Załącznik nr 1 do SWZ
DZ.270.141.2023

Opis przedmiotu zamówienia

I. Skrótowy opis przedmiotu zamówienia:

Przedmiotem zamówienia jest zakup subskrypcji oprogramowania Workspace ONE i Assist oraz świadczenie usługi wsparcia wykonawcy oraz producenta dla wdrożonego w PGL LP centralnego systemu do zarządzania urządzeniami mobilnymi, klasy wyższej niż EMM tj. UEM (ang. Unified Endpoint Management), przez okres 36 miesięcy od dnia podpisania umowy.

Słownik:

Administrator centralny - zdefiniowana w systemie UEM rola administratora mająca dostęp do najwyższych uprawnień w systemie. Administrator centralny posiada wgląd do zasobów systemu UEM we wszystkich jednostkach organizacyjnych PGL LP.

Administrator regionalny - zdefiniowana w systemie UEM rola administratora mająca dostęp do wybranych funkcji w systemie. Administrator regionalny posiada wgląd do zasobów systemu UEM w jednostkach podległych.

Administrator jednostki organizacyjnej PGL LP - zdefiniowana w systemie EUM rola administratora mająca dostęp do wybranych funkcji systemu dla konkretnych użytkowników końcowych i urządzeń w swojej jednostce organizacyjnej.

Android Enterprise Recommended (AER) - program firmy Google zalecający wymagania dla systemu UEM oraz urządzeń mobilnych z systemem Android.

Assist – usługa zapewniającą m.in. udostępnianie pracownikom pomocy technicznej w przedsiębiorstwie podglądu bądź sterowania ekranem na urządzeniu mobilnym w czasie rzeczywistym, dostępu do przeglądania, kopiowania, wgrywania i usuwania plików z pamięci urządzenia. Usługa jest dostępna z poziomu konsoli centralnej do zarządzania urządzeniami mobilnymi i jest zainstalowana w infrastrukturze Zamawiającego.

Architektura systemu - podział oprogramowania na komponenty oraz definicje funkcji tych komponentów oraz występujące między nimi relacje.

Awaria - zgłoszona dysfunkcjonalność Systemu UEM mająca wpływ na działanie usług i funkcjonalności Systemu UEM określonych w wymaganiach OPZ.

Awaria krytyczna - zgłoszona dysfunkcja Systemu UEM polegająca na jego działaniu niezgodne z opisanym w aktualnej dokumentacji, które powoduje zawieszanie się pracy Systemu, wprowadza niespójność w bazie danych lub zaburzenia w integralności danych; sytuacja, w której System w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcji w systemie Zleceniodawcy (w szczególności uniemożliwiona jest realizacja wymiany informacji pomiędzy urządzeniami mobilnymi a poszczególnymi serwisami udostępnionymi dla urządzeń mobilnych w systemach usługowych PGL LP poprzez mikrotunele VPN zestawione przez System UEM); masowe błędne zapisy w bazie spowodowane Błędem w Systemie. Awarią krytyczną jest także sytuacja, kiedy wyżej wymienione zdarzenia spowodowane są błędem uniemożliwiającym współpracę Systemu z systemem operacyjnym lub z bazą danych. Awarią krytyczną jest również podatność w Systemie mogąca zagrozić poufności bądź integralności danych Klienta.

COBO – (ang. Company Owned, Business Only) tryb pracy urządzenia z systemem Android, który definiuje urządzenie tylko do pracy firmowej wprowadzając większe restrykcje dot. ustawień i zarządzania. Cała zawartość pamięci urządzenia jest firmowa.

COPE – (ang. Company Owned Personally Enabled) tryb pracy urządzenia z systemem Android, który zapewnia podział urządzenia na część firmową i osobistą w oddzielnych kontenerach, dając większą swobodę użytkownikowi m.in. wyboru instalowanych aplikacji, przechowywanych informacji w części osobistej.

Defekty - inne zgłoszone dysfunkcjonalności Systemu UEM nie mające istotnego wpływu na działanie usług i funkcjonalności Systemu UEM określonych w wymaganiach OPZ.

DMZ - wydzielany obszar sieci komputerowej PGL LP nienależący ani do sieci wewnętrznej, ani do sieci publicznej.

Mikrotunel VPN - tunel VPN Systemu UEM umożliwiający wymianę informacji pomiędzy certyfikowanymi aplikacjami mobilnymi, a dedykowanymi im serwisami udostępnionymi dla urządzeń mobilnych w systemach usługowych PGL LP.

Nagios – nazwa własna oprogramowania do monitorowania sieci, urządzeń

sieciowych, aplikacji oraz serwerów, rozpowszechniany na podstawie licencji GPL. Może monitorować hosty oraz usługi według określonych ustawień, dzięki czemu jest możliwe dostosowanie go do swoich potrzeb.

Konsola (operatorska/zarządzająca) Systemu UEM - strony HTML umożliwiające realizację funkcjonalności Systemu EMM z użyciem przeglądarki internetowej.

PGL LP - oznacza Państwowe Gospodarstwo Leśne Lasy Państwowe.

PKI - system świadczenia usług uwierzytelniania, szyfrowania, integralności za pośrednictwem kryptografii klucza publicznego i prywatnego.

Portal samoobsługowy użytkownika - wydzielone funkcje konsoli systemu UEM umożliwiające samodzielne uruchamianie wybranych funkcji UEM przez użytkownika urządzenia mobilnego.

Profil konfiguracyjny – zestaw ujednoliconych ustawień definiowanych przez administratora.

SSL – standard, protokół Secure Socket Layer zapewniający poufność i integralność transmisji danych, a także uwierzytelnienie serwera oraz klienta.

System - w przypadku braku dookreślenia rozumiany jako System UEM.

System EMM - rozszerzony względem Systemu MDM zbiór zaimplementowanych technologii informatycznych ukierunkowanych na zarządzanie urządzeniami mobilnymi, sieciami bezprzewodowymi i mobilnymi usługami komputerowymi z kontekście biznesowym. Celem EMM jest: ustalenie, czy i jak dostępne mobilne urządzenia powinny być zintegrowane z procesami i usługami informatycznymi systemów PGL LP; zabezpieczenie informacji korporacyjnej zapisanej na urządzeniach mobilnych; dystrybucja oprogramowania mobilnego oraz wsparcie pracowników podczas użytkowania urządzeń mobilnych.

System MDM - zbiór zaimplementowanych technologii, usług i funkcjonalności informatycznych służący do administrowania urządzeniami mobilnymi jak smartfony i tablety oraz realizujący polityki bezpieczeństwa przyjęte przez PGL LP w obszarze funkcjonowania urządzeń mobilnych.

SZBiM - System Zgłaszania Błędów i Modyfikacji funkcjonujący w PGL LP, służący do rejestracji zgłoszeń awarii przez użytkowników i automatycznego powiadamiania Wykonawcy.

Środowisko Produkcyjne - wydzielona część Systemów Klienta i Systemu

UEM służąca do gromadzenia i przetwarzania rzeczywistych danych biznesowych.

Token - szczególna seria bitów pełniąca rolę biletu zezwalającego na rozpoczęcie wysyłania danych w sieci.

Tunel VPN - kanał komunikacyjny zabezpieczony przed niepowołanym dostępem (odczytem i modyfikacją) poprzez zastosowanie kryptografii zapewniający poufność, integralność i autentyczność przesyłanych danych.

Użytkownik - pracownik PGL LP, korzystający z Systemu UEM.

UEM - rozszerzony względem Systemu EMM, ujednolicony sposób zarządzania punktami końcowymi w przedsiębiorstwie.

Wysoka dostępność usługi (HA, High Availability) - dostępność systemu na poziomie 99,999% czasu.

Zgłoszenie - informacja przekazana do Wykonawcy o zaistniałej awarii, awarii krytycznej lub defektu poprzez e-mail, SZBiM lub telefonicznie, powinna zostać potwierdzona zwrotnie przez e-mail od Wykonawcy.

