Samsung Knox

bezpieczeństwo na wszystkich poziomach

Środowisko Samsung KNOX w zakresie bezpieczeństwa świetne uzupełnia systemy Mobile Device Management (MDM), wykorzystując kilka zaawansowanych mechanizmów, w celu poprawy ochrony urządzeń mobilnych.

- Urządzenia z systemem Android, mimo, że bardzo popularne w środowiskach biznesowych, często spędzają sen z powiek działom IT. Dzieje się tak ze względu na duże zróżnicowanie wersji oraz ilość ataków, która zawsze rośnie wraz z popularnością systemów operacyjnych. Odpowiedzią na te problemy jest system Samsung Knox. Platforma została zaprojektowana, aby poprawić bezpieczeństwo danych w urządzeniach pracujących pod kontrolą Androida, a jednocześnie nie zaburzyć jego pracy. Co ważne, Knox bez problemu współpracuje z rozwiązaniami do zarządzania urządzeniami przenośnymi zewnętrznych producentów (tzw. MDM, z ang. Mobile Device Management).

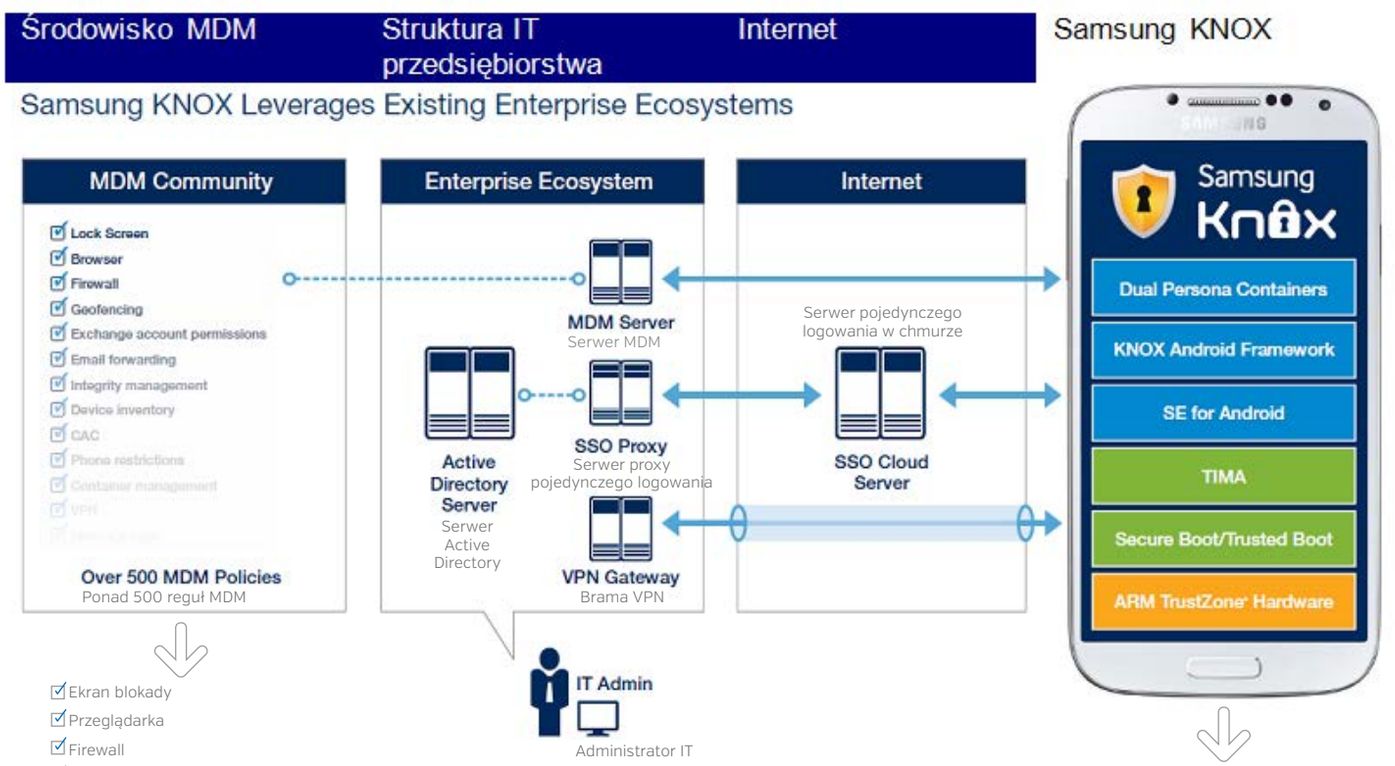
- Samsung Knox pozwala pogodzić sprzeczne interesy przedsiębiorstw, dążących do zachowania kontroli nad urządzeniami mobilnymi, oraz pracowników, którzy często wykorzystują jedno urządzenie zarówno do celów służbowych, jak i prywatnych. System jest gotowy, aby sprostać wymaganiom przedsiębiorstw z dowolnego sektora. Znajduje zastosowanie zarówno w środowiskach BYOD (ang. Bring Your Own Device), jak i COPE (ang. Corporate-Owned, Personally Enabled).

