IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 2, Issue 1. (Mar. - Apr. 2015), PP 06-10
www.iosrjournals.org

Android Management Redefined: An Enterprise Perspective

Pooja Maheshwari

Abstract: *The global enterprise mobility market is expected to reach $174 billion by the year 2017 according to recently published reports! Android, iOS and Windows Phone are the pre-dominant mobile platforms in the market today. Android, by virtue of its open source nature and commercial friendly license holds the maximum market share and is finding increasing applicability beyond just smartphones and tablets. While Android is the top market leader in consumer mobility, enterprises are still figuring out ways of how it can be better managed. Android supported default manageability provisionhas been very limited. Precisely,it is missing many crucial policies that empower the enterprises with the required device manageability. In this paper, we will discuss the business requirements and the challenges faced by enterprises in adopting Android powered devices. We would then discuss in detail how enterprises can plan a manageable yet cost-effective Android solution.*

I. Introduction

Android Market Trends

Statisticsindicate that fifty-two percent of smartphones in the U.S. run on Android operating system. Android allows manufacturers to include an array of custom configurations to meet consumer's desires—everything from sharper cameras to longer-lasting batteries. Talking about the market trends in the context of enterprise mobility device deployment. While the so-called Bring Your Own Device movement is going strong, it is also posing a lot of challenges. As per July 2013 report by J Gold Associates, in the next 3 years, Corporate owned and deployed tablets will grow at an annual average of 64% over the next 3 years, while BYOD tablets will grow at 31%. As a result, most organizations will have a dramatically large base of corporate owned and provisioned devices than BYOD devices which will affect procurement, support, infrastructure, apps and TCO. Also notable is the statistics as per Enterprise Mobility Exchange Report 2013, which indicate 32% of the budget was invested by enterprises in Ruggedized Mobile Devices over the past 18 months.

All thesestatistics speak that Android is undoubtedly taking its place in the enterprise and with time its applicability is expected to increase.

Let us now take a glance at the core business requirements of enterprises with respect to mobility.

Business Requirements

First, real time information flow is a crucial business need. This means required enterprise data should be available seamlessly to all users on the go, whether they are in office or travelling for a business purpose or at home. At the same time, from wherever it is collected, the information captured should get updated seamlessly.Auto-monitoring of data, usage and location is another core need when it comes to tracking of field force, vehicles, gadgets, etc. The third requirement is ofcustomer delight by the way of faster servicewhile addressing customer requests.

While all these business requirements demand for extending certain use cases to mobility, there are many concerns that the CIO organization has while adopting a mobility solution.

Let us understand the challenges with the help of a field force use case. Field force constitutes for a majority of enterprise workforce, when we talk about enterprises in manufacturing, financial, retail and other service sectors. Consider the case of a Financial services company having 10s of thousands field force personnel who need enterprise data on the move for sales and collection of documents etc. Few years back this company deployed Linux terminals for the complete workforce by collaborating with a custom hardware vendor. Dependency on a single vendor for hardware as well as software services resulted in a vendor lock in, there by facing vendor dominance,delay in procurement and frequent SLA breach. Further, the company'sinvestment in expensive Linux terminals increased their spending in procuring and maintenance. On the other hand mobile device based solutions are inexpensive and more suited for such use cases. The company eventually decided to evaluate mobile device options. Android because of its open source nature, commercial-friendly license and wide user acceptance along with an enriched development ecosystem appeared to bean obvious cost-effective option.

Field force use case – The Challenges

However, there were a lot of concerns that need to be addressed before considering any solution for the field force use case. The first and biggest challenge ishaving a fine-grained policy management framework that would ensure that the software and hardware access for various user typesis under enterprise' control.

Consider the case, where the enterprise requires that the device WiFi should only connect to corporate WiFi SSIDs or the user should be able to place phone callsonly to corporate workgroups. Further, in the event of employees exit or a lost device, the admin should be capable of doing a selective or a full wipeas per the need. Policy changes should not involve any type of manual intervention or settings at the device end. Additionally, it should be possible to further enhance or tailor the policies and commands as per theirmobility strategy.

Anotherchallenge from the security perspective is authorized user and data access. Devices should work in a fashion similar to corporate desktops. This means that same password rules and security norms should apply across devices whether it's a corporate PC or a corporate tablet.

Devicescan be used by different enterprise users in different shifts. Depending on the user, access to enterprise data and apps should be provided through user specific workspace. And of course, all this should work seamlessly in offline mode too.

Additionally, it is sometimes desirable, to customize the branding using custom boot animation and launcher application. Removing the unrequired stuff and bundling all enterprise specific apps as a part of device factory settings can convert the device to a purpose-built device solution. The administrator must be able to impose what apps can be installed on the device.

These challenges seem to be huge when measured for vanilla Android platform. Fortunately there is a way out.

Now moving ahead. While I would refer to the field force use case as a practical example for this paper, the process and intricacies of designing a custom Android solution are applicable to pretty much any type of custom device solutions.

Let's now see how you can plan a custom Android solution and some best practices for the same.

Planning

The core factors for enterprise while deciding on any type of custom Android solution would includefour steps.

