy w środowisku on-premises, która umożliwia eksport danych do systemu online.

1.3.1.9. Subskrypcja pakietu biurowego

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

1. Pakiet biurowy musi udostępniać funkcje ułatwień dostępu dla osób niepełnosprawnych takie jak:

    a. Możliwość dyktowania tekstu przez użytkownika
    b. Głosowy odczyt tekstu przez pakiet biurowy
    c. Dodawanie tekstu alternatywnego do grafik
    d. Stosowanie różnych kontrastów dla tła i tekstu
    e. Możliwość wyróżniania wierszy lub akapitów w celu ułatwienia odczytu przez użytkownika
2. Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
    2.1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
3. Wymagania dotyczące interfejsu użytkownika:
    3.1. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
    3.2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    3.3. 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.
    3.4. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
    3.5. 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:

4.1. Posiada kompletny i publicznie dostępny opis formatu:
   4.1.1. Ma zdefiniowany układ informacji w postaci XML zgodnie z załącznikiem nr 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. (tj. Dz.U. 2017, poz. 2247) w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
   4.1.2. Umożliwia tworzenie plików w formacie XML.
   4.1.3. Wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES.
4.2. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
4.3. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
4.4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
4.5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.

5. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   5.1. Edytor tekstów.
   5.2. Arkusz kalkulacyjny.
   5.3. Narzędzie do przygotowywania i prowadzenia prezentacji.
   5.4. Narzędzie do tworzenia drukowanych materiałów informacyjnych.
   5.5. Narzędzie do tworzenia i pracy z lokalną bazą danych.
   5.6. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
   5.7. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
   5.8. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
6. Edytor tekstów musi umożliwiać:
   6.1. 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.
   6.2. 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.
   6.3. Wstawianie oraz formatowanie tabel.
   6.4. Wstawianie oraz formatowanie obiektów graficznych.
   6.5. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
   6.6. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
   6.7. Automatyczne tworzenie spisów treści.
   6.8. Formatowanie nagłówków i stopek stron.
   6.9. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
   6.10. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
   6.11. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
   6.12. Określenie układu strony (pionowa/pozioma).
   6.13. Wydruk dokumentów.
   6.14. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
   6.15. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2013, 2016 , 2019 i późniejsze z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
   6.16. Zapis i edycję plików w formacie PDF.

6.17. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
6.18. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco.
6.19. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.

7. Arkusz kalkulacyjny musi umożliwiać:
7.1. Tworzenie raportów tabelarycznych.
7.2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
7.3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
7.4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
7.5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
7.6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
7.7. Wyszukiwanie i zamianę danych.
7.8. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
7.9. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS.
7.10. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
7.11. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
7.12. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
7.13. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
7.14. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
7.15. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
7.16. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2013, 2016, 2019 i późniejsze, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
7.17. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

8. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
8.1 Przygotowywanie prezentacji multimedialnych, które będą:
8.1.1. Prezentowanie przy użyciu projektora multimedialnego.
8.1.2. Drukowanie w formacie umożliwiającym robienie notatek.
8.1.3. Zapisanie jako prezentacja tylko do odczytu.
8.1.4. Nagrywanie narracji i dołączanie jej do prezentacji.
8.1.5. Opatrywanie slajdów notatkami dla prezentera.
8.1.6. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
8.1.7. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
8.1.8. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
8.1.9. Możliwość tworzenia animacji obiektów i całych slajdów.

8.1.10. 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.
8.1.11. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2013, 2016, 2019 i późniejsze.

9. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
   9.1. Tworzenie i edycję drukowanych materiałów informacyjnych
   9.2. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
   9.3. Edycję poszczególnych stron materiałów.
   9.4. Podział treści na kolumny.
   9.5. Umieszczanie elementów graficznych.
   9.6. Wykorzystanie mechanizmu korespondencji seryjnej.
   9.7. Płynne przesuwanie elementów po całej stronie publikacji.
   9.8. Eksport publikacji do formatu PDF oraz TIFF.
   9.9. Wydruk publikacji.
   9.10. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
10. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
   10.1. Tworzenie bazy danych przez zdefiniowanie:
      10.1.1. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
      10.1.2. Relacji pomiędzy tabelami.
      10.1.3. Formularzy do wprowadzania i edycji danych.
      10.1.4. Raportów.
      10.1.5. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych.
      10.1.6. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów.
      10.1.7. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
   11.1. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory:
      11.1.1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
      11.1.2. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
      11.1.3. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
      11.1.4. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
      11.1.5. Automatyczne grupowanie poczty o tym samym tytule.
      11.1.6. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
      11.1.7. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
      11.1.8. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
      11.2. Zarządzanie kalendarzem:
      11.2.1. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
      11.2.2. Przeglądanie kalendarza innych użytkowników.
      11.2.3. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.