II. Szczegółowy opis przedmiotu zamówienia

1. Opis zakresu dostawy:

W ramach zamówienia wykonawca dostarczy:

1.1 Subskrypcje on premise oprogramowania Workspace ONE *(Workspace ONE Advanced)* i Assist *(Vmware Airwatch Advanced Remote Management)* w liczbie 14105 sztuk *(obecnie w systemie zamawiającego funkcjonują licencje wieczyste on premise, które należy zastąpić)*. Oferowany model subskrypcji nie może wiązać się z koniecznością przeniesienia jakichkolwiek komponentów systemu Zamawiającego do usług chmurowych.

2. Opis usługi *:*

W ramach realizacji przedmiotu zamówienia Wykonawca będzie świadczył/realizował następujące usługi:

2.1 Wykonawca zapewni świadczenie usług wsparcia Producenta dla posiadanego przez PGL LP systemu Workspace ONE *(Workspace ONE Advanced)*

i Assist *(Vmware Airwatch Advanced Remote Management)* firmy VMware, przez cały okres Umowy. Realizacja zamówienia będzie obowiązywać od następnego dnia roboczego po jej podpisaniu przez okres 36 miesięcy.

Wsparcie producenta będzie świadczone zgodnie z następującymi zasadami:

2.1.1. Usługi wsparcia producenta będą świadczone w języku polskim lub w innym przypadku, przy udziale Wykonawcy.

2.1.2. Zgłoszenia będą przekazywane za pośrednictwem Wykonawcy a w szczególnych przypadkach bezpośrednio do producenta za pośrednictwem platformy internetowej do kontaktu z serwisem producenta. Szczególnym przypadkiem może być brak kontaktu z Wykonawcą lub inna przyczyna mająca wpływ na opóźnienie wykonania zgłoszenia.

2.1.3. Awarie i defekty eksploatowanego oprogramowania będą zgłaszane do Wykonawcy za pośrednictwem poczty e-mail, telefonicznie lub przy pomocy platformy funkcjonującej obecnie w systemie zamawiającego – System Zgłaszania Błędów i Modyfikacji zwany dalej SZBiM, z odpowiednim nadaniem uprawnień dla Wykonawcy lub inną drogą uzgodnioną formalnie z Wykonawcą. Zgłoszenia użytkowników, Administratorów regionalnych i w jednostkach LP, będą zatwierdzane po ich zweryfikowaniu do realizacji przez Administratorów centralnych Zamawiającego lub koordynatorów umowy.

2.1.4. Zgłoszenia mogą być przekazywane w trybie 365 dni w roku/7 dni w tygodniu/24 godziny na dobę, również w dni wolne od pracy.

2.1.5. Przewiduje się następujący czas usuwania awarii

	Czas reakcji	Wstępne rozwiązanie problemu – przywrócenie funkcjonalności	Ostateczne rozwiązanie problemu
Poziom 1 Awarie krytyczne	1 godz.	4 godz.	24 godz.
Poziom 2 Awarie	4 godz.	8 godz.	5 dni

Poziom 3 Defekty	8 godz.	3 dni	Rozwiązanie problemu w uzgodnionym czasie

2.1.6. Rozpoczęcie usuwania awarii powinno nastąpić zaraz po otrzymaniu zgłoszenia z zachowanym czasem reakcji przewidzianym dla ustalonego w zgłoszeniu priorytetu.

2.1.7. Wsparcie producenta powinno zapewniać Zamawiającemu możliwość instalacji aktualizacji i poprawek oprogramowania w tym oprogramowania sprzętu przez cały okres świadczenia usługi. Wykonawca zapewni Zamawiającemu dostęp do opisu aktualizacji w języku polskim i będzie uczestniczył w procesie pobierania aktualizacji i odpowiadał za ich poprawną instalację wraz ze sprawdzaniem poprawności działania systemu.

2.1.8. Realizacja usług wsparcia Producenta będzie potwierdzana okresowymi raportami sporządzanymi przez wykonawcę. Wzór raportu oraz terminy jego przekazywania Zamawiającemu określa Umowa.

2.2. Wykonawca zapewni świadczenie usług wsparcia dla prawidłowej eksploatacji systemu Workspace ONE firmy Vmware wraz z modułami dodatkowymi (pomoc zdalna Assist, usługi mapowe i lokalizacji, usługa Load Balancerów, monitoringu działania usług – Nagios) posiadanymi przez PGL LP przez cały okres Umowy.

Wsparcie Wykonawcy będzie świadczone zgodnie z następującymi zasadami:

2.2.1. Usługi wsparcia Wykonawcy będą świadczone w języku polskim.

2.2.2. Wykonawca zapewni utrzymanie systemu w najnowszych wersjach (instalacja musi odbywać się maksymalnie do 4 miesięcy od udostępnienia przez producenta nowszej wersji oprogramowania a w przypadku wykrytych podatności – w czasie przewidzianym jak dla awarii krytycznej) przez cały okres Umowy.

2.2.3. Wykonawca zapewni możliwość uruchomienia wszystkich funkcjonalności, które zapewnia system w ramach posiadanych subskrypcji systemu Workspace ONE (Workspace ONE Advanced) i Assist (Vmware Airwatch

Advanced Remote Management), które Zamawiający będzie wykorzystywał w swoim przedsiębiorstwie.

2.2.4. Wykonawca zapewni poprawną instalację właściwych certyfikatów dla systemu. Certyfikaty odpłatne zapewni Zamawiający najpóźniej 3 dni przed ich wygaśnięciem.

2.2.5. Awarie i usterki eksploatowanego oprogramowania będą zgłaszane przy pomocy poczty elektronicznej, telefonicznie lub przy pomocy SZBiM. Zgłoszenia rejestrowane przez użytkowników systemu będą przekazywane do wykonawcy przez administratorów centralnych lub koordynatorów umowy.

2.2.6. Zgłoszenia mogą być przekazywane w trybie 365 dni w roku/7dni w tygodniu/24 godziny na dobę, również w dni wolne od pracy.

2.2.7. Przewiduje się następujący czas usuwania awarii

	Czas reakcji	Wstępne rozwiązanie problemu – przywrócenie funkcjonalności	Ostateczne rozwiązanie problemu
Poziom 1 Awarie krytyczne	1 godz.	4 godz.	24 godz.
Poziom 2 Awarie	4 godz.	8 godz.	5 dni
Poziom 3 Defekty	8 godz.	3 dni	Rozwiązanie problemu w uzgodnionym czasie

2.2.8. Rozpoczęcie usuwania awarii powinno nastąpić zaraz po otrzymaniu zgłoszenia z zachowanym czasem reakcji przewidzianym dla ustalonego w zgłoszeniu priorytetu.

2.2.9. Wykonawca zapewni dostępność systemu na poziomie 24 godzin na dobę, 7 dni w tygodniu. Maksymalny czas braku dostępności systemu określa się na 1 godzinę miesięcznie.

2.2.10. W przypadku zaistnienia konieczności zmian w architekturze systemu funkcjonującego w PGL LP wymagane jest opracowanie i zgłoszenie do Zamawiającego projektu zmian w celu jego zatwierdzenia przez Zamawiającego. W przypadku dokonania jakichkolwiek zmian w architekturze systemu funkcjonującego w PGL LP, realizowanych przez wykonawcę w ramach wsparcia, zapewni on wykonanie aktualizacji obowiązującej dokumentacji.

2.2.11. Realizacja usług wsparcia Wykonawcy będzie potwierdzana okresowymi raportami. Wzór raportu oraz terminy jego przekazywania Zamawiającemu określa Umowa.

2.2.12. Wykonawca jest zobowiązany do odnotowywania w systemie producenta potwierdzenia zakupu każdej subskrypcji, która zostanie przypisana do konta jednostki PGL LP. Dostęp do podglądu systemu w ww. zakresie powinien być możliwy dla każdego z rodzaju administratorów wymienionych w słowniku – po uprzednim zarejestrowaniu imiennych kont w systemie.

3. Opis dostawy w ramach „prawa opcji”*:*

3.1. Zamawiający w ramach „prawa opcji” w okresie trwania umowy może zlecić Wykonawcy dostawę dodatkowych subskrypcji i wsparcia. Zamówienie w ramach „prawa opcji” oznacza, że zamawiający może zlecić Wykonawcy jego realizację w części lub w całości. Z tytułu niezrealizowania „prawa opcji” Wykonawcy nie przysługuje dodatkowe wynagrodzenie. Zasady zlecania i odbioru „prawa opcji” określa Umowa.

