SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

„Zakup smartfonów wraz z systemem zarządzania”

1. Wymagania Ogólne.

Przedmiotem zamówienia jest zakup smartfonów wraz z systemem zarządzania w ramach projektu „Cyfrowego Obserwatorium Bezpieczeństwa Województwa Śląskiego – Śląska Policja Bliżej Społeczeństwa”. Zamówienie obejmuje sprzedaż i dostarczenie do lokalizacji wskazanych w zał. nr 4 do SIWZ fabrycznie nowych smartfonów wraz z akcesoriami oraz licencją Systemu MDM AirWatch Vmware Blue Management Suite lub równoważną (spełniającą poniższe wymagania) w ilościach 1120 sztuk.

2. Szczegółowy opis przedmiotu zamówienia

W ramach zamówienia Wykonawca:

- dostarczy na własny koszt smartfony wraz z licencją na system zarządzania oraz podstawowym 60 miesięcznym wsparciem (przez wsparcie Zamawiający rozumie: możliwość korzystania z pomocy technicznej w godzinach od 8.00 do -16.00 od poniedziałku do piątku w formie telefonicznej lub przez www, możliwość aktualizacji systemu, dostęp online do bazy wiedzy dotyczącej systemu. Liczba żądań pomocy technicznej ma być nieograniczona)
- Przeprowadzi szkolenie dla 6 administratorów systemu zarządzania w siedzibie Zamawiającego. Czas szkolenia 12 godzin rozłożone na 2 dni robocze po 6 godzin. Materiały szkoleniowe oraz sprzęt potrzebny do szkolenia zapewni Wykonawca .

Wykonawca określi:
- cenę jednostkową dostarczanych smartfonów (wraz z akcesoriami).
- cenę jednostkową licencji Systemu MDM.

3. Wymagania dotyczące zamawianego smartfonu:

- 1120 sztuk o równoważnych lub lepszych parametrach niż:

Lp.	Parametry wymagane:	
1	**Procesor**	Minimum 4 rdzenie, minimum 1.40 GHz
2	**Pamięć RAM**	Minimum 2 GB
3	**Pamięć wbudowana**	Minimum16 GB
4	**Przekątna ekranu**	Od 4,9" do 5,7"
5	**Rozdzielczość ekranu**	1280 x 720 lub większa
6	**Łączność**	Bluetooth Wi-Fi dwuzakresowe 2,4 i 5 GHz 4G (LTE) NFC
7	**System nawigacji satelitarnej**	GPS, A-GPS, GLONASS
8	**Złącza**	Gniazdo kart SIM – rozmiar dowolny (Mini/micro/nano) Czytnik kart pamięci Wyjście słuchawkowe/głośnikowe Micro USB lub USB 2.0 Typ C
9	**Bateria**	Litowo-jonowa minimum 2800 mAh
10	**Zainstalowany system operacyjny**	Android w wersji minimum 7.0 Nougat w języku polski

11	**Aparat**	Minimum 13.0 Mpix - tył minimum 5.0 Mpix - przód
12	**Lampa błyskowa**	Wbudowana
13	**Rozdzielczość nagrywania wideo**	Minimum 1920 x 1080 (FullHD)
14	**Kolor**	Zachowana ciemna tonacja
15	**Dodatkowe informacje**	Pyłoszczelność i wodoszczelność - standard IP68 Czujnik światła Czujnik zbliżenia Akcelerometr
16	**Dołączone akcesoria kompatybilne z zaoferowanym telefonem**	**Ładowarka sieciowa**, **Kabel do połączenia z komputerem,** **Słuchawki douszne przewodowe z wbudowanym mikrofonem oraz regulacją głośności**, Kolor: czarny lub zachowana ciemna tonacja **Instrukcja obsługi w języku polskim**, **Ładowarka samochodowa** o parametrach: Wejście: 12V Wyjście: nie mniej niż 5V przynajmniej jedno gniazdo USB z wydolnością prądową nie mniejszą niż 2000mA Kolor: czarny lub zachowana ciemna tonacja **Kabel łączący ładowarkę samochodową ze smartfonem** Długość przewodu: od 0.9 m do 1,35 m. Przewód ma umożliwiać ładowanie urządzenia bez spadku napięcia przy prądzie 2000mA. Nie może być to ten sam kabel, który będzie służył do połączenia smartfonu z komputerem. Kabel ma być łączony z ładowarką samochodową za pomocą złącza USB. Kolor: czarny lub zachowana ciemna tonacja **Karta pamięci:** Pojemność: minimum 32 GB Prędkość zapisu 20 MB/s lub większa Prędkość odczytu do 80 MB/s lub większa **Szkło ochronne :** Wykonane z hartowanego szkła o twardości 9H Zaokrąglone brzegi Grubość do 0.4mm Szkło ochronne musi zostać naklejone na dostarczony smartfon przez Wykonawcę. Nie może być widocznych na nim tzw. pęcherzyków powietrza oraz śladów odklejania się szkła ochronnego na jego brzegach. Cała powierzchnia szkła powinna jednolicie przylegać do ekranu dotykowego telefonu. **Etui/futerał z klapką na magnes:** (klapka otwierana z góry ku dołowi) Futerał musi posiadać wszystkie niezbędne wycięcia na przyciski, aparat i złącza systemowe, by móc w pełni korzystać z telefonu bez żadnych ograniczeń. Ma być dedykowany pod konkretny model telefonu. Musi posiadać specjalne magnesy zabezpieczające przed niepożądanym otwarciem przedniej klapki. Kolor czarny. Wewnątrz musi znajdować się specjalne mocowanie dostosowane do dostarczonego smartfona. **Uchwyt samochodowy**

