Mobile Device Management and Security Glossary

February, 2011

MOBILE OS

ActiveSync
Exchange ActiveSync (EAS) is a Microsoft technology that allows mobile users to access their Microsoft Exchange mailboxes and use e-mail, calendar, contacts and tasks applications on their mobile devices. Administrators can control which devices have access to the Exchange Server. Exchange ActiveSync works with a wide variety of mobile operating systems, including Windows Mobile, Windows Phone, iOS, Android, Symbian and Palm WebOS.

Android
Android is a mobile operating system developed by Google and managed by the Open Handset Alliance (OHA) and the Android Open Source Project (AOSP). It runs on smartphones from many manufacturers, including Acer, HTC, Huawei, LG, Motorola, Samsung Electronics, and Sony Ericsson. As of September 2010 Android was estimated to be #1 in US market share for mobile operating systems (44%) and #2 in global market share (25%). Over 100,000 apps are available for Android through Google's Android Market (estimates from Canalys).

API
Application Programming Interface

APNS (Apple Push Notification Service)
The Apple Push Notification Service (APNS) is a mobile service created by Apple that "pushes" notifications and alerts from applications on servers to iPhones, iPads and iPods.

Apple Root Certificate Authority
The Apple Root Certificate Authority (CA) manages the generation, distribution and administration of encryption keys for the Apple Public Key Infrastructure (PKI). It facilitates encrypted secure communications between web servers and mobile devices. See Certificate Authority.

BES (BlackBerry Enterprise Server)
The BlackBerry Enterprise Server (BES) is a middleware software package from Research In Motion that synchronizes emails, calendaring information and contacts between BlackBerry devices and messaging servers such as Microsoft Exchange and IBM Lotus Notes. It also connects BlackBerry devices with enterprise applications. BES includes a range of management and security features to help email administrators.

CDMA
Code Division Multiple Access

iOS
iOS, formerly known as "iPhone OS," is a mobile operating system developed by Apple for the iPhone, iPad, iPod Touch and Apple TV. It runs exclusively on devices manufactured by Apple. As of September 2010 iOS was estimated to be #2 in US market share for mobile operating systems (26%), with 17% market share worldwide (estimates from Canalys). Over 300,000 apps are available in Apple's App Store.

Lotus Notes Traveler
IBM Lotus Notes Traveler is a "push" email product for IBM that provides access from mobile devices to email and Personal Information Management (PIM) applications for Lotus Notes users. It allows mobile users to access IBM Lotus Domino servers and use e-mail, calendar, contacts, journal and to-do applications on their mobile devices. Lotus Notes Traveler supports Apple iOS, Android, Windows Mobile, and Symbian devices. Lotus Notes Traveler also provides some MDM features for Lotus Notes users, such as remote wipe, passcode policy management, and event monitoring.

MeeGo
MeeGo is a mobile operating system designed for smartphones, tablets, netbooks, and consumer information appliances such as web-connected televisions and in-vehicle infotainment devices. It is a Linux-based open source project managed by the Linux Foundation and driven by Intel and Nokia. MeeGo is intended to span a wide range of mobile and non-mobile computing devices, including tablet computers, but in 2010 had not yet been released on a smartphone.

Smartphones
Smartphones are handheld devices that include a computing operating system as well as wireless communications capabilities. They allow users to exchange email as well as run mobile applications or "apps." The leading manufacturers, in order of worldwide shipments (3Q 2010) are: Nokia, Samsung, LG, Apple, Research In Motion, Sony Ericsson, Motorola, HTC, ZTE, Huawei Technologies. The leading mobile operating systems, in order of worldwide shipments (3Q 2010) are: Symbian, Android, iOS, Research In Motion, Microsoft Windows Mobile, and Linux (estimates from Gartner).

Symbian OS
Symbian OS is a mobile operating system developed by Symbian Ltd (acquired by Nokia) and managed by the Symbian Foundation, a non-profit open source organization. It runs on smartphones from many manufacturers, including Fujitsu, Mitsubishi, Motorola, Nokia, Samsung, Sharp, Siemens and Sony Ericsson. As of September 2010 Symbian was estimated to be #1 in worldwide share for mobile operating systems (37%), although only #3 in the United States, after Android and Apple iOS (estimates from Gartner).

Windows Mobile
Windows Mobile is a mobile operating system developed by Microsoft and used in smartphones and mobile devices. It is a successor to Windows CE, but will be replaced in the future by Windows Phone 7. It runs on smartphones from manufacturers including HTC, LG and Samsung Electronics. As of September 2010 Windows Mobile was estimated to be only #5 in worldwide mobile operating systems, with a 3% market share (estimate from Canalys and Gartner). See Windows Phone 7.

Windows Phone 7
Windows Phone 7 is a mobile operating system developed by Microsoft and used in smartphones and mobile devices. It is a successor to Windows Mobile. It was released in selected countries in October and November 2010. It has been announced for smartphones from manufacturers including, Dell, Hewlett Packard, HTC, LG, Samsung Electronics and Sony Ericsson. However, Microsoft has indicated that Windows Phone 7 is designed primarily for the consumer market rather than for enterprise applications.