Prawo opcji może być realizowane na rzecz ZILP lub jednostek LP.

4. Opis zamówień w ramach „prawa opcji”:

Zamawiający w ramach prawa opcji w okresie trwania umowy może zlecić Wykonawcy realizację poniższych zamówień. Zamówienie w ramach „prawa opcji” oznacza, że Zamawiający może zlecić Wykonawcy jego realizację w części lub w całości. Z tytułu niezrealizowania „prawa opcji” Wykonawcy nie przysługuje dodatkowe wynagrodzenie. Zasady zlecania i odbioru „prawa opcji” określa Umowa.

4.1 Zamawiający w okresie obowiązywania Umowy może zlecić wykonawcy dostawę kolejnych subskrypcji wraz ze wsparciem, wykraczające poza maksymalną liczbę określoną w zamówieniu podstawowym, o kolejne, do 2295 sztuk. Subskrypcje wraz ze wsparciem mogą być zamawiane pojedynczo - od 1 szt.

5. Opis środowiska IT w którym będzie realizowane zamówienie:

Lasy Państwowe posiadają centralny ujednolicony system klasy UEM firmy Vmware pod nazwą Workspace ONE wraz z funkcjonalnością Assist, zdolny do jednoczesnego zarządzania punktami końcowymi. System ten w Lasach Państwowych jest wykorzystywany do zarządzania urządzeniami mobilnymi typu smartfon i tablet z systemem Android lub iOS. Przeważająca liczba, około 90% stanowią urządzenia z systemem Google Android. System został zainstalowany i skonfigurowany w infrastrukturze klienta, bez konieczności komunikacji z infrastrukturą umieszczoną w zasobach producenta Systemu i obejmuje blisko 50 serwerów wirtualnych w środowisku VMware vSphere użytkowanym przez PGL LP, rozmieszczonych w dwóch centrach przetwarzania danych z zastosowaniem redundancji dla zachowania pełnej dostępności (active-active). Część maszyn wirtualnych stanowią systemy MS Serwer 2016, część systemy dostarczonych przez producenta obrazów VMware Workspace ONE i Assist oraz Load Balancery wykorzystujące usługę HA Proxy (Zamawiający nie wyklucza wykorzystania sprzętowego rozwiązania). System zapewnia odseparowanie części funkcji, które powinny być dostępne z sieci publicznej do strefy DMZ. W skład usługi wchodzi środowisko WorkspaceONE wraz z komponentami dodatkowymi do obsługi pomocy zdalnej, funkcji mapowych oraz usługi Load Balancera, które zapewniają nieprzerwaną pracę usług. Zarządzanie urządzeniami mobilnymi odbywa się z poziomu centralnej konsoli zarządzającej, do której mają dostęp administratorzy centralni, regionalnie i jednostek organizacyjnych Lasów Państwowych, ze wszystkich blisko 500 grup organizacyjnych. Dostępna jest również konsola dla użytkowników, określona jako portal samoobsługowy. Liczba urządzeń zarejestrowanych obecnie w systemie wynosi około 14.000 a konfiguracja została wyskalowana na obsługę minimum 20.000 urządzeń jednocześnie. System zapewnia rejestrację urządzeń w konsoli administracyjnej z wykorzystaniem tokenów i kodów QR. Rejestracja urządzenia mobilnego w systemie pozwala na przypisanie go do konta domenowego w usłudze katalogowej wykorzystywanej przez Zamawiającego. Rejestracja urządzeń z systemem Android jest możliwa w dwóch trybach: COBO i COPE. Rejestracja urządzeń z iOS odbywa się w jednym trybie. Urządzenia mobilne pracują zgodnie ze skonfigurowanymi centralnie profilami i polisami bezpieczeństwa, które można modyfikować. Konsola umożliwia m.in. odczytanie statusu urządzeń i ich parametrów , zapewnieniu tunelowania VPN do zasobów firmowych przez wybrane aplikacje, obsługę służbowej poczty e-mail w usłudze MS Exchange, dostępu do stron intranetowych, usług korporacyjnej chmury firmowej z wykorzystaniem certyfikatów PKI i innych metod uwierzytelniania, obsługę publicznego

i wewnętrznego sklepu z aplikacjami, pomocy zdalnej, map firmowych, lokalizacji wybranych urządzeń i innych usług wynikających z funkcjonalności dostarczonych z Systemem. Praca na urządzeniu pozwala na jednoczesne korzystanie ze stron internetowych oraz aplikacji publicznych dostarczonych na urządzenia. W systemie będą rejestrowane nowe urządzenia mobilne po zakupie kolejnych licencji wraz ze wsparciem producenta dla urządzeń końcowych .
Zamawiający od czasu wdrożenia systemu zarejestrował około 14 tys. urządzeń w widocznych w systemie blisko 500 grupach organizacyjnych rozproszonych w całym kraju. Rejestracja urządzenia w systemie Workspace ONE wiąże się z przywróceniem urządzenia do ustawień fabrycznych. Obecnie wszystkie urządzenia mobilne są w użytkowaniu i służą do codziennego wykonywaniu na nich zadań służbowych na dedykowanych aplikacjach firmowych dostarczonych na urządzenia. Ciągłość dostępności pracy systemu Workspace ONE jest dla Zamawiającego kluczowym celem ponieważ zadania służbowe realizowane przy pomocy systemu muszą być cały czas dostępne. W godzinach pracy biur jednostek Lasów Państwowych, które przypadają w dni powszednie od godziny 6:00-16:00, nie mogą występować awarie, a w przypadku ich wystąpieniu musi następować ich niezwłoczna naprawa.
Zamawiający zakupił do tej pory blisko 14.000 licencji wieczystych oprogramowania Workspace ONE wraz z funkcjonalnością Assist, na urządzenia końcowe zarejestrowane w systemie. Dodatkowo prowadził cykliczne wdrożenia urządzeń do systemu i specjalistyczne szkolenia dla pracowników z zakresu administracji i eksploatacji Systemu i urządzeń aby zaznajomić ich z pełną funkcjonalnością.

III. Opis rozwiązania równoważnego - kryteria stosowane w celu oceny równoważności.

Zamawiający wymaga dostarczenia i implementacji w środowisku serwerowym PGL LP komponentów systemu UEM ogłoszonego przez firmę Google jako systemu zgodnego z wymaganiami programu Google Android Enterprise Recommended oraz spełniającego poniższe wymogi funkcjonalne (oferowane produkty muszą spełniać wszystkie wymagania Zamawiającego wskazane w Opisie przedmiotu zamówienia i w umowie na dzień składania ofert). Wdrożenie innego systemu o takich samych własnościach może wiązać się ze znacznym nakładem pracy i kosztów. Proces ten może być trudny do realizacji na wielu urządzeniach jednocześnie z zachowaniem ich ciągłości pracy. Zamawiający nie posiada zastępczych urządzeń mobilnych a zatem

migracja urządzeń mobilnych do systemu równoważnego wiązałaby się z uruchomieniem wszystkich urządzeń mobilnych jednocześnie lub z podziałem na etapy. Optymalny czas migracji pojedynczego urządzenia musiałby odbyć się w ciągu 12h wraz z przekopiowaniem danych, gdyby system wymagał przywrócenia urządzeń końcowych do ustawień fabrycznych, a następnie przekazania go pracownikowi Lasów Państwowych do pracy w nowym systemie.