		Mocowany do szyby Kolor: czarny lub zachowana ciemna tonacja
17	**Gwarancja na telefon**	60 miesięcy
18	**Gwarancja na akcesoria**	24 miesiące z wyłączeniem baterii na które Zamawiający żąda 12 miesięcy
19	**Wymagania dodatkowe**	-smartfony bez blokady SIMLOCK -smartfony muszą pochodzić z autoryzowanego kanału sprzedaży producenta na rynek Unii Europejskiej.
20	**Parametry pożądane:**	
21	Odporność na wstrząsy i upadki standard MIL-STD-810G	
22	Wymienna bateria	

4. Wymagania dotyczące zamawianego systemu do zarządzania smartfonami:

1120 sztuk licencji Systemu MDM AirWatch Vmware Blue Management Suite wraz z podstawowym wsparciem w okresie 60 miesięcy od dnia podpisania protokołu końcowego odbioru licencji.

W przypadku złożenia oferty z innym systemem niż wskazany powyżej Wykonawca zobowiązany będzie do dostarczenia wnioskowanej liczby licencji oraz do przebudowy całego systemu centralnego wraz z wymianą licencji użytkowanych przez inne jednostki Policji (około 350) oraz rekonfiguracją pracujących urządzeń mobilnych, zapewniając czas niedostępności systemu nie dłuższy niż 24 godziny. Wykonawca zapewni 24 miesięczną gwarancję na system z 60 miesięcznym wsparciem.

System do zarządzania urządzeniami mobilnymi musi posiadać następujące funkcjonalności:

1. **System zarządzania urządzeniami mobilnymi:**

1.1 Wszystkie składniki platformy pochodzą od jednego producenta i są zarządzane z jednej spójnej konsoli zarządzającej;

1.2 Produkt oferowany jest z licencjami wieczystymi (Perpetual). Licencja jest przypisana na stałe do konkretnego urządzenia, a po jego usunięciu oferuje możliwość jej powtórnego wykorzystania w celu rejestracji nowego terminala/urządzenia;

1.3 Oferowane licencje po zakupie przechodzą na własność – licencje wieczyste (Perpetual) i umożliwiają instalacje w środowisku Klienta;

1.4 Produkt umożliwia wdrożenie reguł bezpieczeństwa na urządzeniach mobilnych (zarządzanie urządzeniami mobilnymi);

1.5 W ramach wdrożenia systemu zarządzania urządzeniami mobilnymi, zapewniane jest przeszkolenie administratorów

2. **Lokalizacja infrastruktury wraz z wymaganiami dla systemu zarządzania urządzeniami mobilnymi:**

2.1 Środowisko fizyczne:

2.1.1 System ma zostać zainstalowany w istniejącej infrastrukturze wirtualizującej KGP;

2.1.2 System zapewnia pełne wsparcie technologii wirtualnych maszyn w zakresie platformy wirtualizacyjnej Zamawiającego (brak sprzętowych appliance'ów);

2.2 Integracja z systemami będzie obejmowała:

2.2.1 Integrację z usługami katalogowymi: IBM Domino Directory;

2.2.2 Integracja Systemu z systemem poczty elektronicznej z wykorzystaniem funkcjonalności proxy/relay dla kont pocztowych umożliwiających kontrolę przepływu wiadomości email oraz implementację dodatkowych mechanizmów bezpieczeństwa poczty elektronicznej;

2.2.3 System umożliwia integrację z produktem ISE firmy Cisco, a w szczególności:

2.2.3.1 Ma możliwość zbierania informacji: nazwa urządzenia, system operacyjny, wersja systemu operacyjnego, MAC adres urządzenia, sposób podłączenia do sieci (przewodowy i bezprzewodowy), IMEI, Serial numer.

2.2.3.2 Ma możliwość sprawdzenia statusu zgodności urządzenia według określonego interwału czasowego, ma możliwość sprawdzenia czy system posiada zainstalowany system antywirusowy, sprawdzi stan szyfrowania dysku na urządzeniu.

2.2.3.3 Ma możliwość na podstawie danych zebranych z systemu na zdalne zablokowanie urządzenia, przywrócenie urządzenia do danych fabrycznych, wyczyszczenie urządzenia z danych firmowych.

2.2.3.4 System ma umożliwić produktowi ISE firmy Cisco na podstawie zebranych z systemu danych, przekierowywanie urządzeń do odpowiednich podsieci w przypadku, gdy:

2.2.3.4.1. Urządzenie nie jest zarejestrowane do systemu a użytkownik chce podłączyć się do sieci firmowej zostanie automatycznie przekierowany do portalu rejestracji urządzenia

2.2.3.4.2 Urządzenie jest niezgodne zostanie automatycznie przekierowane do sieci, w której użytkownik ma dostęp tylko do Internetu, a użytkownikowi i administratorowi zostanie wysłane automatyczne powiadomienie e-mail lub SMS.