- Najważniejsze funkcje Knox to wygodne zarządzanie urządzeniami mobilnymi oraz stworzenie bezpiecznego środowiska do uruchamiania aplikacji korporacyjnych w systemie Android. Oferowany poziom ochrony jest na tyle wysoki, że uzyskał akceptację Departamentu Obrony Stanów Zjednoczonych. Administratorzy IT otrzymują możliwość zdalnego zarządzania (aplikacjami, kontami e-mail, licencjami czy hasłami) i monitorowania tabletów oraz smartfonów, a także zabezpieczenia danych przed wyciekiem. Mogą wdrożyć mechanizmy bezpiecznego dostępu do zasobów przedsiębiorstwa. Ponadto Samsung KNOX daje możliwość wsparcia w czasie rzeczywistym dla użytkownika mobilnego.

Integracja z istniejącą infrastrukturą IT

Samsung KNOX działa opierając się na istniejącym środowisku IT i integruje się z takimi komponentami, jak serwer MDM, serwer logowania SSO, Active Directory czy bramka VPN. Oferuje ponad 500 gotowych reguł MDM, dotyczących bezpieczeństwa, integracji z korporacyjnym środowiskiem IT i zarządzaniem kontenerami. Dla użytkowników bardzo wygodnym rozwiązaniem jest pojedyncze logowanie (SSO) w chmurze – jedno potwierdzenie tożsamości wystarcza, by uzyskać dostęp do wielu aplikacji działających środowisku typu cloud.

Samsung KNOX działa w oparciu o istniejącą strukturę IT



- Ekran blokady
- Przeglądarka
- Firewall
- Geofencing
- Zarządzanie kontami Exchange
- Przesyłanie wiadomości e-mail
- Zarządzanie integralnością systemu
- Rejestr urządzeń
- CAC
- Ograniczenia możliwości korzystania z telefonu
- Zarządzanie kontenerami
- Prywatne sieci wirtualne (VPN)
- Archiwum wiadomości

Kontenery w trybie widoku podwójnego
Środowisko KNOX dla systemu Android
SE for Android
TIMA
Funkcja Secure Boot/Trusted Boot
Zabezpieczenia sprzętowe ARM TrustZone®