11.3. Zarządzanie listą zadań:
- 11.3.1. Zlecanie zadań innym użytkownikom.
- 11.3.2. Zarządzanie listą kontaktów.
- 11.3.3. Udostępnianie listy kontaktów innym użytkownikom.
- 11.3.4. Przeglądanie listy kontaktów innych użytkowników.
- 11.3.5. Możliwość przesyłania kontaktów innym użytkowników.
- 11.3.6. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

12. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
- 12.1. Pełna polska wersja językowa interfejsu użytkownika.
- 12.2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
- 12.3. Dostępność aplikacji na platformie Windows 8.1 lub wyższych oraz OSX 10 lub wyższych.
- 12.4. 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.
- 12.5. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
- 12.6. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
- 12.7. Obsługa telekonferencji SKW:
- 12.7.1. Dołączania do telekonferencji.
- 12.7.2. Szczegółowej listy uczestników.
- 12.7.3. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
- 12.7.4. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
- 12.7.5. Głosowania.
- 12.7.6. Udostępniania plików i pulpitów.
- 12.7.7. Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji.
- 12.7.8. Możliwość zmiany kanału komunikacji z pośrednictwem wiadomości błyskawicznych do połączenia głosowego i/lub wideo w ramach pojedynczej, otwartej w aplikacji sesji (bez konieczności przełączania się pomiędzy aplikacjami).
- 12.7.9. Lista adresowa wraz ze statusem obecności, opisem użytkowników SKW, zdjęciami użytkowników, listą dostępnych do komunikacji z nimi kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji oraz wydzielania grup kontaktów typu ulubione lub ostatnie.
- 12.7.10. Status obecności, dający możliwość ręcznego ustawiania statusu (dostępny, zajęty, nie przeszkadzać, z dala od komputera, niedostępny), automatycznej synchronizacji z jego aktywnością w systemie operacyjnym stacji roboczej, a w przypadku instalacji wybranych systemów poczty elektronicznej – dostępu do informacji o dostępności użytkownika na bazie wpisów do jego kalendarza.
- 12.7.11. Możliwość rozszerzania listy adresowej o zewnętrznych użytkowników wraz z informacjami opisowymi i kontaktowymi.
- 12.7.12. Historia ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień.
- 12.7.13. Integracja ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.

12.7.14. Definiowanie i konfiguracja urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
12.7.15. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
12.7.16. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
12.7.17. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.
12.8. Pakiet musi udostępniać możliwość instalacji oprogramowania w wersji offline na 5 komputerach użytkownika końcowego.

1.3.1.10. Usługi zarządzania urządzeniami oraz tożsamością użytkowników

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

1. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy.
2. Zagwarantowanie poziomu dostępności na poziomie min 99,9%.
3. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018 lub równoważnymi.
4. 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.
5. Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania.
6. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi.
7. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego.
8. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
9. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
10. 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”.
11. Dostępność raportów logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
12. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN).
13. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS.
14. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych.
15. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego.
16. Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.
17. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.

18. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.
19. Zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT).
20. Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych.
21. Portal klasy self-service dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej.
22. Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS).
23. Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.
24. Automatyczna klasyfikacja treści dokumentów (przechowywanych na zasobach plikowych, bibliotekach lub transportowanych poprzez system pocztowy) zgodnie z definiowanymi wzorcami,
25. Wykorzystanie klasyfikacji danych do dynamicznego aplikowanie restrykcji związanych z dostępem do informacji zapobiegające niekontrolowanemu wyciekowi informacji.
26. 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, umożliwiające granularną kontrolę dostępu do poufnych informacji i wymuszenie ustalonych polityk ochrony informacji.
27. Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub spoza sieci lokalnej.
28. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia.
29. Jednokrotne logowanie (single sign-on)w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań.
30. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia.
31. 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).
32. Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwalające na audyt i kontrolę zgodności realizacji uprawnień użytkowników z ustalonymi politykami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.
33. Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

1.3.1.11. Podsystem zarządzania tożsamością

System zarządzania tożsamością elektroniczną ma zapewniać pobieranie, agregację oraz synchronizacje danych o użytkownikach z różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego centrum certyfikacji (CA) Zamawiającego.