Warunki równoważności:

1. Wymagania dla architektury:

1.1. system musi zapewniać możliwość instalacji wszystkich jego komponentów w infrastrukturze PGL LP, bez konieczności komunikacji z infrastrukturą umieszczoną w zasobach producenta Systemu;
1.2. system musi gwarantować bezpieczną architekturę w postaci rozdzielności jego funkcji, tak aby dawał możliwość odseparowania części funkcji systemu, które powinny być dostępne z sieci publicznej do strefy DMZ;
1.3. system ma być wdrożony z trybem wysokiej dostępności (HA) poprzez redundancje każdego elementu sytemu w obu centrach przetwarzania Lasów Państwowych (active-active);
1.4. system musi zapewnić możliwość instalacji poszczególnych komponentów systemu na serwerach z systemem operacyjnym Microsoft Windows Serwer 2016 (lub wyższym) lub/i Red Hat 6 (lub wyższym), w środowisku wirtualnym VMware vSphere użytkowanym obecnie przez PGL LP;
1.5. system musi posiadać możliwość obsługi minimum 20 000 urządzeń mobilnych bez potrzeby rozbudowy systemu;

1.6. system musi korzystać z PKI PGL LP.

2. Wymagania dla zarządzania urządzeniami mobilnymi

2.1. Obsługa urządzeń pracujących pod kontrolą systemów operacyjnych:
  2.1.1. Android - minimum w wersji 8.x i wyższych,
  2.1.2. Apple iOS-minimum w wersji 12 i wyższych;
2.2. Pobieranie informacji o zarządzanych urządzeniach mobilnych:
  2.2.1. nazwa urządzenia,
  2.2.2. numer UDID, IMEI/MEID, IMSI, numer telefonu,
  2.2.3. nazwa producenta urządzenia, model,
  2.2.4. numer seryjny urządzenia,
  2.2.5. wersja oprogramowania systemu operacyjnego urządzenia,

2.2.6. lista aplikacji zainstalowanych z wyszczególnieniem typu, wersji, rozmiaru,
2.2.7. wykrywanie statusu złamania zabezpieczeń systemu operacyjnego, urządzenia mobilnego tzw. jailbreak lub rooted,
2.2.8. informacje na temat zajętości pamięci, kondycji baterii (poziom jej zużycia) i poziomu naładowania
2.2.9. śledzenie położenia urządzenia bazując na informacjach z odbiornika GPS, pozwalające na automatyczne wysyłanie przez urządzenie informacji o jego położeniu co jedną minutę bądź wielokrotność;

2.3. Zarządzanie z poziomu centralnej konsoli zarządzającej zawierającej funkcjonalności:

2.3.1. dostęp do konsoli z wykorzystaniem szyfrowanego połączenia SSL poprzez przeglądarkę internetową,
2.3.2. konfiguracja uprawnień z wykorzystaniem zdefiniowanych ról w systemie,
2.3.3. możliwość logicznego podziału systemu z zachowaniem pełnej odrębności ustawień oraz komponentów z możliwością przypisania do każdej z nich dedykowanego administratora (ang. multi-tenant),
2.3.4. definiowanie grup użytkowników oraz przypisywanie różnych polis bezpieczeństwa/uprawnień dla każdej grupy z osobna przez rolę administratora centralnego; grupy użytkowników mają być ustrukturyzowane i odzwierciedlać strukturę drzewiastą AD PGL LP,
2.3.5. polską wersję językową konsoli operatorskiej w zakresie rejestracji urządzeń oraz aplikacji na urządzeniach końcowych, w pozostałym zakresie funkcjonalnym EMM dopuszcza się angielską wersję językową,
2.3.6. definiowanie polityk, grup profili konfiguracyjnych, grup typów urządzeń, wykorzystywanych na wszystkich poziomach zarządzania jedynie z centralnego poziomu zarządzania systemem przez rolę administratora centralnego

2.4. Zarządzanie i monitorowanie danych telekomunikacyjnych:
2.4.1. ustawienia dotyczące restrykcji wykorzystywania urządzeń za granicą (roaming) w zakresie połączeń głosowych oraz transmisji danych,
2.4.2. blokowanie transmisji danych poza wskazanymi sieciami operatorów,
2.4.3. definiowanie i monitorowanie ilości przesyłanych danych za pośrednictwem sieci komórkowej,
2.4.4. monitorowanie statusu sieci komórkowej takich jak nazwa operatora, siła sygnału

2.5. Dedykowany samoobsługowy portal w języku polskim dla użytkowników Systemu zapewniający funkcjonalności:

2.5.1. dostęp do portalu z wykorzystaniem szyfrowanego połączenia SSL poprzez przeglądarkę internetową,
2.5.2. samodzielne resetowanie hasła dostępu do urządzenia,
2.5.3. samodzielne blokowanie urządzenia,
2.5.4. wysłanie wiadomości push na urządzenie mobilne,
2.5.5. wyświetlanie położenia urządzenia na mapie (posiadającej możliwość wyświetlania warstw z serwisów PGL LP w standardzie WMS) bazując na danych z GPS,
2.5.6. kasowanie danych i ustawień firmowych (tzw. enterprise wipe),
2.5.7. zerowanie urządzenia - przywrócenie urządzenia do ustawień fabrycznych (ang. device wipe),
2.5.8. wyświetlanie listy zainstalowanych profili oraz aplikacji na urządzeniu mobilnym,
2.5.9. konfigurowanie przez rolę administratora centralnego do jakich opcji ustawień portalu samoobsługowego mają dostęp użytkownicy,
2.5.10. zdalna obsługa urządzenia mobilnego za pomocą konsoli administracyjnej systemu EMM

2.6. Elementy bezpieczeństwa w urządzeniach mobilnych spełniające wymagania:
2.6.1. możliwość podłączenia urządzeń do Systemu za pomocą agenta zainstalowanego na urządzeniu mobilnym (na przykład z użyciem karty pamięci montowanej w urządzeniu, #tagów, kodów QR, tagów NFC lub w trybie zero-touch z użyciem wsadowego pliku CSV) jak również poprzez stronę WWW (urządzenia z systemem iOS)
2.6.2. możliwość przeprowadzenia procesu rejestracji administratorów systemu w jednostce organizacyjnej PGL LP za pośrednictwem dedykowanego portalu webowego,
2.6.3. możliwość jednoczesnej rejestracji dużej liczby urządzeń do Systemu,
2.6.4. automatyczna dystrybucja profili konfiguracyjnych, certyfikatów (w tym osobistych) dla zarejestrowanych użytkowników oraz aplikacji w trakcie procesu rejestracji urządzenia do systemu,
2.6.5. wymuszenie ochrony urządzenia poprzez ustanowienie hasła dostępowego lub innego mechanizmu ograniczającego dostęp osób postronnych,
2.6.6. wymuszenie polityk okresowej zmiany hasła na urządzeniu mobilnym. Możliwość konfiguracji parametrów takich jak: złożoność hasła (w tym liczba znaków), wymuszenie hasła alfanumerycznego, restrykcje dotyczące niepowtarzalności hasła, liczba błędnych prób wprowadzenia hasła po którym nastąpi zerowanie urządzenia,
2.6.7. możliwość dynamicznego przypisywania polityk bezpieczeństwa w zależności od zdefiniowanych reguł czasowych oraz położenia

geograficznego i sposobu podłączenia urządzenia do sieci teleinformatycznej (np.: WI-FI, komórkowa transmisja danych),

2.6.8. możliwość wymuszenia szyfrowania danych na urządzeniach mobilnych oraz zewnętrznych kartach pamięci

2.6.9. możliwość blokowania przez system wbudowanych funkcji i aplikacji na urządzeniu mobilnym,

2.6.10. definiowanie polityk bezpieczeństwa dla urządzeń mobilnych uniemożliwiających usuwanie profili np. dla poczty elektronicznej, Wi-Fi,

2.6.11. definiowanie polityk bezpieczeństwa uniemożliwiających podłączenie do systemu urządzeń dla których wykryto złamanie zabezpieczeń systemu tzw. jailbreak lub rooted,

2.6.12. wymuszenie automatycznego zestawienia tunelu VPN oraz kierowanie całego lub wybranego ruchu do zdefiniowanych tuneli VPN odpowiedzialnych za podłączenia do kilkunastu serwisów udostępnianych dla urządzeń mobilnych w systemach usługowych PGL LP,

2.6.13. możliwość automatycznego uwierzytelnienia przy nawiązaniu tuneli VPN certyfikatem/ami otrzymanym/i w procesie rejestracji do systemu;

2.7. Wymagania dla zarządzania aplikacjami:

2.7.1. instalowanie oraz usuwanie aplikacji na urządzeniach mobilnych,

2.7.2. zarządzanie blokowaniem instalacji oraz dostępu do poszczególnych aplikacji z zewnętrznych sklepów (np. App Store, Google Play),

2.7.3. tworzenie wewnętrznego sklepu z certyfikowanymi aplikacjami (tzw. Enterprise Store),

2.7.4. tworzenie listy aplikacji niepożądanych, których nie można instalować na urządzeniach mobilnych (tzw. czarna lista),

2.7.5. tworzenie listy aplikacji dozwolonych do instalacji (tzw. biała lista).