2.2.3.4.3 Urządzenie jest zgodne z zasadami bezpieczeństwa to użytkownikowi zostanie udostępniony odpowiedni udział sieciowy

2.2.4 Produkt integruje się z Microsoft PKI, z wykorzystaniem mechanizmów SCEP oraz DCOM;

2.2.5 Produkt wymaga aby uwierzytelnienie do kont pocztowych odbywało się za pomocą certyfikatu dystrybuowanego za pomocą systemu;

2.2.6 Produkt oferuje możliwość implementacji oprogramowania zapewniającego funkcję terminowania szyfrowanych połączeń od aplikacji, które wspierają funkcje szyfrowania i bezpiecznego przesyłania danych;

2.2.7 Wszystkie komponenty Systemu zarządzania dla platform z systemem operacyjnym Android są zaimplementowane we własnej infrastrukturze bez konieczności komunikacji z zewnętrznymi systemami/usługami np. GoogleMassaging;

2.2.8 Produkt zaimplementowany w środowisku Klienta pracuje bez konieczności komunikacji z infrastrukturą teleinformatyczną umieszczoną w zasobach producenta;

2.2.9 Produkt umożliwia testowe instalacje oprogramowania np. do testowania aktualizacji oprogramowania Systemu przed jej instalacją w środowisku produkcyjnym;

2.2.10 Architektura Systemu może być wyskalowana w sposób umożliwiający zwiększenie ilości użytkowników bez rozbudowy sprzętu;

3. **Wymagania dla architektury:**

3.1 System zapewnia możliwość instalacji wszystkich jego komponentów w infrastrukturze serwerowej, bez konieczności komunikacji z infrastrukturą umieszczoną w zasobach producenta Systemu;

3.2 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, (Determilitarized zone);

3.3 System umożliwia rozbudowę do wysokiej dostępności (HA) poprzez redundancję każdego jego elementów;

3.4 System zapewnia możliwość instalacji poszczególnych jego komponentów systemu w środowisku wirtualnym Vmware vSphere;

4. Wymagania dla zarządzania urządzeniami mobilnymi:

4.1 System Zapewnia obsługę urządzeń pracujących pod kontrolą systemów operacyjnych.

4.1.1 System umożliwia zarządzanie systemami operacyjnymi: Android (min. 5.x), iOS(min. 9.X), Windows Phone(min. 8.x) Windows (min 10.x), Apple OSX Sierra(v.10.12) Windows Mobile;

4.1.2 Podstawowe typy urządzeń mobilnych do zarządzania: smartfony, IPhone, IPady, MacBook'i, terminale logistyczne, tablety, telefony komórkowe;
4.2 System zapewnia zapis informacji o urządzeniu:
4.2.1 Nazwa urządzenia
4.2.2 Numer UDID, IMEI/MEID, IMSI
4.2.3 Nazwa producenta urządzenia, model
4.2.4 Numer seryjny urządzenia
4.2.5 Wersja systemu operacyjnego urządzenia
4.2.6 Lista aplikacji zainstalowanych z wyszczególnieniem typu, wersji, rozmiaru
4.2.7 Wykrywanie statusu złamania zabezpieczeń systemu operacyjnego urządzenia mobilnego tzw. Jailbreak lub rooted,
4.2.8 informacje na temat zajętości pamięci oraz pojemności baterii
4.2.9 możliwość śledzenia położenia urządzenia bazując na informacji z odbiornika GPS i BT
4.3. Zarządzanie odbywa się z poziomu centralnej konsoli zarządzającej zawierającej funkcjonalności:
4.3.1. Dostęp do konsoli z wykorzystaniem szyfrowanego połączenia SSL poprzez przeglądarkę internetową,
4.3.2. Transmisja (w tranzycie) dokumentów poprzez zaszyfrowane połączenie (AES-256 SSL)
4.3.3. Konfiguracja uprawnień z wykorzystaniem zdefiniowanych ról w systemie MDM
4.3.4. Możliwość logicznego podziału systemu z zachowaniem pełnej odrębności ustawień oraz komponentów z możliwością przypisania do każdej z nich dedykowanego administratora (ang. multi-tenant)
4.3.5. Definiowanie grup użytkowników oraz przypisanie różnych polis bezpieczeństwa/uprawnień dla każdej z grup z osobna,
4.3.6. Definiowanie alertów i powiadomień dla administratorów
4.3.7. Wysyłanie powiadomień/komunikatów na urządzenie mobilne,
4.3.8. Polska wersja konsoli operatorskiej
4.4. System zapewnia dedykowany samoobsługowy portal dla użytkowników systemu zapewniający funkcjonalności:
4.4. 1. Dostęp do portalu użytkownika powinien być realizowany poprzez przeglądarkę WWW z wykorzystaniem bezpiecznego połączenia SSL
4.4. 2. Portal użytkownika powinien być dostępny w polskiej wersji językowej z możliwością dostosowania kolorystyki oraz znaków firmowych zgodnie z wymaganiami.
4.4.3. Samodzielne resetowanie hasła dostępu do urządzenia,
4.4.4. Samodzielne blokowanie urządzenia,
4.4.5. Wysyłanie wiadomości push na własne urządzenie mobilne,
4.4.6. Wyświetlanie położenia urządzenia na mapie bazując na danych z GPS lub BST
4.4.7. Kasowanie danych i ustawień firmowych (tzw. enterprise wipe)
4.4.8. Zerowanie urządzenia – przywrócenie urządzenia do ustawień fabrycznych (tzw. device wipe)
4.4.9. Wyświetlanie listy zainstalowanych profili oraz aplikacji na urządzeniu mobilnym,
4.4.10. Konfigurowanie przez administratora systemu do jakich opcji ustawień portalu samoobsługowego mają dostęp użytkownicy – z przydziałem takich praw dla grup użytkowników/urządzeń
4.4.11. Możliwość samodzielnego rejestrowania urządzeń
4.4. 2. Możliwość uzyskiwania informacji o audytach zgodności, zainstalowanych i profilach
4.4.13. Dostęp do wybranych aplikacji
4.4.14. Uzyskanie wsparcia technicznego

