Załącznik nr 1 do Zapytania Ofertowego

**Opis przedmiotu zamówienia**

**Dostawa systemu do zarządzanie urządzeniami mobilnymi on-premise. Zamawiający wymaga licencji dla min. 350 urządzeń wraz 36 miesięcznym wsparciem technicznym.**

|  |  |
| --- | --- |
| **Lp.** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO** |
| **1.** | System musi umożliwiać instalację:   * on-premise * w chmurze * w chmurze prywatnej |
| **2.** | System musi wspierać instalację na serwerach:   * wirtualnych * fizycznych |
| **3.** | System musi wspierać backup maszyn wirtualnych (snapshot, checkpoint) |
| **4.** | System musi wspierać konfiguracje firewall serwera |
| **5.** | System musi umożliwiać zarządzanie z poziomu przeglądarki |
| **6.** | System musi mieć wsparcie dla min. trzech języków (PL, EN, DE) |
| **7.** | System musi umożliwiać wdrożenia w modelu High Availability |
| **8.** | System musi mieć wbudowane centrum certyfikacji |
| **9.** | System musi mieć wbudowany VPN |
| **10.** | System musi mieć wsparcie dla protokołu SCEP |
| **11.** | System musi mieć wsparcie dla Android Enterprise |
| **12.** | System musi mieć wsparcie dla Android zero-touch |
| **13.** | System musi mieć wsparcie dla Apple Business Manager |
| **14.** | System musi mieć wsparcie dla Apps and Books |
| **15.** | System musi mieć wsparcie dla Knox Mobile Enrollment |
| **16.** | System musi posiadać systemowe narzędzie do backupu serwera |
| **17.** | System musi posiadać wsparcie dla Domino Directory |
| **18.** | System musi posiadać wsparcie dla LDAP |
| **19.** | System musi posiadać wsparcie dla Active Directory |
| **20.** | System musi posiadać wsparcie dla Microsoft Exchange |
| **21.** | System musi posiadać wsparcie dla Lotus Domino |
| **22.** | System musi posiadać wsparcie dla ActiveSync, POP, IMAP |
| **23.** | System musi posiadać możliwość konfiguracji ACL dla konsoli |
| **24.** | System musi mieć możliwość zmiany motywów konsoli (główny kolor, logo, favicon) |
| **25.** | System musi mieć możliwość uwierzytelniania dwuskładnikowego dla konsoli |
| **26.** | System musi mieć możliwość audytu integralności danych i bezpieczeństwa serwera |
| **27.** | System musi mieć możliwość automatycznej i manualnej aktualizacji serwera |
| **28.** | System musi wspierać min. systemy operacyjne:   * Android 5.0.1 lub nowszy * Samsung KNOX 2.3 lub nowszy * iOS 10.3 lub nowszy * Windows 10 Pro |
| **29.** | System musi wspierać rejestracje urządzeń za pomocą:   * App + kod – Rejestracja urządzeń poprzez aplikacje za pomocą loginu i hasła, kodu QR lub SMS. * Autoenrollment – Rejestracja bez potrzeby podawania poświadczeń. * Enterprise QR Code – Rejestracja przez kod QR dostępny z poziomu ekranu „Witaj”. * Native – Rejestracja poprzez natywne ustawienia urządzenia. |
| **30.** | System musi mieć możliwość zbierania informacji o zarejestrowanych urządzeniach takie jak:   * Pamięć wewnętrzna * RAM * Procesor * Operator * Roaming * Język urządzenia * Szyfrowanie urządzenia * IP sieci komórkowej * IP sieci Wi-Fi * Adres MAC sieci Wi-Fi * SSID sieci Wi-Fi * Rozdzielczość ekranu * ICCID 1 / ICCID 2 * Numer telefonu * IMEI 1 / IMEI 2 * Numer seryjny * Ostatni kontakt * Status (online/offline) * Karta SD * Aplikacje na urządzeniu * Alias urządzenia * Użytkownik urządzenia * Raport wykorzystania pamięci * Raport wykorzystania danych mobilnych * Raport wykorzystania danych przez Wi-Fi * Raport wykorzystania aplikacji * Informacja o nadanym uprawnieniu do rysowania po aplikacjach |