MOBILE PLATFORM

Enterprise App Store
An App Store is an online service that allows users to browse a web site and download applications to their smartphones. The most widely-known app stores are from vendors such as Apple (iTunes Store, Google (Android Market) and Microsoft (Windows Marketplace for Mobile). An Enterprise App Store is an app store created by a single enterprise or government agency to distribute apps developed in-house or authorized and supported by the IT group.

iDEP (iOS Developer Enterprise)
The iOS Developer Enterprise Program (iDEP) is an Apple program to encourage corporate and government software developers to create in-house mobile applications for the iOS operating system. These applications are for internal use and do not get published on the public App Store.

NETWORK

Cloud Extender
A cloud extender is a cloud-based service, for example a database or a backup service, which can interact with and extend the functionality of other cloud-based services and applications.

Configuration Profile
A configuration profile is a set of parameters used to configure a mobile device for a user or group of users. The parameters might include minimum requirements for the passcode, information on how to connect to the corporate email server, virtual private network (VPN) settings, and authorized Wi-Fi networks.

OTA Configuration
Over-the-air (OTA) configuration, also known as over-the-air programming and over-the-air provisioning (OTAP), is the ability to configure and assign policies to remote mobile devices solely through a wireless connection. OTA configuration eliminates the need for IT administrators or support personnel to physical touch devices in order to prepare them for email and corporate applications. This is particularly important when there are many distributed users, and when users purchase their own devices. OTA configuration can also refer to distributing software and application updates to mobile devices.

Provisioning Profile
A provisioning profile is a file installed on mobile devices, especially iPhones, that allows specific in-house applications to be installed and executed. Administrators can use provisioning profiles to restrict applications to specific devices.

TCP
Transmission Control Protocol

SECURITY AND COMPLIANCE

AES
Advanced Encryption Standard

Certificate Authority
A certificate authority (CA) is a trusted organization that issues digital certificates. Digital certificates are used with Public Key Infrastructure (PKI) technology to facilitate encrypted secure communications between web servers and endpoints such as mobile devices, laptops and PCs. When an endpoint contacts the server it requests a digital certificate with information about the owner of the web site and a public key. The endpoint sends the certificate to the Certificate Authority, who validates that it comes from the purported source (e.g. the user's employer or the user's bank). The endpoint uses the public key to establish an encrypted connection with the server. Third party certificate authorities include VeriSign, Entrust and GoDaddy. Enterprises and government agencies can set up their own CAs.

Device Encryption
Device encryption is the ability to encrypt selected files or all of the files on a device to protect them from unauthorized access if the device is lost or stolen. Typically the user must enter a PIN before the device will decrypt and display encrypted files.

Lock/Unlock
Lock is an MDM (Mobile Device Management) feature that allows administrators or users to prevent anyone from using a mobile device or seeing data stored on it. Remote Lock is usually accomplished by sending an SMS message from a server to the device. Locking can also be enforced locally, for example if the wrong passcode is entered too many times. An Unlock command removes the lock. All MDM systems provide an over-the-air Lock feature for administrators, and some also provide self-service locking and unlocking for users through a web portal.

MDM (Mobile Device Management)

Mobile Device Management (MDM) systems are used to provision, monitor, manage, secure, support and secure mobile devices. Most MDM systems include a server-based management component and an agent or app that runs on each device. Some systems are vendor-specific (e.g., work only with iOS or RIM BlackBerry devices), while others span multiple operating systems and manufacturers (e.g. iOS, Android, Windows Mobile and Symbian). Most MDM solutions are premise-based, although cloud-based alternatives are emerging.

Typical features of MDM systems include:

- Tracking of devices by serial number, user name, manufacturer and operating system.
- Inventory of software and hardware on devices.
- Management of passcode policies.
- The ability to distribute and manage Wi-Fi and VPN policies.
- Remote "over-the-air" configuration and provisioning.
- Remote wipe, lock and unlock.
- The ability to block or disable cameras, browsers and access to app stores.
- Reporting on the status and configuration of devices.

MSM (Mobile Services Management)

Mobile Service Management (MSM) products gather network, server and application health and performance data in order to provide end-to-end monitoring of mobile applications. This allows an administrator to track when users are having trouble connecting, or are getting slow performance on email and mobile applications. Some MSM vendors are branching out by adding MDM features to their solutions.

Passcode

A passcode is a string of characters or numbers used to authenticate a user to a device. Most mobile devices can be configured with passcode policies, for example a requirement that passcodes have a minimum number of characters, or include at least one alphabetic and one numeric character, or be changed within a certain time period.

SCEP

The Simple Certificate Enrollment Protocol (SCEP) is an industry standard protocol designed to simplify the issuing and revocation of digital certificates. It allows administrators to securely issue certificates to large numbers of network devices using an automatic enrollment technique. See Certificate Authority.

eAgency, Inc.
6 Upper Newport Plaza
Newport Beach, CA 92660