5. System udostępniania plików i ich współdzielenie:

5.1. System udostępniania i współdzielenia plików i folderów może być zaimplementowany w wewnętrznej infrastrukturze organizacji bez konieczności komunikacji z chmurą usługową producenta systemu
5.2. System posiada bezpieczną architekturę pozwalającą na rozdział funkcjonalny umożliwiający wyniesienie modułów sytemu do strefy DMZ oferujących usługi bezpiecznego dostępu dla komputerów oraz urządzeń mobilnych znajdujących się poza sieci wewnętrzną

5.3. System umożliwia bezpieczny szyfrowany dostęp do plików oraz folderów znajdujących się w wewnętrznej infrastrukturze organizacji. Dostęp jest możliwy z każdego miejsca w tym z urządzeń znajdujących się poza infrastrukturą Organizacji (Internet). Realizacja bezpiecznego szyfrowanego dostępu do zasobów z sieci Internet jest realizowana na bazie mechanizmów i funkcjonalności Systemu bez konieczności stosowania dodatkowych rozwiązań szyfrujących pochodzących od innych dostawców. Możliwość ta dotyczy każdego sposobu dostępu do zasobów z komputerów czy urządzeń mobilnych.

5.4. System posiada możliwość wdrożenia w trybie wysokiej dostępności zapewniającej redundancje elementów sytemu.

5.5 System posiada możliwość zainstalowania poszczególnych komponentów systemu na środowisku wirtualnym Vmware

5.6 Docelowo system powinien umożliwiać rozbudowę umożliwiającą dostęp do zasobów z np. 2000 urządzeń takich jak Windosw PC, MacOSx, Smartfon, Tablet, IOS, Android, urządzenia Windows Phone;

5.7 System umożliwia zakup licencji wieczystej z ponoszeniem rocznych kosztów serwisu producenta platformy;

5.8 Wszystkie komponenty produktu są dostarczone przez Wykonawcę

6. Funkcje zarządzania systemem udostępniania plików i ich współdzielenia

6.1. Zarządzanie systemem odbywa się z centralnej konsoli zarządzającej obsługiwanej przez przeglądarkę internetową z wykorzystaniem szyfrowanego połączenia SSL

6.2. System umożliwia definiowanie ról w systemie w celu umożliwienia podziału uprawnień administracyjnych

6.3. System umożliwia logiczny podział systemu z zachowaniem pełnej odrębności ustawień oraz komponentów z możliwością przypisania do każdej z nich dedykowanego administratora (ang. multi-tenant)

6.4. System umożliwia logiczny podział funkcjonalny pozwalający na integrację wydzielonych przestrzeni z odrębnymi domenami Active Directory.

6.5. System umożliwia definiowanie grup użytkowników oraz przypisywanie różnych polityk bezpieczeństwa/uprawnień dla każdej grupy z osobna

6.6 System umożliwia personalizację konsoli zarządzającej, portalu użytkownika oraz aplikacji na urządzeniach mobilnych pozwalającą na dostosowanie kolorystyki konsoli oraz zamieszczenie własnego logo oraz grafiki firmowej.

6.6.1 Zarządzanie systemami operacyjnymi urządzeń mobilnych: Windows (XP, Vista,7, 8.x,10) MacOSx, iOS (ver.4-9.x), Android(ver 2.2-5.x), Windows CE (5,6 i 7), Windows Mobile (5.x, 6.1, 6,5 Professional i Standard) Windows Embedded 6.5, Symbian (S60 3rd Edition, OS 9.3, FP1 and FP2, S60 5th Edition, OS 9,4), Chrome OS, Tizen

6.7 System dostępny jest w polskiej wersji językowej dotyczy to zarówno konsoli operatorskiej, portalu użytkownika oraz aplikacji dostępnych dla komputerów PC oraz urządzeń mobilnych;

7. Integracja z systemami zewnętrznymi systemu udostępniania plików i ich współdzielenia

7.1. System umożliwia synchronizację użytkowników z usługami katalogowymi: IBM Domino Directory, Active Directory, LDAP

7.2. System pozwala na pobieranie użytkowników oraz atrybutów z systemu Active Directory w trybie manualnym i automatycznym

7.3. System oferuje dostęp do zasobów plikowych i folderów umieszczonych na firmowych serwerach SharePoint 2007,2010, 2013, SharePoint Online (Office 365), Google Drive, One Drive, Box, file serwerach sieciowych (NFS)

7.4. System integruje się z innymi systemami służącymi do przechowywania i wymiany plików wykorzystujących otwarty standard CMIS(Content Management Interoperability Services)

7.5. System umożliwia przechowywanie danych w ramach osobistej przestrzeni dyskowej użytkowników na zewnętrznych serwerach oraz macierzach dyskowych z wykorzystaniem funkcji Remote File Storage oraz Network File Storage

