

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa oraz wdrożenie systemu zarządzania i ochrony urządzeń mobilnych MDM (Mobile Device Management), wraz z kompletem niezbędnych licencji, przeszkoleniem pracowników oraz zapewnieniem wsparcia technicznego dla zaoferowanego systemu.

I. Szczegółowe wymagania dotyczące systemu MDM

1. Obsługiwane platformy mobilne:

1.1. Google Android w wersji min. 13.0

1.2. iOS w wersji min. 14

2. Zarządzanie urządzeniami:

2.1. System musi wspierać rejestrację urządzeń w MDM poprzez:

- Secure Wi-Fi
- Kod QR
- Moduł NFC
- Kabel USB
- Metodę self-enrollment

2.2 System musi pozwalać na przejęcie kontroli nad urządzeniem przenośnym oraz zdalne zablokowanie i wyczyszczenie urządzenia ze wszystkich danych z poziomu interfejsu systemu w razie potrzeby.

2.3 System musi wspierać następujące modele zarządzania urządzeniami:

- BYOD z możliwością konteneryzacji, separacji danych prywatnych i konfiguracją profili służbowych
- COBO
- COSU
- COPE

2.4. System musi pozwalać na grupowanie urządzeń, utworzenie osobnych polityk dla każdej z utworzonej grup i administrowanie urządzeniami w danych grupach zgodnie z potrzebami Zamawiającego.

2.5. System musi zapewniać zdalną dystrybucję składników systemu, polityk, konfiguracji i aktualizacji na jednym lub wielu urządzeniach mobilnych z poziomu interfejsu systemu.

2.6. System musi automatycznie pobierać dane inwentaryzacyjne urządzenia takie jak:

- Producent
- Model
- Numer seryjny
- IMEI
- Wersja systemu operacyjnego zainstalowanego na urządzeniu
- Wersja firmware
- Informacja o połączeniu sieci Wi-Fi oraz nadane IP
- Adres MAC

- Numer seryjny karty SIM

Oraz zapewniać przestrzeń do przechowywania pobranych informacji o dodanych urządzeniach i kartach SIM w sposób spójny i przejrzysty.

2.7. System musi wykonywać i przechowywać kopie zapasowe zarejestrowanych urządzeń, w szczególności danych takich jak:

- Kontakty
- Wiadomości SMS
- Dziennik połączeń
- Multimedia

przez okres min. miesiąca i w razie potrzeby umożliwiać wgranie zachowanej kopii zapasowej na urządzeniu tożsamym dla tej kopii bądź innym.

3. Zarządzanie aplikacjami:

3.1. System musi blokować próby instalacji lub usunięcia aplikacji przez użytkownika.

3.2. System musi umożliwiać instalację, deinstalację i aktualizację zainstalowanych aplikacji na jednym lub wielu urządzeniach na raz z poziomu interfejsu.

3.3. System musi raportować o stanie zainstalowanych na urządzeniu aplikacji m.in.:

- Wersji
- Użyciu zasobów urządzenia
- Czasie użytkowania

3.4. System musi pozwalać na zdalną administrację i konfigurację zainstalowanych aplikacji m.in.:

- Zdalne wymuszenie ochrony aplikacji hasłem
- Zdalny restart zainstalowanych aplikacji
- Zdalny dostęp do aplikacji w celu weryfikacji działania bądź rozwiązania konkretnych problemów zgłoszonych przez użytkowników

3.5. System musi uniemożliwiać próby ingerencji użytkowników w ustawienia i konfiguracje zainstalowanych aplikacji.

3.6. System musi zawierać opcję utworzenia dedykowanej whitelisty/blacklisty dla aplikacji.

3.7. System musi umożliwiać stworzenie dedykowanego sklepu z wybranymi aplikacjami.

4. Zarządzanie bezpieczeństwem:

W celu zapewnienia wymaganego stopnia bezpieczeństwa system MDM powinien zawierać poniższe opcje zabezpieczeń:

4.1. Wymuszenie wyboru jednego z dostępnych sposobów zabezpieczenia odblokowania urządzenia przez użytkownika oraz zdefiniowanie stopnia złożoności wybranego zabezpieczenia.