As in case of any type of solution, start by understanding requirements.Next, choose the device as per the requirements, followed by preparing the device for enterprise use by adding the necessary policies, if not already present. And at last, perform required platform level customizations and branding if any.

While understanding the requirements is a much discussed topic and there are many approaches followed in the industry.From a mobility perspective,the focus should be on the use cases that actually represent the mobility needs out of the huge functionality available throughIT solutionsalready deployed in the enterprise.Further, non-functional requirements such as good user experience, internationalization, upgradability, etc. should be analyzed before freezing the solution scope and requirements.

The focus of this paper is how to choose the best fit device and the approach while building a custom android solution. Let uslook at these 2 aspects in detail.

Choosing a device

Making an informed decision when choosing a device is important as itwill drive your budget, device service SLAs, user productivity, user acceptance and new device procurement. Some of these factors may appear to be very minor initially, however they may cost you real business time being lostat a later stage.

There are two device types to choose from. Consumer devices and purpose-built devices.

Purpose-built devicesare manufactured for specific enterprise needs. Like the point of sale terminals, self-service kiosks, Automotive IVI, etc. The time for procuring new custom devicesand service SLAs would vary for different OEMs.

You should go for a purpose-built device only whenthe following conditions are fulfilled.

1. First, there should be a need to deploy the devices at a huge scale. For example, 10,000 or more.
2. Second, are there very specific hardware needs like finger print sensor, printer, etc. for the solution.
3. Third, in case of multiple hardware accessories requirement, you may need the device to be assembled as a single unit from the portability and durability perspective.

If you find that your requirement is very distinct from the models offered by custom hardware vendors,only then you should go for getting a totally new custom device hardware design. Don't forget that this option is the most expensive from an initial investment as well as maintenance perspective.

If your requirementsdonot fit into this criteria for purpose-built devices,consider an available consumer device along with third party hardware accessories. This optionwould usually work best in terms of cost of purchase and maintenance, service SLAs and procurement.

Consumer devices like those offered by various OEMs like Samsung, HTC, etc. fall under this type. Any specific hardware accessory needs such as fingerprint sensor or printer can be added as needed. There are many Bluetooth and USB powered accessories available in the market which support Android.

Let's look at the recommended configuration when selecting the device for your solution.There are a variety of device configurations available but it is advisable that you

1. Choose a high configuration System on Chip (i.e. SoC) like NVidia Tegra 3, Snapdragon S4 or Samsung Exynos 4 Quaddepending on the OEM.
2. Choose a good RAM size of minimum 1GB.
3. Go for a capacitive touch screen at the minimum.
4. If your mobility use cases need good amount of data management, go for a tablet form factor. Usually, 7" or 8" tablets are preferred in the industry.
5. For applicationsnot involving too much data management,go for a smartphone form factor. For example in use cases focused on monitoring, receipting, etc. go for a smartphone.
6. Another important consideration is the Android version on the device.At the minimum it should be Jelly bean or Kitkat.

Jelly bean provides multi-user support as the major addition and other features include support for Bluetooth smart ready, optimized location and sensor capabilities, better digital rights management, UI automation, localization utilities and support for restricted profiles. Of special note, are the enhancements in Android Jellybean for enterprise security in many areas including support for SELinux. SELinux protects the operating system against potential security vulnerabilities.Further, KitKat has some good feature added from enterprise perspective like printing support, batch sensor event support, enhanced payment support through NFC and support for infra-red blasters.

Choosing one of these versions would also benefit in terms of overall device acceptance and adoption in the enterprise.

Let us now understand how we can make the chosen Android device enterprise ready.

Making Android enterprise ready

Android, by default provides device management APIs that support management of device password, device storage encryption and camera related policies, in addition to full wipe and remote lock operations. Many crucial policies can be added especially when looking for fine-grained remote manageability cases such as thefield force case we saw.

American Airlines is the first airline in US to have branded Android tablets for crew management needs.Thismanaged Android solution was deployedby leveraging Samsung for Enterprise better known asSAFEpowered devices for 17000+ flight attendants of American Airlines.

So, how canyou achieve manageability for your Android powered solution?

If you are looking for a ready-made option then go for Android devices that support manageability such as those based on Samsung SAFE, KNOX, 3LM, Android+, etc. These solutions provide for a few hundred policies to manage the devices.

But, if you are going for a purpose-built device, you will need a custom solution for managing them.

The Solution Approach

Given on the slide are the 3 key components that would be required to achievefine-grained management for android in the enterprise. The first core component is Enterprise Android platform. This component would require changes at Embedded Android layers and hence, need of Custom ROM. This platform should expose certain management APIs to help the Android platform be managed externally by a trusted entity. Next component is the trusted entity i.e. an agent which should reside on the device and act as a bridge between the backend and the device platform itself. The Agent needs to communicate and make all the dynamic updates effective in real time on the device.

The policy and command managementoperations will need to beperformedat the backend by the Administrator using an Admin Console. The Admin Console exposes crucial features related to user management, device management, policy and command management.

Let us now understand how these components would work when put together in an enterprise eco-system.