3. Wymagania integracji z systemami wykorzystywanymi przez PGL LP:

3.1. wymagana jest integracja z usługami katalogowymi: Active Directory, w wersji użytkowanej przez PGL LP- 2016 lub wyżej;

3.2. wymagane jest aby baza użytkowników systemu oraz atrybutów była pobierana z Active Directory w trybie manualnym oraz automatycznym;

3.3. wymagana jest integracja z Infrastrukturą PKI zamawiającego opartą Microsoft Certification Authority – 2012 R2 lub wyżej w zakresie autentykacji użytkowników;

3.4. wymagana jest integracja z wykorzystywanym aktualnie systemem poczty elektronicznej Zamawiającego w wersji Microsoft Exchange i 365.

3.5. wymagana jest integracja oraz raportowanie do zewnętrznego systemu dziennika zdarzeń w standardzie syslog;

3.6. wymagana jest obsługa mechanizmów SAML (ang. Security Assertion Markup Language) wykorzystywanych do pośredniczenia

w uwierzytelnianiu i automatycznym przekazywaniu informacji o uprawnieniach użytkowników między systemami i aplikacjami.

4. Wymagania dla obsługi klienta poczty elektronicznej:

4.1. system musi wspierać automatyczną konfigurację kont pocztowych w procesie rejestrowania do systemu bazujących na rozwiązaniach: Exchange 2016 (ActiveSync) lub wyższych, z wykorzystaniem standardowych protokołów pocztowych SMTP, POP3, IMAP (również w wersji szyfrowanej);

4.2. system musi obsługiwać uwierzytelnianie się do konta pocztowego za pomocą certyfikatu osobistego wydanego przez PKI PGL LP, otrzymanego w procesie rejestracji urządzenia do systemu;

4.3. system musi umożliwiać konfigurację kont pocztowych Microsoft Exchange ActiveSync w celu kontroli przepływu wiadomości email oraz implementacji dodatkowych mechanizmów bezpieczeństwa poczty elektronicznej, takich jak:

4.3.1. blokowanie wysyłania/odbierania załączników na urządzeniach mobilnych,

4.3.2. ograniczenie wielkości wysyłanych oraz odbieranych załączników,

4.3.3. blokowanie dostępu do wiadomości pocztowych w przypadku naruszenia lub niespełnienia zdefiniowanych polityk bezpieczeństwa przez urządzenie mobilne,

4.3.4. blokowanie dostępu do systemu pocztowego dla urządzeń, które nie zostały zarejestrowane w systemie,

4.3.5. definiowanie oprogramowania do odbioru poczty firmowej na urządzeniu mobilnym.

4.4. dopuszcza wykorzystanie wbudowanych w iOS i Android klientów pocztowych do obsługi bezpiecznej poczty firmowej o ile możliwa będzie ich instalacja w kontenerze EMM.

5. Wymagania dla bezpiecznej przeglądarki WWW:

5.1. producent rozwiązania UEM musi dostarczyć bezpieczną i zarządzaną przez system UEM, przeglądarkę stron WWW serwisów PGL LP, wspierającą wybrane przez Zamawiającego systemy mobilne;

5.2. system musi posiadać funkcję uniemożliwiającą korzystanie z niezarządzanych przez system UEM przeglądarek WWW dostępnych na urządzeniach mobilnych;

5.3. wymagane jest aby dostarczone przez producenta systemu przeglądarki WWW umożliwiały:

5.3.1. szyfrowane tunelowanie ruchu WWW do sieci wewnętrznej za pośrednictwem komponentów rozwiązania UEM,

5.3.2. dostęp do wewnętrznych stron WWW (Intranet) bez konieczności zestawiania tunelu VPN przez dodatkowe aplikacje,

5.3.3. automatyczne logowanie się do intranetowych stron webowych z wykorzystaniem mechanizmu Kerberos domeny Windows AD,
5.3.4. kontrolę i definiowanie stron do jakich użytkownicy i grupy użytkowników mogą mieć dostęp,
5.3.5. definiowanie i blokowanie dostępu do stron niepożądanych.

6. Rodzaj licencji

Zamawiający wymaga dostawy 36 miesięcznych subskrypcji on premise. Model licencjonowania nie może zakładać przeniesienia jakichkolwiek komponentów systemu Zamawiającego do usług chmurowych.

7. Specyfikacja wymagań implementacyjnych

7.1. Wykonanie projektu technicznego wdrożenia systemu UEM w środowisku PGL LP. Wykonany projekt wymaga zaakceptowania przez Zamawiającego w trybie podpisania protokołu odbioru przed podjęciem dalszych prac implementacyjnych.
7.2. Instalacja komponentów systemu EMM na serwerach wirtualnych PGL LP.
7.3. Integracja systemu EMM z systemem AD oraz PKI PGL LP.
7.4. Konfiguracja szablonów w Urzędzie certyfikacji Zamawiającego (Microsoft CA).
7.5. Konfiguracja profili bezpieczeństwa dla urządzeń mobilnych z systemami Apple iOS, Google Android.
7.6. Obsługa tunelowania aplikacji za pomocą wbudowanego w system UEM rozwiązania lub przygotowanie do integracji systemu EMM z systemem VPN Zamawiającego (Check Point) i realizacja połączeń.
7.7. Przygotowanie profili konfiguracyjnych dla urządzeń mobilnych z systemami Apple iOS i Google Android, w zakresie uzgodnionym z Zamawiającym.
7.8. Praktyczne szkolenie w języku polskim dla centralnych administratorów systemu EMM - maksymalnie 5 osób w siedzibie Zamawiającego w wymiarze minimum 24 godzin łącznie, nie więcej niż 6 godzin dziennie.
7.9. Praktyczne szkolenie w języku polskim dla regionalnych administratorów UEM - maksymalnie 25 osób w miejscu wskazanym przez Zamawiającego lub jednym z ośrodków szkoleniowych PGL LP w wymiarze minimum 16 godzin,
7.10. Szkolenia dla centralnych administratorów muszą odbywać się przed terminem szkolenia dla regionalnych administratorów UEM.
7.11. Przygotowanie dokumentacji powykonawczej systemu UEM.
7.12. Oferowany system UEM musi przejść testy zgodnie z procedurą

testową stanowiącą załącznik nr 1 do OPZ. Zamawiający uzna wymagania wskazane w załączniku za spełnione jeżeli dostarczony system UEM przejdzie pozytywnie wszystkie testy na minimum 6 urządzeniach wskazanych w załączniku nr 2.

7.13. System musi zapewniać zarządzanie urządzeniami mobilnymi tzw. ,,Mobile Device Management" (MDM) oraz bezpieczny dostęp z urządzeń mobilnych do systemów PGL LP takich jak: portale intranetowe WWW, portale intranetowe Microsoft SharePoint, zasobów plikowych, poczty elektronicznej.

7.14. Wymaganie, aby dostęp do systemów pocztowych, jak również do wybranych serwisów wewnętrznych PGL LP odbywał się z wykorzystaniem autoryzacji za pomocą osobistego certyfikatu wydawanego dla użytkownika lub logowaniem hasłem domenowym.

7.15. Zamawiający nie dopuszcza, aby oferowane rozwiązanie UEM zbudowane zostało w oparciu o komponenty i oprogramowanie więcej niż jednego producenta produkującego oprogramowanie UEM.

7.16. Zamawiany system UEM powinien móc funkcjonować w systemie Android Enterprise zarówno w modelu „Work Profile", jak i „Device Owner".