4.2. Wymuszenie wygaszania ekranu po X czasie.

4.3. Zdalne blokowanie urządzenia z poziomu konsoli.

4.3. Zdalne wymuszenie restartu lub wyłączenia urządzenia.

4.4. Automatyczne blokowanie dostępu do urządzenia po:

- Próbie wymiany karty SIM
- Zdefiniowanej przez administratora ilości błędnych prób odblokowania telefonu
- Wykryciu próby obejścia zabezpieczeń poprzez root/jailbreak
- Wykryciu próby ingerowania w działanie lub próbę usunięcia agenta systemu MDM na urządzeniu

4.5. Definiowanie dedykowanych polityk zabezpieczeń z rozróżnieniem na grupy urządzeń/użytkowników. Polityki powinny być konfigurowalne z poziomu konsoli zarządzania i automatycznie egzekwowane na urządzeniach po ich przypisaniu do odpowiednich profili lub grup.

4.6. Szyfrowanie pamięci wewnętrznej i zewnętrznej urządzenia.

4.7. Automatyczne informowanie administratora o próbach naruszenia bezpieczeństwa poprzez e-mail, wiadomość SMS lub wiadomość PUSH na wskazanych urządzeniach.

4.8. Blokowanie bądź ograniczenie wybranych funkcjonalności urządzenia poza granicami kraju.

4.9. Blokowanie dostępu bądź ograniczenie możliwości wprowadzania zmian przez użytkownika w funkcjach systemowych takich jak:

- Przywracanie ustawień fabrycznych
- Moduł NFC
- Zewnętrzna pamięć - karta SD
- Zarządzanie plikami poprzez USB
- Ustawienia telefonu
- Tryb samolotowy
- Tryb awaryjny
- Wi-Fi i USB Tethering
- Interfejs Wi-Fi
- Interfejs Bluetooth
- Dane mobilne
- Aparat
- Nagrywanie głosu w aplikacjach

4.10 Zdalne usunięcie danych z urządzenia poprzez:

- Przywrócenie urządzenia do ustawień fabrycznych
- Usunięcie danych służbowych pozostawiając dane prywatne

4.11 Wbudowane centrum certyfikacji pozwalające na generowanie własnych certyfikatów o długość klucza 2048, 3072, 4096, algorytm podpisu SHA256, SHA384, SHA512, czas życia klucza wyrażony w dniach oraz możliwość zarządzania certyfikatami na Urządzeniu.

4.12 Aplikacja agenta instalowana na zarządzanych urządzeniach mobilnych powinna spełniać standardy bezpieczeństwa mobilnego. Oznacza to, że agent nie powinien wprowadzać podatności na urządzeniu, jego komunikacja z serwerem musi być szyfrowana, a kod aplikacji powinien być odpowiednio zabezpieczony przed prostą inżynierią wsteczną i zapewniać utrudniony dostęp do wrażliwych zasobów aplikacji. Aplikacja agenta powinna pochodzić z zaufanego źródła.

4.13 Zastosowanie mechanizmów klasy DLP dla plików udostępnianych jak i załączników poczty e-mail:

- Blokowanie kopiowania i wklejania danych z aplikacji zarządzanych przez system do aplikacji zewnętrznych.
- Możliwość wyłączenia eksportu lub zapisu plików poza kontrolowane środowisko.
- Możliwość zablokowania opcji udostępniania, drukowania oraz zrzutów ekranu.
- Wsparcie dla polityk warunkowych pozwalających na ograniczenie dostępu w przypadku niespełnienia warunków zgodności.
- Wyłączenie lub włączenie możliwości udostępniania danych poza kontener.

5. Architektura i integracja z infrastrukturą IT:

5.1. System wraz z wszelkimi komponentami wymaganymi do prawidłowego działania musi zostać dostarczony w wersji on-premise do instalacji lokalnie na sprzęcie zamawiającego. Dodatkowo, system nie może wymagać do działania stałego utrzymania danych poza Infrastrukturą IT, z wyjątkiem niezbędnych usług zewnętrznych takich jak serwery push producentów Urządzeń (Apple, Google) – które to usługi są standardowym elementem ekosystemu MDM.