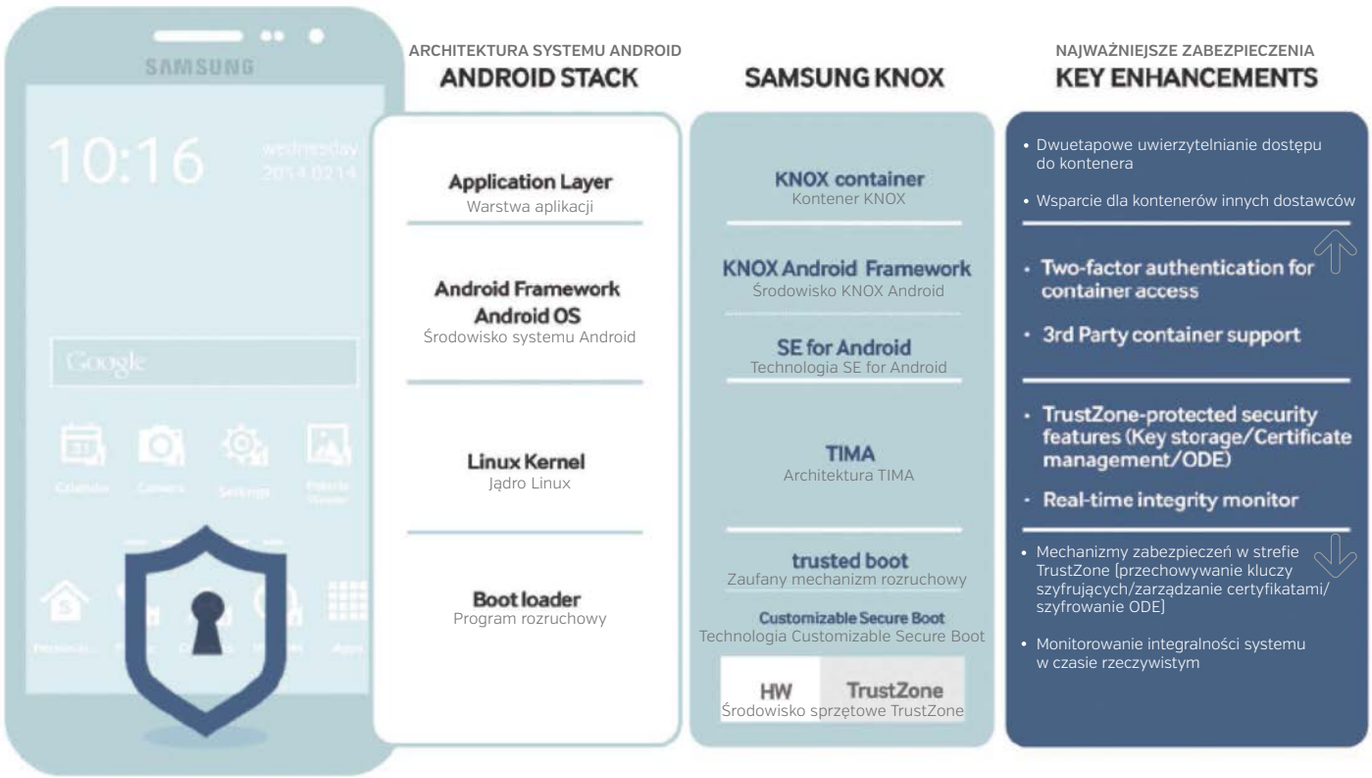
Technologia

- Samsung KNOX zapewnia bezpieczeństwo urządzeń mobilnych na wszystkich poziomach, począwszy od warstwy sprzętowej, poprzez proces uruchamiania systemu operacyjnego (warstwa systemowa), na bezpiecznych kontenerach do uruchamiania programów skończywszy (warstwa aplikacji).

- W najniższej warstwie sprzętowej o bezpieczeństwo dba ARM TrustZone. Ta technologia chroni urządzenie przed przejęciem kontroli z zewnątrz lub wewnątrz i zapobiega wykonaniu niebezpiecznych operacji przy użyciu procesora. Sprawia, że metody włamań znane ze świata komputerów x86 stają się nieskuteczne. Następnie do działania wkraczają funkcje Secure boot oraz Trusted boot, które zapewniają integralność systemu w czasie rozruchu. Pilnują, aby na urządzeniu uruchamiane było tylko sprawdzone i dopuszczone do użytku oprogramowanie. Ta technologia umożliwia także stosowanie certyfikatów bezpiecznego rozruchu. Dzięki takiemu rozwiązaniu klienci o większych potrzebach w zakresie bezpieczeństwa mają możliwość nabycia standardowych urządzeń oraz wykorzystania certyfikatów na potrzeby bezpiecznego rozruchu.