7.17. Zamawiający zapewni niezbędne licencje systemów operacyjnych dla produkcyjnego działania systemu UEM, w tym Microsoft Windows Serwer, Red Hat, w ramach wirtualnej platformy VMware vSphere wykorzystywanej przez PGL LP dla poszczególnych elementów systemu jak również informację o urządzeniach i użytkownikach mobilnych w zakresie niezbędnym do realizacji zamówienia. Pozostałe licencje wymagane do uruchomienia systemu stanowią przedmiot zamówienia.

IV. Lista urządzeń testowych w przypadku zaoferowania rozwiązania równoważnego dostępna jest pod adresem: https://www.zilp.lasy.gov.pl/lista-urzadzen

V. Załączniki do Opisu przedmiotu zamówienia *(jeżeli dotyczy):*

Integralną część opisu przedmiotu zamówienia stanowią:

1. Załącznik nr 1 – procedura testowa (w przypadku zaoferowania rozwiązania równoważnego)
2. Załącznik nr 2 SZBIM

Procedura testowa

Lp	Testowana funkcjonalność	Procedura testowa
I. Testy ogólne		
1	System powinien umożliwiać jednoczesne zarządzanie urządzeniami dla wielu organizacji, bez wzajemnego dostępu do urządzeń różnych organizacji (multi-tenancy).	Sprawdzenie czy **Administrator** jednostki organizacyjnej PGL LP może zarządzać tylko urządzeniami zgodnie ze swoimi uprawnieniami.
2	Obsługa systemu na poziomie **Administratora** jednostki PGL LP, oraz aplikacji na urządzeniach w języku polskim.	Sprawdzenie wersji językowej systemu i aplikacji na urządzeniach pod kontem poprawnej obsługi w języku polskim, dla procesów obsługi na poziomie **administratora** jednostki organizacyjnej PGL LP.
3	Dostęp do konsoli systemu poprzez szyfrowany protokół https.	Sprawdzenie czy **Administratorzy** mogą uzyskać dostęp do konsoli z użyciem szyfrowanego protokołu https.

4	System powinien zapewnić wsparcie dla przeglądarek Internet Explorer wer. 11 i nowsze, Edge (Windows 10), Chrome wer. 57 i nowsze oraz Mozilla Firefox wer. 52 i nowsze. Pełna funkcjonalność obsługi musi być zapewniona przynajmniej na jednej z wymienionych przeglądarek.	Weryfikacja w dokumentacji systemu wspieranych przeglądarek, należy zaznaczyć jakie wersje są wspierane. Wykonanie podstawowych czynności obsługi systemu w/w przeglądarkach, zalogowanie, zarządzanie użytkownikami, zarządzanie urządzeniami, zarządzanie politykami itp. Należy zawrzeć spostrzeżenia **administratora** czy nie występowały anomalie związane z obsługą.
5	Dostęp do systemu dla **użytkownika** z podziałem na uprawnienia dostępu do poszczególnych funkcjonalności w oparciu o definiowalne role (szablony uprawnień). Polityki zostaną zdefiniowane w projekcie technicznym.	Należy zweryfikować poziomy uprawnień przypisane do roli w odniesieniu do funkcji udostępnianych **użytkownikowi**.
6	Zapewnienie pełnej instalacji systemu w infrastrukturze Zamawiającego.	Należy zweryfikować zainstalowane komponenty w odniesieniu do projektu technicznego, oraz sprawdzić czy nie występują odwołania do obcej infrastruktury.
7	Zapewnienie pracy systemu w trybie fail-over (High Availability) w infrastrukturze Zamawiającego.	Należy zweryfikować działanie funkcji HA, poprzez symulację awarii aktywnego węzła, w odniesieniu do utrzymania pełnej dostępności systemu UEM.

8	Wsparcie co najmniej dla systemów operacyjnych Android (minimum w wersji 6.x i wyższych), Apple iOS (minimum w wersji 9 i wyższych).	Weryfikacja w dokumentacji systemu dostępności wymaganej funkcjonalności.
9	Integracja z serwerami Active Directory, LDAP w zakresie zarządzania uprawnieniami.	Należy zweryfikować czy uprawnienia nadawane w AD pokrywają się z uprawnieniami pobranymi do systemu UEM.
10	Wsparcie dla bezpiecznej poczty e-mail.	Należy zweryfikować wsparcie bezpiecznej poczty dla MS Exchange.
11	Widok listy urządzeń powinien być możliwy do definiowania przez administratora, wraz z wizualizacją alertów dotyczących naruszenia polityki bezpieczeństwa dla poszczególnych urządzeń.	Należy zweryfikować wymaganie zgodnie ze zdefiniowaną funkcjonalnością.
12	Administrator może udostępniać dla użytkownika informacje o jego urządzeniu, wraz z wizualizacją alertów dotyczących naruszenia polityki bezpieczeństwa dla poszczególnych urządzeń.	Należy zweryfikować wymaganie zgodnie ze zdefiniowaną funkcjonalnością.
13	System musi umożliwiać na pojedynczym urządzeniu, na wszystkich urządzeniach jednocześnie lub na określonych grupach urządzeń z poziomu konsoli administracyjnej: instalację i konfigurację aplikacji oraz wykonanie kopii zapasowej danych firmowych (Zamawiający nie przewiduje wykonywania kopii zapasowych danych prywatnych).	Należy zweryfikować wymaganie zgodnie ze zdefiniowaną funkcjonalnością.

14	Integracja serwera z systemem SNMP Nagios (możliwość zaprezentowania na wykresie aktualnego stanu systemu). Zamawiający dopuszcza integrację Nagios-a z wykorzystaniem web API (JSON, REST, itp.).	Należy zweryfikować czy system został zintegro-wany z zewnętrznym systemem monitorującym Zamawiającego lub uruchomionym w ramach wdrożenia, w zakresie wizualizacji stanu krytycznych komponentów systemu UEM.
15	Licencjonowanie - system powinien pozwalać na pełne zarządzanie określoną w licencji ilością urządzeń aktywnych oraz umożliwiać jednocześnie nielimitowane przechowywanie informacji o urządzeniach nieaktywnych np. „w naprawie”.	Należy zweryfikować wymaganie zgodnie ze zdefiniowaną funkcjonalnością.
II. Test w zakresie zdalnej konfiguracji		
1	Konfigurację polityk dostępu do sieci, punktów dostępu do Internetu, ustawienia punktów dostępowych WiFi (również opartych o EAP-TLS), konfiguracja poczty e-mail (dla systemu MS Exchange).	Należy zweryfikować wymaganie zgodnie ze zdefiniowaną funkcjonalnością, poprzez wykonanie każdego z wymienionych etapów konfiguracji i weryfikacji wyników na urządzeniu końcowym

2	Możliwość konfiguracji cyklicznego raportowania danych o zarządzanych urządzeniach, użytkownikach i kartach SIM. Raporty powinny zawierać: -typ i model urządzenia -wersję systemu operacyjnego zainstalowanego na urządzeniu, -użytkownik, -stan urządzenia (np. zarządzany, niezarządzany, w serwisie itp.), -listę zainstalowanych aplikacji firmowych wraz z ich wersją, -lista urządzeń z zabronionymi aplikacjami, -ilość zajętej i wolnej pamięci wewnętrznej i zewnętrznej, -numer seryjny karty sim, -ilość wykorzystanych danych z sieci GPRS, -ostatnia lokalizacja urządzenia, -Ilość wykorzystanych danych z sieci Wi-Fi, -nr identyfikujący urządzenie np. IMEI, -adres MAC.	Wykonać raporty zgodnie z zawartą funkcjonalnością, zweryfikować poprawność uzyskanych danych w odniesieniu do testowych urządzeń zamawiającego.
3	System musi umożliwiać grupowania raportów w zakresie: -bezpieczeństwo, alerty (naruszenie polityk), -urządzenia i ich stan, -dane użytkowników, -dane kart SIM, -lokalizacja.	Wykonać raporty zgodnie z zawartą funkcjonalnością, zweryfikować poprawność uzyskanych danych w odniesieniu do testowych urządzeń zamawiającego
4	Możliwość łączenia konfiguracji w pakiety (zbiory konfiguracji) oraz ich instalacji na urządzeniach.	Przygotować pakiet konfiguracji i przeprowadzić instalację na urządzeniu końcowym, zweryfikować konfigurację urządzenia końcowego w korelacji z