5.2. Wszystkie składniki Systemu muszą pochodzić od jednego producenta i być zarządzane z jednej spójnej konsoli administracyjnej.

5.3. System gwarantuje bezpieczną architekturę w postaci rozdzielności jego funkcji i daje możliwość odseparowania części funkcji Systemu, które powinny być dostępne z sieci publicznej do strefy DMZ.

5.4. Wykonawca zobowiązany jest podać minimalne wymagania sprzętowe i programowe niezbędne do instalacji Systemu np. serwerów, systemów operacyjnych, baz danych.

5.5. Wykonawca jest zobowiązany dostarczyć informacje o adresacji IP, nazwach DNS, portach i protokołach sieciowych używanych przez System np. połączenia wychodzące do usług Apple Push Notification Service, Google Firebase Cloud Messaging, tak aby możliwe było odpowiednie skonfigurowanie zapór sieciowych (firewall) u Zamawiającego.

5.6. System musi wspierać integrację z usługami katalogowymi typu Active Directory, LDAP wraz z szyfrowanymi protokołami komunikacji (np. HTTPS, LDAPS) podczas komunikacji urządzeń z serwerem MDM. Integracja powinna umożliwiać m.in. uwierzytelnianie administratorów i użytkowników urządzeń za pomocą kont domenowych, synchronizację kont użytkowników lub grup użytkowników pomiędzy AD a systemem MDM oraz wykorzystanie grup i ról z AD do nadawania polityk urządzeniom w systemie MDM.

5.7. System musi wspierać wirtualizację i umożliwiać instalację komponentów Systemu na udostępnionych przez zamawiającego maszynach wirtualnych.

5.8. Architektura systemu musi być w pełni skalowana, poczynając od architektury dla min. 100 urządzeń z możliwością zwiększenia liczby obsługiwanych urządzeń do tysiąca bez znaczącego wpływu na wydajność i szybkość działania systemu. Czas synchronizacji polityk i otrzymywania komend przez Urządzenia powinien być na poziomie umożliwiającym efektywne zarządzanie, tj. w czasie rzeczywistym lub z minimalnym opóźnieniem.

5.9. Zamawiany system musi posiadać udokumentowane API umożliwiające integrację z innymi systemami informatycznymi m.in.:

- Apple DEP

- Samsung KNOX, w tym Samsung E-FLOTA
- Android Enterprise, w tym Android Zero-Touch

5.8. System MDM musi zapewniać integrację z systemem poczty elektronicznej MS Exchange Server w wersji m.in 19. Musi wspierać automatyczną konfigurację kont pocztowych w procesie rejestrowania do Systemu. System musi ponadto obsługiwać skrzynki pocztowe udostępnione oraz współdzielone. System musi zapewniać uwierzytelnianie do kont pocztowych użytkowników z wykorzystaniem certyfikatu dystrybuowanego za pomocą Systemu lub rozwiązania KCD, bez wymogu wprowadzania hasła przez użytkownika. System musi umożliwiać synchronizację skrzynki pocztowej, kalendarza i kontaktów z aplikacją na Urządzeniu mobilnym.

5.9. System powinien umożliwić integrację z infrastrukturą monitorującą Zamawiającego, w celu nadzorowania dostępności, wydajności oraz stanu Systemu MDM, jak również musi zapewnić możliwość integracji z systemem SIEM w celu przesyłania logów bezpieczeństwa i powiązanych z tym zdarzeń w Systemie MDM.

6. Interfejs i zabezpieczenie systemu MDM:

6.1. System musi posiadać centralną konsolę administracyjną dostępną poprzez przeglądarkę internetową lub dedykowaną aplikację administracyjną. Konsola administracyjna powinna być dostępna co najmniej w języku polskim i angielskim.