- Poziom wyżej działa technologia TrustZone-based Integrity Measurement Architecture (TIMA), która weryfikuje integralność jądra systemu Linux w czasie rzeczywistym. W razie wykrycia naruszenia integralności jądra lub programu rozruchowego następuje odpowiedź ze strony architektury na podstawie ustalonych reguł. Jedna z reguł powoduje zablokowanie dostępu do jądra oraz wyłączenie urządzenia.

- Kolejną warstwę zabezpieczeń stanowią rozszerzenia Security Enhancements for Android (SE for Android). Ich zadaniem jest precyzyjna kontrola dostępu, pozwalająca odizolować usługi systemowe od aplikacji innych producentów. Sprawiają one również, że tzw. rootowanie systemu staje się bezużyteczne. Te zabezpieczenia powstały na bazie SELinux (Security-Enhanced Linux) i zawierają reguły bezpieczeństwa dla użytkowników i aplikacji, na przykład blokują dostęp do chronionych plików systemowych. Technologia pozwala na tworzenie wydzielonych obszarów przechowywania aplikacji i danych z myślą o minimalizacji ryzyka i skutków naruszenia lub obejścia zabezpieczeń poprzez wprowadzenie do systemu złośliwego lub wadliwie zabezpieczonego oprogramowania. Dopiero nad tą warstwą jest zlokalizowane właściwe środowisko KNOX dla systemu Android.



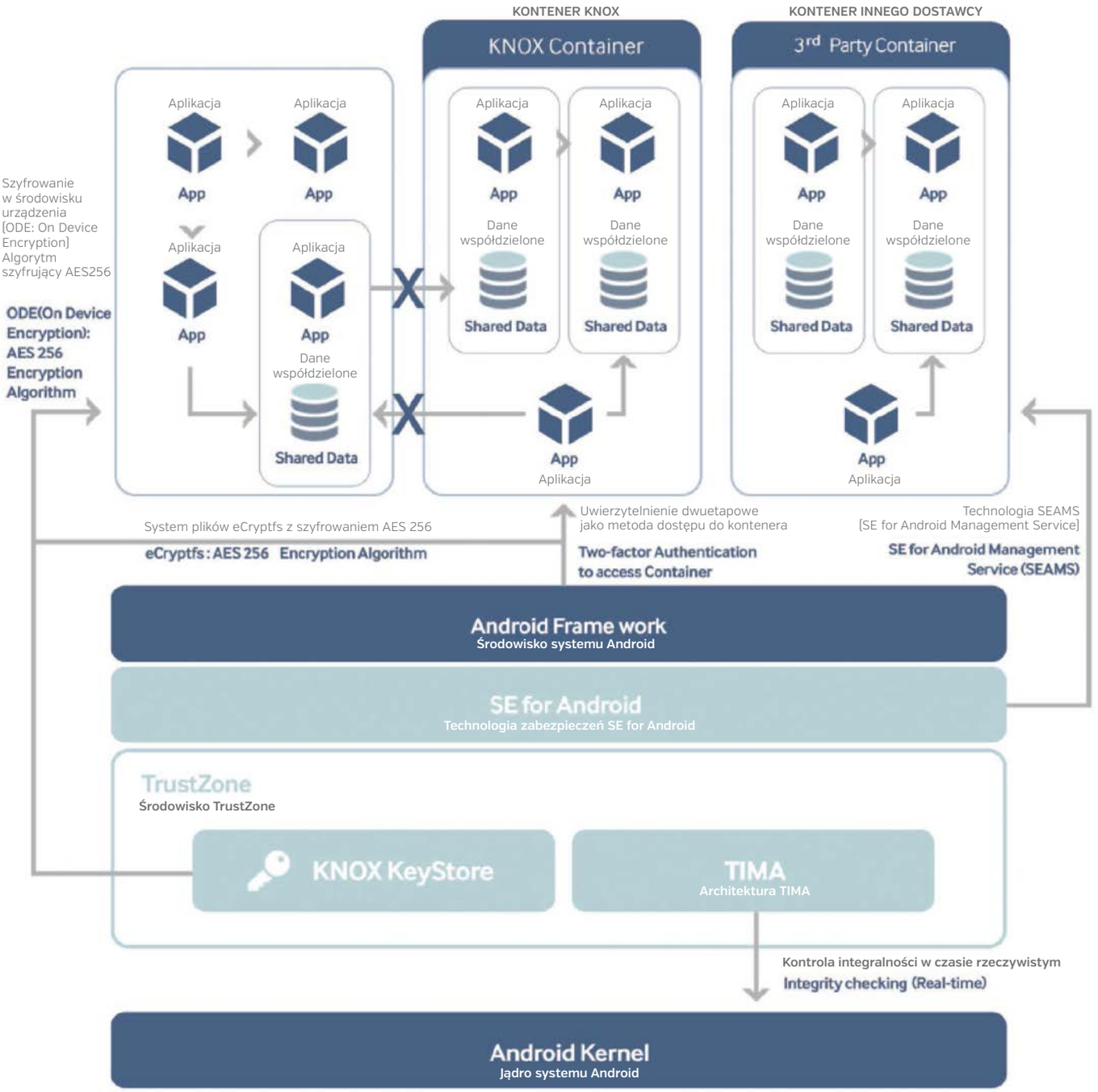
Poziomy zabezpieczeń w środowisku Samsung KNOX