7.6. System ma możliwość integracji z platformą typu EMM (Mobile Device Management) w zakresie automatycznej dystrybucji aplikacji, możliwości jej usunięcia, implementacji mechanizmów pojedynczego logowania (SSO) na urządzeniach mobilnych;

7.7 System raportuje zdarzenia do systemów monitoringu bezpieczeństwa klasy SIEM: ArcSight, Splunk, RSA enVision, IBM Q1Labs;

8. Dostęp do zasobów dla systemu udostępniania i współdzielenia plików:

8.1 System umożliwia dostęp do wewnętrznych zasobów umieszczonych na serwerach z komputerów Windows PC oraz z urządzeń mobilnych z systemami iOS, Android oraz Windows Phone

9. Aplikacja systemu udostępniania i współdzielenia plików dla urządzeń mobilnych oraz komputerów.

9.1. System wymiany plików oferuje możliwość dostępu do zasobów na serwerach firmowych oraz przestrzeni osobistej z urządzeń mobilnych z systemem operacyjnym Android, iOS, Mac OSX, Windows Phone 8.1 oraz z komputerów z systemem operacyjnym Windows 10, 7, 8,8.1 XP.

9.2. Wymiana danych pomiędzy urządzeniami użytkownika a serwerami firmowymi odbywa się z każdego miejsca (sieć wewnętrzna/Internet) i jest transmisją szyfrowaną np. SSL

9.3. Aplikacja przechowuje dane w formie zaszyfrowanej z wykorzystaniem mechanizmów klucza szyfrującego AES 256-bit

9.4. Dostęp do aplikacji może być chroniony loginem, hasłem dostępu użytkownika oraz dodatkowo dla urządzeń mobilnych zdefiniowanym PIN-em.

9.5. Aplikacja umożliwia dostęp do zasobów plikowych i folderów umieszczonych na serwerach Sharepoint 2007,2010, 2013, SharePoint Online (Office 365), Google Drive, One Drive, Box, file serwerach sieciowych (NFS)

9.6. Aplikacja pozwala na dostęp do plików oraz folderów osobistych oraz współdzielonych

9.7. Dla urządzeń mobilnych aplikacja daje możliwość otwierania oraz przeglądania plików o następujących popularnych formatach : xls, xlsx, ppt, pptx, doc, docx, pdf, rtf, png, jpg, bmp, gif, txt

9.8. Aplikacja dla platform Android oraz iOS umożliwia zapisywanie oraz edycję plików z pakietu MS Office (World, Excel, PowerPoint)

9.9. Aplikacja dla platform Android oraz iOS umożliwia umieszczanie plików wideo oraz zdjęć i ich zapisywanie w przestrzeni lokalnej, osobistej oraz współdzielonej

9.10. System umożliwia automatyczne wykasowanie danych umieszczonych w aplikacji w przypadku przekroczenia limitu błędnie wpisanego hasła

9.11. Aplikacja jest dostępna w polskiej wersji językowej

10. Wymagania dla zarządzanie aplikacjami

10.1. Instalowanie oraz usuwanie aplikacji na urządzeniach mobilnych

10.2. Blokowanie instalacji oraz dostępu do aplikacji ze sklepów (AppStore, Google Play, Mobile Store)

10.3. Tworzenie wewnętrznego sklepu z aplikacjami (tzw. Enterprise Store)

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

10.5. Tworzenie listy aplikacji dozwolonych do instalacji (tzw. biała lista)

10.6. Aplikacje zarządzane z Systemu muszą mieć możliwość instalacji zdalnej przez administratora systemu lub na żądanie użytkownika z dedykowanego sklepu wewnątrz firmowego stworzonego przez administratora systemu

10.7 System posiada integrację z systemem badania reputacji aplikacji (ang. App Reputation takimi jak Veracode i Palo Alto Networks WildFire, tak aby wszystkie informacje na temat badanej aplikacji dostępne były z poziomu konsoli zarządzającej;

10.8. System zapewnia narzędzia, które pozwalają zabezpieczać aplikacje mobilne. Narzędzia te pozwalają na zabezpieczenie aplikacji bez dodatkowej pracy programistów, a w szczególności pozwalają na:
  10.8.1. Uwierzytelnianie użytkownika
  10.8.2. Sprawdzanie statusu zgodności i ewentualne usunięcie aplikacji gdy urządzenie nie będzie zgodne z polityką bezpieczeństwa
  10.8.3. Dostęp do aplikacji za pomocą certyfikatu wgranego przez system MDM na urządzenie mobilne
  10.8.4. Tunelowanie aplikacji
  10.8.5. Zabezpieczą możliwość drukowania z poziomu aplikacji
  10.8.6. Zabronią przed możliwością kopiowania treści do innych aplikacji (tzw. Copy and Paste)

10.9. System zapewnia narzędzia które zostaną udostępnione developerom aplikacji i umożliwiają jeszcze lepszą integrację z systemem, a w szczególności pozwalają dla nowo powstałej aplikacji na:

10.9.1. Wymuszanie logowania do aplikacji za pomocą konta z systemu Active Directory, LDAP
10.9.2. Dostęp do aplikacji za pomocą certyfikatu wgranego na urządzenie mobilne
10.9.3. Sprawdzanie statusu zgodności i ewentualne usunięcie aplikacji w momencie niezgodności urządzenia z polityką bezpieczeństwa
10.9.4. Tunelowanie aplikacji w celu dostępu do wewnętrznych zasobów bez konieczności zestawiania połączenia VPN,
10.9.5. Automatyczne zestawienie połączenia VPN w momencie uruchomienia aplikacji,
10.9.6. Logowanie się do aplikacji za pomocą unikatowego hasła zdefiniowanego przez użytkownika systemu podczas rejestracji urządzenia (tzw. SSO – ang. Single Sign On),
10.9.7. Zablokowanie kopiowania treści do innych aplikacji (ang. Copy and Paste),
10.9.8. Zabronienie załączania jakichkolwiek plików gromadzonych przez aplikację w postaci załączników wiadomości poczty e- mail,
10.9.9. Otwieranie plików gromadzonych przez aplikację tylko w aplikacjach zabezpieczonych przez Platformę,

11. Wymagania dotyczące Bezpieczna przeglądarka

11.1. Możliwość blokowania natywnych przeglądarek WWW dostępnych na urządzeniach mobilnych

11.2. Przeglądarka dostarczona przez producenta Systemu umożliwia:
  11.2.1. Szyfrowane tunelowanie ruchu WWW do sieci wewnętrznej za pośrednictwem komponentów rozwiązania MDM
  11.2.2. Dostęp do wewnętrznych stron WWW (Intranet) bez konieczności zestawiania tunelu VPN przez dodatkowe aplikacje
  11.2.3. Automatyczne logowanie się do stron wewnętrznych na podstawie danych o loginie i haśle
  11.2.4. Kontrola i definiowanie stron do jakich użytkownicy mogą mieć dostęp
  11.2.5. Definiowanie i blokowanie dostępu do stron niepożądanych
  11.2.6. Organicznie działania przeglądarki tylko do 1 strony, tryb KIOSK
  11.2.7. Możliwość logowania się do przeglądarki w trybie Single Sign-On
  11.2.8. Ograniczenie możliwości drukowania oraz kopiowania stron otwartych za pomocą przeglądarki
  11.2.9. Bezpieczna przeglądarka powinna być integralną częścią systemu MDM i pochodzić od tego samego producenta co System

12. Wymagania do obsługi poczty elektronicznej

12.1 Produkt oferuje integrację z rozwiązaniem poczty elektronicznej IBM Lotus Notes

(wymagana jest integracja z systemem IBM Lotus Notes w wersji 8.5.3) oraz Microsoft Exchange 2010/2013/2016 z wykorzystaniem standardowych protokołów pocztowych SMTP, POP3, IMAP:

12.1.1 System ma możliwość integracji oraz raportowania do systemów monitoringu bezpieczeństwa klasy SIEM

12.1.2 Dostępna jest obsługa mechanizmów SAML (ang. Security Asserition Markup Language) wykorzystywanych do poświadczenia w uwierzytelnianiu i automatycznym przekazywaniu informacji o uprawnieniach użytkowników między systemami i aplikacjiami

12.2. System wspiera automatyczną konfigurację kont pocztowych w procesie rejestrowania do systemu bazując na rozwiązaniach: Exchange 2010/2013/2016 (ActiveSync), IBM Domino (ActiveSync) oraz z wykorzystaniem standardowych protokołów pocztowych SMTP, POP3, IMAP,

12.3. System obsługuje uwierzytelnianie się do konta pocztowego za pomocą certyfikatu osobistego wydanego przez dowolny PKI, otrzymanego w procesie rejestracji urządzenia do systemu,

12.4. Posiada funkcjonalność podpisywania i szyfrowania wiadomości email z wykorzystaniem certyfikatu użytkownika S/MIME

12.5. System umożliwia konfigurację dostępu do kont pocztowych IBM Lotu Notes oraz Microsoft Exchange ActiveSync w trybie proxy/relay w celu kontroli przepływu wiadomości email oraz implementacji dodatkowych mechanizmów bezpieczeństwa poczty elektronicznej, takich jak:

12.5.1. Wymuszenie zaszyfrowania załączników przed dostarczeniem ich do urządzenia mobilnego

12.5.2. Blokowania wysyłania/ odbierania załączników na urządzeniach mobilnych

12.5.3. Ograniczenia wielkości odbieranych oraz wysyłanych załączników

12.5.4. Blokowanie dostępu do wiadomości pocztowych w przypadku naruszenia, lub nie spełnienia zdefiniowanych polityk bezpieczeństwa przez urządzenie mobilne

12.5.5. Blokowanie dostępu do systemu pocztowego dla urządzeń które nie zostały zarejestrowane w systemie,

12.5.6. Definiowanie oprogramowania do odbioru poczty firmowej na urządzeniu mobilnym

12.5.7. Bezpieczny dedykowany klient pocztowy pochodzący od producenta systemu MDM – dla platformy iOS i Android.

12.5.8. Ograniczenie użytkownikowi możliwości eksportu lub otwarcia załączników w innych aplikacjach niż dedykowane kontenery firmowe dostarczone w ramach systemu MDM

12.5.9. Załączniki przechowywane w bezpiecznym kontenerze na pocztę elektroniczną będą przechowywane w postaci zaszyfrowanej

12.5.10. Kontener na pocztę firmową ma możliwość dodatkowego zabezpieczenia hasłem lub PINem, o poziomie trudności, która może zostać zdefiniowana przez administratora systemu MDM

12.5.11. Możliwość definiowania restrykcji dotyczących otwierania załączników tylko w firmowych aplikacjach np. w firmowym kontenerze na dokumenty