6.2. Dostęp do konsoli systemu powinien odbywać się za pomocą szyfrowanych protokołów takich jak HTTPS oraz SSL z wymogiem uwierzytelnienia użytkownika oraz wsparciem dla rozwiązań MFA.

6.3. Konsola systemu MDM powinna umożliwiać intuicyjne zarządzanie dużą liczbą urządzeń, posiadać funkcje wyszukiwania, grupowania urządzeń, a także wysyłania komunikatów/poleceń na urządzenia. System powinien wspierać powiadomienia push, e-mail, SMS do wszystkich urządzeń jednocześnie.

6.4. Dane wrażliwe przechowywane w bazie danych systemu (m.in. hashe hasel, klucze, tokeny uwierzytelniające, kopie konfiguracji Urządzeń zawierające dane) muszą być zabezpieczone kryptograficznie.

II. Monitorowanie, raportowanie i analityka

System musi umożliwiać:

1. Podgląd lokalizacji urządzenia z wykorzystaniem dostępnych narzędzi geolokalizacyjnych (GPS, sieci komórkowe, Wi-Fi) w czasie rzeczywistym przedstawione na mapie z poziomu konsoli.

2. Generowanie raportów o zarządzanych urządzeniach mobilnych:

- Na podstawie wcześniej przygotowanych szablonów;
- W oparciu o wskazane urządzenie, użytkownika lub grupy w określonym przedziale czasu;
- Okresowo, automatycznie wysyłane za pośrednictwem e-mail;
- W czytelnych i edytowalnych formatach np. CSV, XSL, DOC, TXT z możliwością eksportu do formatu PDF

3. Monitorowanie statusu i kondycji każdego, dodanego do systemu urządzenia m.in:

- Stanu baterii

- Ilości wolnej i zajętej pamięci
- Obciążenia procesora i pamięci RAM
- Stanu polityk
- Operatora używanych kart SIM
- Informacji o ostatnim kontakcie urządzenia z serwerem

4. Monitorowanie aktywności internetowej urządzenia i możliwość blokady bądź ograniczenia funkcjonalności następujących opcji:

- Otwieranie linków
- Otwieranie i pobieranie załączników
- Udostępnianie plików poprzez wiadomości e-mail, komunikatory
- Dostęp do stron WWW

III. Wymagania dotyczące dostawy oprogramowania, wdrożenia oraz licencji:

1. Wykonawca jest odpowiedzialny za dostarczenie i kompleksowe wdrożenie oferowanego systemu w wersji on-premise wraz z niezbędnymi aplikacjami, modułami oraz dodatkami wymaganymi do prawidłowego działania systemu MDM.

2. Wykonawca zainstaluje wszystkie wymagane komponenty Systemu MDM na wirtualnym środowisku serwerowym przygotowanym przez Zamawiającego zgodnie z wytycznymi Wykonawcy. Instalacja obejmuje m.in. konfigurację bazy danych, instalację serwerów aplikacji MDM, przygotowanie konsoli administracyjnej oraz wdrożenie i skonfigurowanie innych komponentów koniecznych do prawidłowego działania rozwiązania.

3. Po instalacji Wykonawca zobowiązany jest do zintegrowania dostarczonego systemu MDM z istniejącą infrastrukturą IT Zamawiającego, a w szczególności:

- Integracja z usługą katalogową Active Directory – import kont użytkowników, uwierzytelnianie
- Integracja z serwerem poczty elektronicznej
- Integracja z oprogramowaniem antywirusowym ESET bądź zapewnienie, że dostarczony system nie będzie kolidować z wyżej wspomnianym oprogramowaniem
- Wszelkie integracje wymagane do spełnienia zamawianych funkcjonalności

4. Wykonawca we współpracy z Zamawiającym opracuje i zaimplementuje w Systemie podstawowy zestaw polityk bezpieczeństwa i konfiguracji dla Urządzeń mobilnych, zgodny z wymaganiami Zamawiającego.