| **31.** | System musi mieć możliwość zdalnego zarządzania urządzeniami. Minimalne akcje i konfiguracje urządzeń:   * Blokada urządzenia * Wykonanie zdjęcia podczas blokady urządzenia * Lost Mode * Zdalny pulpit * Zdalny pulpit z możliwością kontroli urządzenia z konsoli * Reset hasła * Zmiana hasła * Przywrócenie do ustawień fabrycznych * Usunięcie danych służbowych * Zablokowanie ekranu * Wysłanie notyfikacji * Wyświetlenie dialogu * Wysłanie alarmu * Przekierowanie połączeń * Odświeżenie urządzenia * Restart urządzenia * Sprawdzenie statusu (online/offline) * Eksport SMS * Eksport kontaktów * Eksport dziennika połączeń * Eksport logów audytowych * Lokalizacja urządzenia na żądanie * Lokalizacja urządzenia w interwałach czasowych * Lokalizacja urządzenia w ruchu * Historia lokalizacji urządzenia * Ograniczenia czasowe dla lokalizacji * Zablokowanie / odblokowanie aplikacji na urządzeniu * Uruchomienie aplikacji na urządzeniu * Wysłanie konfiguracji aplikacji na urządzeniu * Usunięcie aplikacji z urządzenia * Backup SMS / MMS * Backup kontaktów * Backup dziennika połączeń * Instalacja aplikacji * Instalacja aplikacji z pliku * Aktualizacja aplikacji z pliku * Dodawanie i instalowanie aplikacji z pliku w różnych wersjach * Cicha instalacja aplikacji * Instalacja skonfigurowanej aplikacji * Zarządzanie uprawnieniami aplikacji * Firmowy sklep z aplikacjami * Włączenie Activation Lock * Wyłączenie Activation Lock * Konfiguracja ActiveSync * Konfiguracja ActiveSync z szyfrowaniem S/MIME * Konfiguracja IMAP/POP * Konfiguracja Wi-Fi * Konfiguracja Enterprise Wi-Fi * Blokada usuwania dodanych sieci Wi-Fi * Konfiguracja SCEP * Dostarczenie certyfikatu * VPN * VPN per aplikacja * Odblokowanie aplikacji domyślnych * Biała lista aplikacji * Ukrywanie aplikacji w ruchu * Blokowanie aplikacji w ruchu * Czarna lista aplikacji * Dostarczenie kontaktów służbowych * Dostarczenie dokumentów służbowych * Konfiguracja tapety ekranu głównego * Konfiguracja tapety ekranu blokady * Konfiguracja APN * Tryb kiosk – pojedyncza aplikacja * Tryb kiosk – wiele aplikacji * Tryb kiosk – wiele aplikacji z logowaniem użytkownika * Personalizacja trybu kiosk (ekran główny, ikona, ułożenie aplikacji) Konfiguracja MTP * Geofencing * Biała lista kodów MNC i MCC dla usług łączności * Biała lista krajów dla usług łączności * Biała lista kontaktów * Integracja z Android Enterprise * Integracja z Android ZeroTouch * Integracja z Apple Business Manager * Integracja z Apps & Books * Wsparcie dla Custom Apps * Integracja z Knox Mobile Enrollment * Wsparcie dla OEM Config * Wsparcie dla Factory Reset Protection * Zarządzanie Play Protect * Ustawienie wymagań minimalnych hasła * Ustawienie wymagań minimalnych hasła w przestrzeni służbowej * Wymuszanie skomplikowanego hasła * Pozwalaj na użycie biometrii do odblokowania urządzenia * Pozwalaj na użycie biometrii do odblokowania przestrzeni służbowej Wiadomość na zablokowanym ekranie * Zablokuj Bluetooth * Zablokuj wykrywanie przez Bluetooth * Zablokuj możliwość konfiguracji sieci komórkowej * Wykrywanie i reagowanie statusu Root: Dangerous * Wykrywanie i reagowanie statusu Root: Critical * Wykrywanie i reagowanie na wypalony Knox Warranty Bit * Wykrywanie i reagowanie na włączone debugowanie przez USB * Wykrywanie i reagowanie na brak zaszyfrowania urządzenia * Wykrywanie i reagowanie na włączone opcje developerskie * Wykrywanie i reagowanie na podatność BlueBorne * Wykrywanie i reagowanie na wyłączony SELinux * Wykrywanie i reagowanie na niezaufanych administratorów * Wykrywanie i reagowanie na instalacje niedozwolonej aplikacji * Wykrywanie i reagowanie na połączenie do niezabezpieczonej sieci Wi-Fi * Wykrywanie i reagowanie na podłączenie do sieci podszywającej się pod sieć firmową * Wykrywanie i reagowanie na zmianę konfiguracji DNS * Wykrywanie i reagowanie na zmianę konfiguracji proxy * Wykrywanie i reagowanie