12.5.12. Możliwość definiowania restrykcji dotyczących otwierania linków WWW tylko w firmowej przeglądarce

12.5.13. Możliwość zdalnej konfiguracji przez administratora ustawień synchronizacji dla klienta pocztowego dostarczonego z systemem MDM, a w szczególności:

12.5.5.1. Ilość dni w których zostanie synchronizowana poczta elektroniczna na urządzeniu mobilnym (np. ostatnie 7 dni, ostatnie 14 dni)

12.5.5.2. Możliwość zdalnego ustawienia interwału synchronizacji (wymagane: Push, Nie synchronizuj automatycznie i np. co 5 minut sprawdzaj, czy nie ma nowej poczty)

13. Funkcjonalności raportów generowane z systemu EMM

13.1. Administrator systemu EMM ma możliwość definiowania następujących parametrów raportów:

13.1.1. Format raportu - możliwość wysyłania w formacie: .csv; .pdf; .xls

13.1.2. System ma możliwość definiowania do jakich osób powinien dany raport zostać wysłany z systemu MDM, nawet jeżeli dana osoba nie jest zarejestrowana jako użytkownik Systemu.

13.1.3. Administrator systemu ma możliwość edycji tematu wiadomości z raportem
13.1.4. Raport generowany z systemu ma możliwość definiowania dla jakiej grupy użytkowników ma być on tworzony oraz dla urządzeń zarejestrowanych w wyznaczonym przez administratora okresie.
13.2. System ma możliwość definiowania raportów w sposób automatyczny w zdefiniowanym przez administratora interwale czasowym oraz termin zakończenia wykonywanej operacji.
13.3. System MDM ma możliwość wygenerowania raportu o następujących parametrach:
13.3.1. Nazwy użytkownika wraz z powiązanym z nim urządzeniem (platforma, system operacyjny, model) wraz z numerem UDID, IMEI/MEID, IMSI
13.3.2. Stan zgodności wprowadzonych polityk bezpieczeństwa w systemie MDM z stanem zgodności zarządzanych urządzeń
13.3.3. Raport odnośnie historii logowania kont administratorów
13.3.4. Szczegóły aplikacji urządzenia
13.3.5. Przegląd zainstalowanych aplikacji wg. grupy organizacyjnej
13.3.6. Urządzenia aktualnie podłączone w bezprzewodowej sieci LAN
13.3.7. Urządzenia aktualnie podłączone w bezprzewodowej sieci WAN
13.3.8. Podsumowanie ilości urządzeń w każdej grupie organizacyjnej
13.3.9. Podsumowanie urządzeń wg. typu i modelu
13.3.10. Szczegóły urządzenia oraz informacje o zainstalowanym Agencie systemu MDM
13.3.11. Raport odnośnie aktualnie zarejestrowanych urządzeniach
13.3.12. Raport odnośnie urządzeń wyrejestrowanych z systemu
13.3.13. Historia urządzeń współdzielonych
13.3.14. Stan wdrożonych aplikacji z systemu MDM
13.3.15. Lista wszystkich użytkowników administracyjnych według roli w Grupie Organizacyjnej
13.3.16. Raport odnośnie czarnych list aplikacji wg. grup organizacyjnych
13.3.17. Historia zagrożonych urządzeń
13.3.18. Raport odnośnie wdrożonych urządzeń w wybranym przedziale czasu
13.3.19. Raport pokazujący duplikaty rekordów urządzeń w wybranej Grupie Organizacyjnej
13.3.20. Szczegóły profilu dla urządzeń z systemem MDM

14. Kalendarz i kontakty

14.1 Kontener na kontakty firmowe pochodzi od tego samego dostawcy co System i umożliwia na platformach iOS oraz Android następujące funkcjonalności
14.1.1 Blokada możliwości eksportu kontaktów z kontenera firmowego,
14.1.2 Zezwolenie na eksport pojedynczych kontaktów,
14.1.3 Zezwolenie na eksport wszystkich kontaktów z kontenera firmowego do natywnych kontaktów
14.2 W przypadku wykonania operacji tj. Enterprise Wipe (usunięcie danych firmowych) lub w przypadku wyrejestrowania urządzenia z systemu kontakty ze strefy prywatnej, które zostały wyeksportowane z kontenera firmowego również muszą zostać usunięte;
14.3 System umożliwia zdalne wgrywanie listy kontaktów na urządzenia z systemem Android;
14.4 System umożliwia synchronizację kontaktów firmowych umieszczonych w Exchange w bezpiecznym kontenerze na kontakty firmowe. System powinien umożliwiać synchronizację domyślnej książki adresowej użytkowników, która w systemie Exchange jest zdefiniowana jako GAL;
14.5 System umożliwia jednoczesną konfigurację poczty e-mail w bezpiecznym kontenerze pocztowym i jednocześnie konfiguracje kontaktów w natywnej/wbudowanej liście kontaktów;
14.6 Dla systemu Android, System powinien posiadać dedykowany kontener na kalendarz firmowy pochodzący od tego samego dostawcy co System, który umożliwia następujące funkcjonalności:
14.6.1 Możliwość podglądu spotkań utworzonych w systemie Exchange