1. **Bezpieczeństwo:**

1.1. System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).
1.2. System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami firewall oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
1.3. System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
1.4. System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

2. Skalowalność:

2.1. System zarządzania tożsamością musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie do 100 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.

3. Interoperacyjność:

3.1. System zarządzania tożsamością musi 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.
3.2. System zarządzania tożsamością musi zapewniać możliwość realizacji dwukierunkowej, uprawnionej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

4. Skalowalność funkcjonalna:

4.1. System zarządzania tożsamością powinien umożliwiać rozszerzanie funkcjonalności o połączenia z nowymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu.
4.2. System zarządzania tożsamością powinien umożliwiać rozszerzanie rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.

5. Wymagania w zakresie cech i funkcjonalności rozwiązania:

5.1. Agregacja i synchronizacja danych.
5.2. System musi zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
5.3. System zarządzania tożsamością, w ramach początkowego wdrożenia musi zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
5.3.1. Pliki tekstowe CSV, AVP, LDIF.
5.3.2. Bazy danych MS SQL 2000 – 2016 i późniejsze, Oracle.
5.3.3. Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.

6. System musi 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.
7. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.
8. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.

9. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
10. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
11. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
12. System musi 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.
13. Repozytorium danych teleadresowych:
    13.1. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
14. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.
15. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla
16. wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.
15. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.
16. Zarządzanie kartą elektroniczną:
    16.1. Zarządzanie kartami elektronicznymi musi obejmować: zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów).
    17. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 50 000 użytkowników.
    18. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnym przechowywanym i wygenerowanym na karcie).
19. System musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów dla jednego użytkownika).
20. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania itp..
21. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP.
22. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI.
23. System musi wspierać zarządzanie certyfikatami używanymi do uwierzytelnienia w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
24. System musi umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów.
25. Po wystawieniu certyfikatu, system musi umożliwić włączenie automatycznej publikacji certyfikatu w katalogu LDAP.
26. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP.

27. 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).
28. 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).
29. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:
    29.1. Użytkownik lub administrator wprowadza PIN inicjujący.
    29.2. PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW.
    29.3. System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku.
    29.4. PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API).
30. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.
31. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego.
32. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego).
33. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:
    33.1. Nie mniej niż 6 znaków.
    33.2. Wymagane cyfry litery małe i duże.
    33.3. PIN może się powtarzać przez N zmian.
34. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne.
35. 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.
36. Workflow musi umożliwiać, implementacji następujących scenariuszy użycia:
    36.1. W pełni automatyczne wystawianie certyfikatów dla użytkowników.
    36.2. Wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu.
    36.3. Automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia.
    36.4. Weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu.
    36.5. Powiadamianie administratorów systemu o wygasaniu certyfikatów dla serwerów /urządzeń wchodzących w skład infrastruktury teleinformatycznej.
    36.6. Wbudowane 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:
        36.6.1. 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.
        36.6.2. Certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW systemu.
        36.6.3. Definiowanie takich reguł musi być dostępne bezpośrednio dla operatora systemu i nie może wymagać dodatkowych opłat licencyjnych.

37. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, liczby zmian PIN'ow, czy liczby odblokowanych kart.
38. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania).
39. Podsystem zarządzania urządzeniami mobilnymi.
40. Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
    40.1. Integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy komunikacyjne.
    40.2. Wykorzystanie bazy użytkowników znajdujących się w Active Directory.
    40.3. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych.
41. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji:
    41.1. Nazwa urządzenia.
    41.2. Identyfikator urządzenia.
    41.3. Nazwa platformy systemu operacyjnego.
    41.4. Wersja oprogramowania układowego.
    41.5. Typ procesora.
    41.6. Model urządzenia.
    41.7. Producent urządzenia.
    41.8. Architektura procesora.
    41.9. Język urządzenia.
    41.10. Lista aplikacji zainstalowanych w ramach przedsiębiorstwa.
42. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
43. Wymagania w zakresie dystrybucji oprogramowania:
    43.1. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych 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.
    43.2. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji.
    43.3. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
    43.4. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych:
    43.5. *. appx (Windows RT).
    43.6.. *.xap (Windows Phone 8).
    43.7. *.ipa (iOS).
    43.8. *.apk (Android).
    43.9. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
        43.9.1. Windows Store.
        43.9.2. Windows Phone Store.
        43.9.3. Android Google Play Store.
        43.9.4. iOS App Store.
44. W obszarze polityki haseł usługa zapewni:
    44.1. Zdefiniowanie wymuszenia hasła.
    44.2. Określenie minimalnej długości hasła.