Podwójny kontener

Najwyższym poziomem stosu zabezpieczeń jest tryb widoku podwójnego (Dual Persona), który służy do szczelnego odseparowania środowiska służbowego od prywatnego. Ten mechanizm powoduje utworzenie bezpiecznej przestrzeni w urządzeniu, w której znajdują się firmowe dane i aplikacje mające dostęp do sieci korporacyjnej. Natomiast w części prywatnej pozostawia się użytkownikowi swobodę, na przykład brak restrykcji co do instalowania aplikacji z publicznych sklepów.

Z punktu widzenia użytkownika urządzenia Dual Persona to dwa pulpity z zestawem różnych aplikacji. Kontener Samsung KNOX obejmuje własny ekran główny, program uruchamiający, a także własne aplikacji i widżety. Aplikacje i dane przechowywane wewnątrz kontenera są oddzielone od aplikacji pozostających na zewnątrz. Taka architektura rozwiązuje typowy dla modelu BYOD problemu wycieku danych. W bezpiecznym kontenerze dane są przechowywane w szyfrowanym systemie plików, który funkcjonuje zupełnie niezależnie od aplikacji pozostających na zewnątrz.

Szyfrowanie danych realizowane jest w standardzie Advanced Encryption Standard (AES) z kluczem 256-bitowym (AES-256). Poza tym kontener daje dostęp do klienta WSP z certyfikatem FIPS. Klient WSP umożliwia administratorom środowiska IT przedsiębiorstwa konfigurowanie i udostępnianie wirtualnej sieci prywatnej dla każdej aplikacji (do pięciu równoległych bezpiecznych połączeń), a także możliwość zarządzania taką siecią. Kontener zapewnia również obsługę wirtualnej sieci prywatnej w architekturze IPSec, w tym algorytmu kryptograficznego Suite B.



Rozbudowane środowisko Samsung KNOX

Bezpieczeństwo odpowiednie dla wojska

Zabezpieczenia zaimplementowane w Samsung KNOX docenił Departament Obrony Stanów Zjednoczonych. Platforma została zatwierdzona przez Agencję Systemów Informatycznych Obrony Stanów Zjednoczonych do użycia w sieciach Departamentu Obrony. Rozwiązanie to zapewnia ochronę danych w ruchu (Data In-transit, DIT) zgodną ze standardem FIPS 140-2. Szyfrowanie danych w spoczynku (Data At-rest), czyli przechowywanych w urządzeniu, również spełnia wymogi tego standardu. Ponadto oferuje obsługę kart chipowych oraz monitorowanie integralności systemu.

Bezpieczny sprzęt, bezpieczna platforma, bezpieczne kontenery aplikacji