5. Udzielenie licencji bezterminowych ze wsparciem producenta podczas trwania umowy na korzystanie z oprogramowania dla 100 urządzeń w ramach zamówienia podstawowego, z możliwością dokupienia dodatkowych z gwarancją stałej ceny w czasie trwania umowy. Licencje powinny być dostarczone z legalnego źródła w formie elektronicznej.

6. Dostarczone licencje nie powinny być przypisane na stałe do konkretnego urządzenia mobilnego, a po jego usunięciu powinna być możliwość ich powtórnego wykorzystania w celu rejestracji tego samego lub nowego urządzenia.

7. Po zakończeniu wdrożenia, Wykonawca zobowiązuje się do przeprowadzenia szkolenia z zamawianego oprogramowania w zakresie administracji i obsługi wdrożonego oprogramowania dla 4 osób wyznaczonych przez Zamawiającego w terminie 30 dni od dnia podpisania protokołu odbioru.

8. Wykonawca dostarczy Zamawiającemu kompletną dokumentację powykonawczą zrealizowanego wdrożenia systemu MDM, sporządzoną w języku polskim w formie elektronicznej (plik PDF lub DOCX).

9. Dokumentacja powykonawcza powinna być sporządzona w taki sposób, aby umożliwić Zamawiającemu samodzielne utrzymanie i administrację Systemu po zakończeniu prac wdrożeniowych, a w szczególności zawierać:

- Opis architektury Systemu (schematy, topologia instalacji, zależności między komponentami),
- Konfigurację serwerów (adresy, konta usługowe, zainstalowane komponenty, wersje oprogramowania),
- Listę adresów IP/portów,
- Listę wdrożonych polityk i ich ustawienia,
- Sposób integracji z innymi systemami (m.in. punkty integracji z AD, integracja z Exchange, integracji z centrum certyfikacji)

IV. Zakres wsparcia technicznego i serwisu dla zakupionego oprogramowania:

Zakres wsparcia Producenta oprogramowania w trakcie trwania obejmuje:

1. Dostęp do pomocy technicznej w dni robocze w godzinach 8:00-16:00 przez czas trwania umowy drogą mailową lub przez dedykowany system zgłoszeniowy Wykonawcy.

2. Usługę konsultacji w zakresie konfiguracji, optymalizacji i innych czynności dotyczących zamawianego oprogramowania w ilości 80 roboczogodzin, zgodnie z zapotrzebowaniem Zamawiającego.

3. Usuwanie usterek i błędów z zachowaniem poniższych zasad:

- Usunięcie błędu krytycznego lub przygotowanie obejścia błędu krytycznego umożliwiające dalsze działanie systemu MDM nastąpi w czasie 48 godzin od momentu przekazania zgłoszenia przez Zamawiającego. Jeżeli bezpośrednią przyczyną powstania błędu krytycznego systemu jest wada w oprogramowaniu MDM, usunięcie błędu krytycznego nastąpi poprzez współpracę Wykonawcy z Producentem w możliwie najszybszym z punktu widzenia producenta, nie dłuższym niż 10 dni roboczych od przyjęcia zgłoszenia.
- Usunięcie błędu, pomimo którego praca z systemem MDM jest możliwa, lecz znacznie wpływa na czas i jakość działania systemu nastąpi w ciągu 5 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
- Usunięcie pozostałych błędów nastąpi w ciągu 10 dni od przekazania zgłoszenia przez Zamawiającego.
- W przypadku braku możliwości usunięcia błędów w podanych wyżej terminach, Dostawca zobowiązany jest dostarczyć i wdrożyć równoważne rozwiązanie zastępcze. Rozwiązanie zastępcze musi zostać każdorazowo uzgodnione i zaakceptowane przez Zamawiającego.
- Rozwiązanie zastępcze nie może funkcjonować dłużej niż 30 dni od daty jego wdrożenia.

4. Dostęp do poprawek i nowych wersji oprogramowania i systemu wraz z informacją o wprowadzanych zmianach.

5. Dostęp do dokumentacji technicznej, dostępnej co najmniej w języku angielskim.

6. Dostęp do bazy wiedzy udostępnianej przez Producenta.