14.6.2 Kalendarz posiada możliwość zdalnej konfiguracji przez administratora, a w szczególności zdefiniowania przedziału czasowego jaki ma się domyślnie zsynchronizować
14.6.3 Możliwość dodawania nowych spotkań
14.6.4 Możliwość akceptacji, odrzucania, wstępnej akceptacji otrzymanych zaproszeń w kalendarzu
14.6.5 Możliwość edycji czasu, kiedy aplikacja będzie przypominać o wydarzeniu
14.6.6 Możliwość przekazywania zaproszeń do innych osób zaproszenia na wydarzenie oraz możliwość odpowiedzi do wszystkich na zaproszenie do wydarzenia,
14.6.7 Możliwość podglądu wydarzeń utworzonych w kalendarzu IBM Lotus
14.7 Kalendarz posiada możliwość wyświetlania wydarzeń wg. opcji: z całego dnia, tygodnia, miesiąca, wg. planu spotkań.
14.8 Możliwość synchronizacji kalendarza systemu IBM Lotus.

15. Tunelowanie aplikacji:
15.1 System posiada możliwość tunelowania aplikacji mobilnych dla platformy iOS i Android do wewnętrznej sieci Intranetowej, bez konieczności zestawiania tunelu VPN dla całego urządzenia tzw. Per-app VPN;
15.2 Zestawienie tunelu ma odbywać się bez konieczności dodatkowej obsługi użytkownika systemu urządzenia mobilnego
15.3 Tunelowanie aplikacji do wewnętrznych zasobów Intranetowych musi się odbywać przez bezpieczne połączenie za pomocą dedykowanego serwera proxy instalowanego na systemach Windows lub Linux z użyciem protokołu SSL VPN
15.4 Dostęp do wewnętrznych zasobów zasobów firmowych z użyciem bezpiecznego połączenia SSL VPN dla technologii (per-app VPN) musi być zarządzany z poziomu centralnej konsoli do zarządzania systemu
15.5 Komponenty służące do tunelowania aplikacji na serwerach aplikacyjnych jak i na urządzeniach końcowych muszą być integralną częścią systemu
15.6 Technologia per-app VPN wspiera uwierzytelnianie za pomocą certyfikatu dystrybuowanego przez platformę z centralnego systemu PKI lub systemu PKI wbudowanego w system.

5. WYMAGANIA DOTYCZĄCE WARUNKÓW GWARANCJI I SERWISU DLA SMARTFONÓW

a) Wykonawca zapewni obsługę gwarancyjną producenta dostarczonych smartfonów w okresie 60 miesięcy od dnia podpisania protokołu końcowego odbioru i 24 miesiące na akcesoria z wyłączeniem baterii, na które Zamawiający żąda 12 miesięcy od dnia podpisania protokołu końcowego odbioru. Bieg okresu rozpocznie się od daty podpisania bez zastrzeżeń protokołu końcowego odbioru.
b) Gwarancja obejmuje: wady materiałowe i konstrukcyjne, a także niespełnienie deklarowanych przez producenta parametrów i/lub funkcji użytkowych, naprawę wykrytych uszkodzeń w tym wymianę uszkodzonych podzespołów na nowe, usuwanie wykrytych usterek i błędów funkcjonalnych w działaniu urządzeń i oprogramowaniu.
c) Wykonawca dostarczy wersję edytowalną oraz papierową z numerami IMEI dostarczonych Smartfonów.
d) Wykonawca zapewni bezpłatny odbiór uszkodzonego sprzętu i dowóz naprawionego wolnego od wad sprzętu
e) odbiór i dowóz sprzętu dokonywany będzie z siedziby Zamawiającego Wydział Teleinformatyki KWP, Katowice ul. Lompy 19 w godzinach 8:00 - 14:00.
f) Maksymalny czas naprawy urządzenia - 30 dni kalendarzowe od dnia przekazania do naprawy.
W przypadku przekroczenia maksymalnego czasu naprawy wymiana sprzętu na nowy.
g) Czas reakcji na zgłoszenie uszkodzonego sprzętu (odebranie do naprawy): 48 godzin uwzględniając dni robocze.
h) Wykonawca nie może odmówić usunięcia wad ze względu na wysokość związanych z tym kosztów

i) Wykonawca w ramach realizacji przedmiotu zamówienia będzie zobligowany do wykonania procedury serwisowej polegającej na wymianie baterii w dostarczonych smartfonach w okresie od 18 miesięcy do 30 miesięcy od dnia zawarcia umowy. Nowe baterie muszą posiadać te same parametry lub lepsze oraz zostać wyprodukowane przez tego samego producenta co baterie dostarczone/zainstalowane w zakupionych smartfonach. Na nowe baterie Wykonawca udziela 12 miesięcznej gwarancji liczonej od dnia podpisania protokołu odbioru procedury serwisowej. Bateria musi być wyprodukowana nie wcześniej niż 6 miesięcy od dnia wykonania procedury serwisowej. Wykonawca wykona procedurę serwisową w terminie 2 miesięcy od dnia wysłania powiadomienia na adres e-mail Wykonawcy w przypadku zaoferowania smartfonu z bateriami wymiennymi oraz 3 miesięcy od dnia wysłania powiadomienia na adres e-mail Wykonawcy w przypadku zaoferowania smartfonu z bateriami niewymiennymi. Wykonawca wykona procedurę serwisową w lokalizacjach wskazanych w załączniku nr 4 do SIWZ. Wykonawca w terminie 7 dni przed dokonaniem procedury serwisowej poinformuje bezpośredniego odbiorcę oraz Zamawiającego.