44.3. Określenie czasu wygasania hasła.
44.4. Określenie liczby pamiętanych haseł.
44.5. Określenie liczby prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia.
44.6. Określenie czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła. 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.

1.3.1.12. Podsystem ochrony informacji

1. 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:
   1.1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania.
   1.2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2016 lub nowszych poprzez wbudowany w te produkty interfejs.
   1.3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji.
   1.4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji.
2. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
   2.1. Brak uprawnień dostępu do informacji.
   2.2. Informacja tylko do odczytu.
   2.3. Prawo do edycji informacji.
   2.4. Brak możliwości wykonania systemowego zrzutu ekranu.
   2.5. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej.
   2.6. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej.
   2.7. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
3. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej.
4. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji.
5. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji.
6. Możliwość wykorzystania na platformach systemu Windows 8.1 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT.
7. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

1.3.1.13. Podsystem usługi katalogowej

Usługa katalogowa musi zapewnić:

2. Możliwość zintegrowania jednokrotnego logowania (SSO) dla popularnych aplikacji typu SaaS.
3. Gotowe mechanizmy uwierzytelniania do aplikacji webowych dla użytkowników zewnętrznych.
4. Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji.
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.
10. Konsolę zarządzania tożsamością i dostępem.

1.3.2. Subskrypcja usług komunikacyjnych, bezpieczeństwa i pakietu biurowego klasy desktop typ II (subskrypcja na użytkownika) (Subskrypcja pakietu M365 EDU A3 Unified ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft (P/N: AAD-38397))

Subskrypcja zgodna z opisem w punkcie 1.4.1 przeznaczona dla studentów jednostki Zamawiającego.

1.3.2.1. Oprogramowanie biurowe:
Microsoft Office 2016 i nowsze.

1.3.2.3. Repozytorium dokumentów
Microsoft OneDrive/Share Point.

1.3.2.4. Usługa komunikacji wielokanałowej On-Line
Microsoft Teams.

1.3.2.5. Usługa chmurowa
Microsoft 365 A3/Microsoft Azure AD

3. Okres realizacji zamówienia
3.1. Realizacja zamówienia w ciągu 4 dni od zawarcia umowy.

W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca zobowiązany jest do przeprowadzenia migracji użytkowników wraz z przypisywanymi do nich zasobami (pliki, skrzynki pocztowe, zespoły, grupy) z usług Wykorzystywanych przez Zamawiającego opisanych w punkcie 2 OPZ, w terminie 4 dni od dnia zawarcia umowy w sposób umożliwiający użytkownikom Zamawiającego, bezprzerwowe korzystanie z usług w trakcie migracji.

3.2. Realizacja zamówień aktualizacyjnych
W ciągu 4 dniu od otrzymania zamówienia od Zamawiającego

3.3. Całkowity okres realizacji umowy
36 miesięcy od dnia rozpoczęcia realizacji przedmiotu umowy

4. Warunki płatności

Termin płatności 30 dni od daty doręczenia faktury po podpisaniu umowy rozłożona na 3 równe części na podstawie faktur VAT wystawionych w terminach:
- pierwsza FV po zrealizowaniu zamówienia,
- druga FV w pierwszą rocznicę zamówienia,
- trzecia FV w drugą rocznicę zamówienia

4.1. Za zamówienie Zamawiający zapłaci wykonawcy Wynagrodzenie z tytułu realizacji przedmiotu niniejszej umowy, płatnego na podstawie faktur VAT wystawionych
4.1.1 po odebraniu dostawy przedmiotu umowy zrealizowanej w ramach zamówienia