		konfiguracją zawartą w pakiecie.
III. Test w zakresie instalacji aplikacji		
1	Zdalna instalacja aplikacji na urządzeniach mobilnych z konsoli **administratora**.	Wykonać zdalną instalację aplikacji na urządzeniu końcowym. **Administrator** wykonuje instalację, na urządzeniu końcowym wymagana jest interakcja z **użytkownikiem**.
2	Zdalna instalacja aplikacji w trybie cichym na urządzeniach mobilnych z konsoli **administratora**	Wykonać zdalną instalację aplikacji na urządzeniu końcowym i zweryfikować czy była wymagana reakcja po stronie użytkownika urządzenia końcowego. W trybie cichym **użytkownik** końcowy nie powinien być angażowany do procesu instalacji.
3	Podgląd listy zainstalowanych aplikacji.	Wykonać podgląd listy zainstalowanych aplikacji i zweryfikować czy jest zgodna ze stanem faktycznym na urządzeniu końcowym.
4	Możliwość zablokowania samodzielnej instalacji aplikacji przez **użytkownika** na urządzeniach Zamawiającego.	Wykonać test na urządzeniu końcowym polegający na samodzielnej próbie instalacji przez **użytkownika** zablokowanej aplikacji. Użytkownik nie powinien posiadać możliwości instalowania zablokowanych aplikacji.

5	Możliwość cichego usunięcia niepożądanych aplikacji – dotyczy aplikacji zainstalowanych przez administratora lub użytkownika w tym np. ze sklepu firmowego (własne aplikacje), Google Play lub Apple App Store na urządzeniach Zamawiającego.	Wykonać, w trybie cichym, odinstalowanie aplikacji i zweryfikować czy była konieczna reakcja po stronie użytkownika końcowego. W trybie cichym użytkownik końcowy nie powinien być angażowany do procesu odinstalowania aplikacji.
6	Zdalna instalacja i konfiguracja klienta pocztowego lub dostarczonego w ramach rozwiązania.	Wykonać zdalną instalację i konfigurację klienta pocztowego umożliwiającą poprawną komunikację Zamawiającego w tym wysyłanie i odbieranie wiadomości zaszyfrowanych. Zweryfikować stan konfiguracji na urządzeniu końcowym w odniesieniu do konfiguracji zdefiniowanej zdalnie.
7	Możliwość skonfigurowania wewnętrznego sklepu z aplikacjami “corporate appstore”.	Należy skonfigurować wewnętrzny sklep “corporate appstore” i wykonać instalację udostępnionych aplikacji. Test przeprowadzić dla udostępnionych aplikacji np. Leśnik+, ODK Collect, klient poczty.
8	Możliwość konfiguracji aplikacji firm trzecich np. monitorowanie i zarządzanie dedykowanym oprogramowaniem antywirusowym.	Np.: Przesłanie agenta antywirusa na urządzenie mobilne i weryfikacja poprawności jego działania.
IV. Test w zakresie konfiguracji bezpieczeństwa		

1	Konfiguracje polityk dotyczących uwierzytelniania na urządzeniach mobilnych: -wymuszenie uwierzytelnienia przy uruchamianiu urządzenia -definiowanie stopnia skomplikowania hasła lub pinu (wybór z grup znaków), -definiowanie czasu bezczynności, po którym następuje automatyczna blokada wymuszająca ponowne uwierzytelnienie, -definiowanie maksymalnej ilości prób uwierzytelnienia, po której następuje blokada urządzenia, -wymuszenie okresowej zmiany hasła/pinu, -przechowywanie historii haseł/pinów uniemożliwiającej ponowne ich użycie.	Wykonać test polityki definiującej zasady bezpieczeństwa hasła, polegający na weryfikacji wymienionych funkcjonalność na urządzeniu końcowym
2	Zdalne usunięcie danych z urządzenia w przypadku jego utraty.	Należy zweryfikować czy po uruchomieniu procedury zdalnego usunięcia danych, faktycznie zostały usunięte dane firmowe z urządzenia końcowego
3	Możliwość zdalnego wykonania resetu fabrycznego na urządzeniu mobilnym.	Zdefiniować zdalny reset fabryczny, zweryfikować wynik na urządzeniu końcowym.
4	Możliwość zdalnego zablokowania resetu fabrycznego na urządzeniu mobilnym.	Zdefiniować blokadę resetu fabrycznego, zweryfikować wynik na urządzeniu końcowym.
5	Możliwość zdalnego zablokowania (hot-spot).	Zdefiniować blokadę (hot-spot), zweryfikować wynik na urządzeniu końcowym.

6	Możliwość zdalnego zablokowania urządzenia.	Zdefiniować zdalne zablokowanie, zweryfikować wynik na urządzeniu końcowym.
7	Możliwość zdefiniowanie i wysłania komunikatu do “znalazcy” po zablokowaniu urządzenia.	Zdefiniować komunikat do ”znalazcy”, zweryfikować wynik na urządzeniu końcowym.
8	Możliwość generowania zapasowej kopii danych z urządzenia, zdefiniowanych folderów lub zawartości kontenerów firmowych, na podstawie harmonogramu lub uruchamianych ręcznie. Generowanie kopii zapasowych musi być uzależnione od warunków sieci dostępnej dla urządzenia końcowego.	Zdefiniować generowanie kopii zapasowych, zweryfikować ich wykonanie, wykonać procedurę odzyskania danych.
9	Możliwość zablokowania deinstalacji Systemu UEM.	Zdefiniować blokady, zweryfikować wynik na urządzeniu końcowym.
10	Definiowanie białej listy (whitelist) – dozwolonych aplikacji	Zdefiniować białą listę aplikacji, zweryfikować wynik na urządzeniu końcowym. Tylko aplikacje z listy mogą być dostępne do użycia.
11	Definiowanie czarnej listy aplikacji (blacklist), z których nie mogą korzystać użytkownicy zarządzanych urządzeń.	Zdefiniować czarną listę aplikacji, zweryfikować wynik na urządzeniu końcowym. Aplikacje z listy nie mogą być dostępne do użycia.
12	Zablokowanie możliwości instalacji aplikacji przez użytkownika z uwzględnieniem odpowiednich definicji białej i czarnej listy.	Zdefiniować blokadę, zweryfikować wynik na urządzeniu końcowym, w odniesieniu do białej i czarnej listy.

13	Blokowanie możliwości edycji ustawień urządzenia przez użytkowników.	Zdefiniować blokady, zweryfikować wynik na urządzeniu końcowym
V. Test w zakresie separacji danych firmowych i użytkownika		
1	Możliwość zdalnego zablokowania i odblokowania kontenera danych firmowych.	Należy zweryfikować możliwość wykonania zdalnego zablokowania i odblokowania kontenera danych firmowych. Weryfikację przeprowadzić przy użyciu konsoli Systemu UEM.
2	Możliwość zdalnego usunięcia kontenera danych firmowych.	Należy zweryfikować możliwość wykonania zdalnego usunięcia kontenera danych firmowych. Weryfikację przeprowadzić przy użyciu konsoli Systemu UEM.
3	Możliwość dostępu użytkownika do danych prywatnych znajdujących się poza kontenerem danych firmowym.	Należy zweryfikować czy użytkownik bez zalogowania się do kontenera uzyskuje dostęp do danych prywatnych.
VI. Test w zakresie funkcjonalności geolokalizacyjnych		
1	Lokalizacja urządzeń na podstawie danych z czujników GPS lub BTS.	Należy zweryfikować możliwość wykonania lokalizacji na podstawie danych z czujników. Weryfikację przeprowadzić przy użyciu konsoli Systemu UEM, wizualizacja musi być przedstawiona na mapie.