na zmianę konfiguracji gateway * Blokowanie trybu samolotowego * Zablokowanie danych mobilnych w roamingu * Zablokowanie tetheringu i mobilnych hotspotów * Zablokowanie nowych konfiguracji Wi-Fi * Konfiguracja Wi-Fi w trybie uśpienia * Zablokowanie konfiguracji VPN przez użytkownika * Zablokowanie podłączania nośników fizycznych * Zablokowanie usuwanie użytkowników * Zablokowanie połączeń wychodzących * Zablokowanie SMS * Zablokowanie transferu plików przez USB * Automatyczne ustawienie czasu * Automatycznie ustawienie strefy czasu * Ustawianie metody wprowadzania danych * Ustawianie usług dostępności * Domyślny launcher * Zarządzanie usługami lokalizacji * Pozwalaj odinstalowywać aplikacje * Ustawianie sposobu nadawania uprawnień * Aktualizacja aplikacji ze sklepu Google Play * Zablokowanie dodawanie użytkowników * Zablokowanie zrzutów ekranu * Zablokowanie opcji developerskich * Zablokowanie safe boot * Zablokowanie przywracania do ustawień fabrycznych * Zablokowanie czyszczenie danych aplikacji * Zablokowanie dodawania konta Google * Zablokowanie instalowanie aplikacji z nieznanych źródeł * Ustawienie maksymalnego czasu nieaktywności * Wymuszanie cyklicznego połączenia urządzenia z serwerem * Wykonaj akcje w przypadku przekroczenia czasu nieaktywności * Zablokowanie Smart Lock * Zablokowanie NFC * Zablokowanie WiFi Direct * Zablokowanie WAP push w roamingu * Zablokowanie OTG przez USB * Zablokowanie mikrofonu * Zablokowanie nagrywania audio * Zablokowanie wysyłanie crash report do Google * Zablokowanie zmian tapety * Zablokowanie cookies * Zablokowanie JavaScript * Zablokowanie popupów * Zablokowanie Google Play * Wymuszanie szyfrowania urządzenia * Zablokowanie aktualizacji systemu operacyjnego * Zablokowanie firmware recovery * SIM pinning * Zablokowanie S Voice * Zablokowanie usług Android backup * Zablokowanie FaceTime * Zablokowanie zrzutów ekranu i nagrywania ekranu * Zablokowanie AirDrop * Zablokowanie iMessage * Zablokowanie usług Apple Music * Zablokowanie usługi radio * Zablokowanie głosowego wybierania numeru na zablokowanym ekranie Zablokowanie Siri * Zablokowanie iBooks * Zablokowanie zakupów w aplikacji * Zablokowanie hasła iTunes podczas zakupów * Zablokowanie iCloud backup * Zablokowanie synchronizacji dokumentów w iCloud * Zablokowanie Keychain w iCloud * Zablokowanie backupu iCloud aplikacji zarządzanych * Zablokowanie backupu służbowych książek * Zablokowanie dzielenia zdjęć z iCloud * Zablokowanie biblioteki zdjęć z iCloud * Zablokowanie My Photo Stream * Wymuszanie ograniczonego śledzenia reklam * Zablokowanie niezaufanych certyfikatów TLS * Zablokowanie instalacji profili konfiguracyjnych * Zablokowanie modyfikowanie kont * Zablokowanie zmiany nazwy urządzenia * Zablokowanie konfiguracji Find My Friends * Zablokowanie zmian notyfikacji * Zezwalaj otwierać dokumenty z niezarządzanych źródeł w zarządzanych aplikacjach * Zezwalaj otwierać dokumenty z zarządzanych źródeł w niezarządzanych aplikacjach * Zablokowanie zarządzania AirDrop * Zablokowanie Handoff * Zablokowanie wyników wyszukiwania z Internetu w Spotlight * Zablokowanie danych diagnostycznych Apple * Zablokowanie wykrywania Apple Watch * Zablokowanie parowanie Apple Watch * Zablokowanie klawiatury predykcyjnej * Zablokowanie skrótów klawiszowych * Zablokowanie autokorekty * Zablokowanie sprawdzania pisowni * Zablokowanie Define * Zablokowanie notyfikacji Wallet na ekranie blokady * Zablokowanie Control Center na ekranie blokady * Zablokowanie Notification Center na ekranie blokady * Zablokowanie widoku Today na ekranie blokady * Zablokowanie AirPrint * Zablokowanie przechowywania poświadczeń AirPrint * Zablokowanie wykrywania iBeacon w AirPrint * Zablokowanie dyktowania * Zablokowanie modyfikacji eSIM * Zablokowanie autouzupełniania haseł * Opóźnienie aktualizacji systemu operacyjnego * Wymagaj autentykacji przed autouzupełnianiem haseł * Wymuszanie korzystania z WiFi * Zablokowanie iTunes * Zablokowanie News * Zablokowanie Podcasts * Zablokowanie Game Center * Zablokowanie Safari * Konfiguracja Safari * Zablokowanie App Store * Zablokowanie klawiatury QuickPath * Zablokowanie dostępu Files do dysków sieciowych * Zablokowanie dostępu Files do dysków USB * Zablokowanie Find My Device * Zablokowanie Find My Friends * Zablokowanie usuwania aplikacji systemowych * Ustawienie dostępnych treści * Filtrowanie treści w Safari * Dostosowywanie Dex * Zarządzanie klawiaturą Samsung * Konfiguracja Quick Panel * Dostosowywanie ekranu blokady * Konfiguracja firewall * Manualna konfiguracja proxy * Proxy auto-config (PAC) * Konfiguracja UCM plugin * Białe i czarne listy kont * Zarządzanie aktualizacjami systemu operacyjnego * Wykonywanie własnych skryptów * Zarządzanie BitLocker * Pozwalaj na App Clips * Pozwalaj na spersonalizowane reklamy Apple * Dodanie użytkownika do urządzenia * Odjęcie użytkownika z urządzenia |
| **31.** | Wdrożenie zaoferowanego Systemu w modelu HA i architekturze z podziałem na osobne instancje (z serwerami w DMZ i w LAN) w terminie 30 dni od daty podpisania umowy.  W ramach wdrożenia wykonane zostaną następujące czynności:  - Analiza ustaleń i przygotowanie projektu konfiguracji fizycznej i logicznej  - Konfiguracja wirtualnych serwerów w infrastrukturze zamawiającego  - Instalacja i konfiguracja elementów systemu  - Konfiguracja funkcjonalności ustalonych z Zamawiającym  - Dodanie 5 urządzeń Zamawiającego do systemu  - Testy poprawnego działania systemu  - Wykonanie dokumentacji powykonawczej wraz z procedurami disaster recovery |
| **32.** | Przygotowanie i przeprowadzenie warsztatów z administracji Systemem dla 3 administratorów i 4 operatorów Zamawiającego w terminie uzgodnionym z Zamawiającym lecz nie dłuższym niż 10 dni roboczych od daty wdrożenia zaoferowanego Systemu.  Warsztaty muszą być przeprowadzone w języku polskim.  Dla każdego uczestnika warsztatów muszą zostać dostarczone materiały szkoleniowe w postaci elektronicznej. |
| **33** | Wdrożenie zaoferowanego Systemu oraz warsztaty z administracji Systemu muszą być wykonane przez inżynierów posiadających ważne certyfikaty wystawione przez producenta Systemu. |
| **34** | W ramach realizacji przedmiotu zamówienia Wykonawca dla dostarczonego Systemu będzie świadczył usługi wsparcia technicznego na rzecz Zamawiającego |
| **35** | W ramach usług wsparcia technicznego Zamawiający ma prawo do:   * nieograniczonej ilości zgłoszeń serwisowych; * przeprowadzenia nieograniczonej liczby konsultacji technicznych przez pracownika serwisu producenta Systemu lub autoryzowanego przedstawiciela producenta Systemu; * konsultacji technicznych świadczonych w dni robocze, w godzinach od 8:00 do 18.00 telefonicznie pod wskazanym numerem telefonu, wskazanym adresem e-mail oraz w sesji zdalnego połączenia; * dostępu do poprawek i uaktualnień Systemu objętego usługą wsparcia * dostępu do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta System * obsługi zgłoszeń w okresie wsparcia technicznego świadczonej w języku polskim |
| **36** | W terminie 10 dni roboczych od daty podpisania umowy Wykonawca dostarczy Zmawiającemu dokument potwierdzający nabycie prawa przez Ministerstwo Rozwoju, Pracy i Technologii do usług wsparcia technicznego przez producenta Systemu na poziomie odpowiadającym wymaganiom określonym w niniejszym załączniku przez okres 36 miesięcy. |