Solution Overview

Consider the case where a group ofenterprise usersare using devices powered with Enterprise ready Android solution.Each device accepts only enterprise user login and may have multiple enterprise users registered. Every enterprise user is mapped to a distinct device user for ensuring data privacy between the users.

Device provisioning getstriggered, whenever a new enterprise user is added by the device admin user through the device. Device admin user is the one having all the rights for user and other device manual management related workflows. Other users on device are linked with enterprise user and work in their own space and can manage only that space without affecting others.

The on-device agent co-ordinates with backend for user provisioning and authentication. It is also responsible for fetching and applying of policy and command updates on the device for various registered users.

At server end, an Enterprise Administrator approves new users andmanages policies for variousroles.He can issue and track commands like full or selective wipe,remote lock, etc. as per need. All this is done using the Admin Console which acts as a central management console for fine-grained management of the enterprise devices.

Another important component is a robust update system. The system must allow the administrator to upload ROM images onto the Update server via an OTA Update Center. At the device end, there would be an update fetcher component. Subsequently, the update would get installed through the updater component on the device. This update system should work seamlessly.

All these features help you achieve effective management of your custom Android solution.

Here I would like to mention a case wheresuchenterprise ready Android solutionwas deployed for field force use case where sales personnel were provided a non-GSM WiFi supported 3G Android tablet,installed with pre-bundled apps for field usage. For enterprise data security and privacy reasons, the Admin wants to enablea WIFI policy for thefield staff devices and connect to WiFi SSIDs within the company area.
Thistype of solution can help to increase the productivity of device end users, and reduce the overall operating cost for the organization.

Recommendations - Android Management

I would like to emphasize on adopting the convention of blacklist, whitelist and on/off for all policies.

One of theareas to look at is Communication Management. It can involve enabling and disabling of communication channels like outgoing or incoming SMS and phone calls. It may also include whitelisting and blacklisting of contacts for various communication channels.

Security management is the most crucial amongst all. Security of data on the move requires that the data flowing through the networks from and to the device is secure.

For Data at rest which denotes the data residing on the device, it is important to consider device encryption and SD Card encryption. Also, the encryption may be present at app layer for data saved in the DataBase and files. However, that can be best handled at the app layer by introducing a mobile application management library.

For security of data on the move security, Always VPN on policy should ensure that the device can be connected to network only if it is on VPN. This is very important if the enterprise needs that all the network traffic always gets routed through the enterprise server. This is particularly required for devices dealing in excessive private data like customer financial information and transactions. Further, HTTPS must be treated as mandatory.

Further, it is recommendedto provide for enabling or disabling hardware and other features. It is crucial for devices deployed in field staff use cases that they be able to use certain features only. For instance, the camera, Bluetooth, screen capture, tethering and other hardware/software features may totally be disallowed for a particular user profile to maintain enterprise data security and to avoid device misuse. Enforced Firmware OTA policy may also be introduced if an enterprise is looking for forced upgrades beyond a particular timeline for crucial OS updates.

Next, expense management is an important category to be able to control the cost incurred per user. Automated location tracking policy can be used for achieving location logging for the device, thereby enabling the enterprise to track user's transit allowances. Not only this, it would also help monitor employee's productivity and variances. Other important policies to be considered under this head are to enable or disable data communication while roaming, limit data, phone or SMS usage, etc.

Having the option of Kiosk mode application enables locking the device to run only thatapplication. This may also involve remapping or disabling of hardware keys.

For enterprise profile management, thepre-bundled launcher should utilize an enterprise login moduleso that the same rules apply to mobile device access just like the desktop access.

Subsequently, this login should then be used as a basis for all enterprise app workflow access rights as assigned by the admin.

An important last step ingetting your solution ready to workis throughintegration with 3rd party hardware or software and custom branding.

Customization and branding

Broadly speaking, there are three steps to this.

The first step is to do all necessary customizations for integrating any third party hardware or software as required. This step would involve understanding of the third party hardware, whether it is Android compatible or not. Next if there is an SDK available, then you would need to utilize that SDK at the application layer and you are done. But if the hardware requires driver development and then exposing APIs for use by application layer, then you would need to customize the Android platform. In order to include a third party software, you would need to modify the Core libraries layer and expose APIs through the framework layer or use that library through NDK.

Enterprise branding can be achieved by using enterprise themed boot splash, boot animation and launcher app. In fact, all the apps on the device should be modified to have enterprise theme.

This helps in better user acceptance and a short learning curve.

After applying these customizations and branding changes, the device would be ready to be released for use by your enterprise workforce.

Summary

To summarize, fine-grained management of hardware and software features on Android platform is the biggest challenge seen by the enterprises in its adoption for serious use cases. In this paper, we discussed about intricacies of these challenges. We also discussed the crucial steps in carving a manageable and cost-effective custom Android solution. Based on your specific requirements it is important to carefully choose between consumer devices with third party hardware accessories or go with purpose-built device that is specially assembled with required hardware accessories. We touched upon certain best practices that can help you decide which device to go for.

We then discussed a solution approach in detailfor achieving fine-grained policy management on your custom Android devices. We also saw the components of an enterprise ready Android platform and various recommendations.