2	Możliwość powiadamiania użytkownika końcowego o włączeniu / wyłączeniu funkcji lokalizacji z konsoli systemu UEM.	Należy zweryfikować możliwość odczytania powiadomień na urządzeniu końcowym.
3	Odpytywanie o lokalizację dostępne dla administratorów i użytkownika urządzenia.	Należy zweryfikować możliwość odczytania lokalizacji.
4	Odpytywanie o lokalizację w trybie ciągłym, z możliwością zdefiniowania interwałów z zależności od: -zmiany lokalizacji o konkretną odległość, -konfigurowalnego interwału czasowego, -zmiany ID stacji bazowej, w której znajduje się telefon komórkowy	Należy zweryfikować możliwość wykonania lokalizacji ciągłej z uwzględnienie testowanych funkcjonalności. Weryfikację przeprowadzić przy użyciu konsoli Systemu UEM.
VII. Test w zakresie zdalnego wsparcia urządzeń		
1	Możliwość zarządzania plikami na urządzeniu mobilnym (otwieranie, kopiowanie, kasowanie i zapisywanie).	Wykonać test zgodnie z weryfikowaną funkcjonalnością w zakresie zarządzania plikami.
2	Możliwość wysyłania powiadomień (PUSH) (do wszystkich, do poszczególnych grup lub do indywidualnych użytkowników.	Wykonać test wysyłania powiadomień do wymienionych grup i użytkowników.
3	Użytkownik końcowy urządzenia mobilnego może sam przy użyciu portalu internetowego dokonać czyszczenia danych lub/i blokady swojego urządzenia (np. w przypadku kradzieży).	Wykonać test zgodnie z weryfikowaną funkcjonalnością.

4	Możliwość wykonania zdalnego restartu urządzenia.	Wykonać test zgodnie z weryfikowaną funkcjonalnością.
VIII. Test w zakresie obsługi systemu Leśnik+		
1	Instalacja startowa aplikacji.	Sprawdzenie czy system automatycznie i poprawnie zainstaluje aplikację na „czystym” urządzeniu, zgodnie z polityką przyjętą dla aplikacji Leśnik+.
2	Konfiguracja parametrów pracy systemu (w tym ustawień transferu) + synchronizacja danych.	Wykonać test działania synchronizacji danych Rejestrator-SILP zgodnie z ustalonymi parametrami Załącznik nr 1 do OPZ konfiguracyjnymi.
3	Zmiana w konfiguracji parametrów adresu domeny serwera z danymi (test przełączania pomiędzy serwerami produkcyjnymi, a testowymi) + synchronizacja danych.	Wykonać test poprawności działania synchronizacji danych Rejestrator-SILP po zmianie adresu domeny serwera, sprawdzenie możliwości „przepinania się” pomiędzy serwisami WAN
4	Uruchomienie aplikacji i zalogowanie w systemie w 2 trybach dostępu do sieci: -online, -offline.	Wykonać test poprawności logowania do aplikacji w różnych trybach dostępu do sieci.
5	Przelogowywanie użytkowników o różnych rolach (Administrator / Leśniczy / Podleśniczy).	Wykonać test poprawności logowania do aplikacji dla różnych ról użytkowników o różnych uprawnieniach.

6	Wykonanie synchronizacji danych (import/eksport): -z wykorzystaniem Interfejsu Leśnik-LAS, -z wykorzystaniem serwisu mapowego ArcGIS.	Sprawdzenie działania modułu synchronizacji danych dla różnych serwisów.
7	Aktualizacja wersji oprogramowania aplikacji Leśnik+: - z automatycznym wymuszeniem instalacji, - na życzenie.	Należy zweryfikować możliwość wymuszenia aktualizacji wersji oprogramowania
8	Sprawdzenie możliwości instalacji aplikacji Leśnik+ poza kontenerem firmowym (obsługa blokady takiej możliwości).	Należy zweryfikować możliwość ustawienia blokady dotyczącej instalacji dedykowanego oprogramowania poza kontenerem.
9	Generowanie wydruków na drukarki termiczne i stacjonarne: -w połączeniu Bluetooth, -w połączeniu WiFi.	Sprawdzenie działania modułu wydruków dla różnych rodzajów połączeń.
10	Sprawdzenie poprawności działania systemu GPS w module mapowym: -online, -offline.	Sprawdzenie poprawnego działania systemu GPS w module mapowym w różnych trybach dostępu do sieci.
11	Generowanie i wydruk obrazów „Historii pracy”.	Sprawdzenie poprawnego działania zapisu i obsługi wydruków grafik (wygenerowanych PNG).
12	Próba ingerencji w dane – próba wejścia do katalogu aplikacji Leśnik+ narzędziami zewnętrznymi (np. za pomocą explorerów plików).	Sprawdzenie czy dane aplikacji są bezpieczne.

13	Zdalne pobranie danych z rejestratora na serwer (ściąganie konkretnych danych z konkretnego rejestratora np. baza SQLite bądź logi błędów).	Sprawdzenie czy istnieje możliwość zdalnego pobrania plików z konkretnego rejestratora na serwer.
14	Zdalne odinstalowanie aplikacji Leśnik+ np. w przypadku wycofania urządzenia z użytku, spowodowane cofnięciem licencji: -automatycznie z wykorzystaniem odpowiednio zdefiniowanej polityki, -„ręcznie” na życzenie, z poziomu serwera.	Sprawdzenie czy istnieje możliwość usuwania dedykowanego oprogramowania, szczególnie w sytuacjach np. kradzież urządzenia lub odebrania roli użytkownikowi.

Załącznik nr 2 do OPZ, DZ.270.141.2023

Opis Systemu: System zgłoszeń Błędów i Modyfikacji (SZBM)

Zamawiający przekazuje podstawowe informacje o wymogach, które nakłada na Wykonawcę stosowanie się do procedur obowiązujących w SZBM. Szczegółowe informacje zostaną podane podczas podpisywania Umowy.
SZBM jest systemem internetowym, dostępnym dla wszystkich jednostek LP, który umożliwia zgłaszanie błędów i problemów powstałych podczas użytkowania systemu oraz propozycji modyfikacji. Systemem zgłoszeń objęte są wszystkie podsystemy wchodzące w skład Systemu Informatycznego Lasów Państwowych.
Zgłoszenia są grupowane tematycznie w grupy związane z poszczególnymi podsystemami systemu informatycznego Lasów Państwowych.
Każdemu zgłoszeniu SZBM nadaje automatycznie unikalny numer, który jest używany podczas odwoływania się do zgłoszenia.
Zgłoszenia są pogrupowane w kategorie. Przykładowymi kategoriami zgłoszeń są: „błąd", „modyfikacja", „konsultacje".
Każdemu zgłoszeniu jest nadawany status zgłoszenia. Przykładowe statusy zgłoszeń: „wprowadzone", „usunięte", „zatwierdzone do realizacji", „w trakcie realizacji", „zrealizowane", „do uzupełnienia".
Każde zgłoszenie użytkownika jest weryfikowane przez upoważnionych pracowników Zamawiającego. Wykonawca obsługuje jedynie zgłoszenia zatwierdzone do realizacji przez koordynatorów Zamawiającego.
Za czas reakcji Wykonawcy na zgłoszenie zatwierdzone do realizacji jest przyjmowany czas, jaki upłynął od zatwierdzenia zgłoszenia do zmiany jego statusu przez Wykonawcę na status „W trakcie realizacji".
Za czas realizacji zgłoszenia przyjmowany jest czas, jaki upłynął od przyjęcia przez Wykonawcę zgłoszenia do realizacji do momentu zmiany statusu zgłoszenia przez Wykonawcę na „Zrealizowane".
Czas reakcji liczymy do momentu pierwszego przyjęcia do realizacji: zmiana statusu na „W trakcie realizacji".
Czas realizacji jest liczony od pierwszego przyjęcia zgłoszenia do realizacji przez Wykonawcę, z wyłączeniem okresu uzupełniania zgłoszenia o dodatkowe informacje przez Zamawiającego.
Zmiana statusu przez Zamawiającego na „Zatwierdzony" ponownie uruchamia odliczanie czasu realizacji.

Realizacja zgłoszenia jest weryfikowana przez Zamawiającego.

SZBM zawiera również podsystem powiadomień. System ten rozsyła do określonych użytkowników Zamawiającego i określonych pracowników Wykonawcy informacje o każdym nowym zgłoszeniu, jak również informacje o każdej zmianie statusu zgłoszenia istniejącego.