| **37** | W ramach usług wsparcia technicznego Zamawiający będzie miał prawo do zgłoszeń usterek. Przez usterkę rozumie się awarię/nieprawidłowe działanie Systemu.   1. Zgłoszeń usterek Zamawiający będzie dokonywać w dni robocze tj. od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w godzinach od 8.00 do 16.00. 2. Zgłoszenie o wystąpieniu danego zdarzenia, awarii/nieprawidłowego działania Systemu będzie polegało na telefonicznym lub mailowym powiadomieniu na wskazany przez Wykonawcę nr telefonu lub adres e-mail. 3. Zamawiający w zgłoszeniu usterki przekaże Wykonawcy, na wskazany przez niego adres e-mail, informację dotyczącą zdarzenia. wraz z określeniem priorytetu usterki zgodnie z następującymi definicjami: 4. błąd krytyczny - błąd powodujący brak dostępności Systemu, mający krytyczny wpływ na systemy Zamawiającego; 5. błąd poważny – błąd nie powodujący braku dostępności Systemu, Ma wpływ na główną funkcjonalność lub występuje znaczące obniżenie wydajności mający bardzo duży wpływ na systemy Zamawiającego; 6. błąd niewielki – błąd nie powodujący braku dostępności Systemu, występuje częściowa, niekrytyczna utrata możliwości korzystania z usługi, która ma średni lub niski wpływ na systemy Zamawiającego, 7. Wykonawca potwierdzi na adres mailowy przyjęcie zgłoszonej usterki. Czas reakcji Wykonawcy na zgłoszenie usterki wynosi o priorytecie:    1. błąd krytyczny - maksymalnie do 30 minut;    2. błąd poważny - maksymalnie do 2 godzin roboczych;    3. błąd niewielki - maksymalnie do 4 godzin roboczych. 8. Wykonawca po dokonaniu naprawy/zamknięciu zgłoszenia przekaże Zamawiającemu na wskazany przez niego adres mailowy podsumowanie wykonanych czynności/napraw. W terminie 1 dnia roboczego od dnia przekazania informacji o dokonaniu naprawy, o której mowa w zdaniu poprzedzającym, Zamawiający dokona odbioru naprawy usterki lub zawiadomi Wykonawcę o zastrzeżeniach do realizacji naprawy usterki. Za wystarczające uznaje się formę elektronicznego powiadomienia na wskazany przez Wykonawcę adres mailowy. 9. Naprawy usterek o priorytecie:    1. błąd krytyczny       1. wstępne rozwiązanie problemu/tymczasowa propozycja obejścia problemu – następować będą w ciągu 8 godzin roboczych;       2. ostateczne rozwiązanie problemu – 24 godziny robocze;    2. błąd poważny       1. wstępne rozwiązanie problemu/ tymczasowa propozycja obejścia problemu – następować będą w ciągu 8 godzin roboczych;       2. ostateczne rozwiązanie problemu – 5 dni roboczych ;    3. błąd niewielki       1. wstępne rozwiązanie problemu/ tymczasowa propozycja obejścia problemu – następować będą w ciągu 3 dni roboczych;       2. ostateczne rozwiązanie problemu – w następnej wersji oprogramowania lub w uzgodnionym z Zamawiającym czasie.   Wyjątkiem są potwierdzone błędy krytyczne, poważne i niewielkie producenta oprogramowania, gdzie czas naprawy może być dłuższy niż określony w ppkt 1-3  zdania poprzedniego i zostanie uzgodniony przez Strony w każdym przypadku zgłoszonej usterki oprogramowania.  Przez czas naprawy usterki rozumie się okres od momentu upłynięcia terminu czasu reakcji na zgłoszenie usterki o określonym przez Zamawiającego priorytecie, o którym mowa pkt. 4, do momentu przywrócenia pierwotnie normatywnych funkcjonalności i efektywności działania systemu. |
| **38** | Wykonawca zapewni świadczenie usługi wsparcia technicznego z najwyższą starannością, z aktualnym poziomem wiedzy technicznej, przy wykorzystaniu wiedzy i doświadczeniu. |

Definicje:

**Dzień roboczy -** Dni pracy Zamawiającego, od poniedziałku do piątku w godz. 8:00-

16:00 z wyłączeniem dni ustawowo wolnych od pracy w Polsce.

**Godzina robocza -** Godziny od 8:00 do 16:00 w Dni robocze.

**System**  - systemu do zarządzanie urządzeniami mobilnymi on-premise**.**