Red Bend Software

From Hardware Manufacturer to Service Provider

5 Software-Based Services that Can Transform OEMs

White Paper

Published: October 2013

Notices

vLogix Mobile® Notice

vDirect Mobile® Notice

vRapid Mobile® Notice

vSense Mobile® Notice

Red Bend Software Management Center Notice

Table of Contents

Introduction

PC makers understand better than most manufacturers the challenges of operating in a commoditized market. Standardization on the Wintel architecture famously enabled the proliferation of PCs to the mass market, but left OEMs with little room for differentiation and constant downward pricing pressure.

In the world of wirelessly connected devices, similar market forces are at work. From smartphones to tablets to cars and consumer electronics, today's buyers find the same feature set: a sleek touch-screen powered by a high-level operating system connected to a robust application market.

The combination of open source operating systems such as Android and Linux, chipset vendors that supply a full SoC (system on chip) with their boards and low-cost manufacturing resources in countries like China and India has significantly lowered the barrier to become a device OEM. As a result, over the last few years, hundreds of new manufacturers have entered the market with competitively priced, feature-rich products that challenge big brand manufacturers.

Whether marketing to consumers or enterprises, or selling direct, in retail, through channels or online, mobile device manufacturers are rethinking their go-to-market strategies and business models. Their goal is to compete with a differentiated user experience that can build lifelong customer relationships and that can generate ongoing revenue streams beyond the product sale.

> "The combination of rugged Panasonic hardware, hardware-protected firmware architecture and Red Bend's advanced management software has created an incredibly powerful Enterprise-capable platform for our business customers. Our approach means that businesses will be able to deploy our Android-powered Toughpad computers to their mobile workers with world-class Enterprise software management and security capabilities."
>
> –*Stephen Yeo, European Marketing Director* at Panasonic Computer Product Solutions

This white paper is for manufacturers of mobile phones, tablets, automotive vehicles, consumer electronics and other wirelessly connected devices (in the paper, described as "mobile devices") that are interested in using their hardware products as platforms from which to deliver value-added services.

The paper describes how Mobile Software Management (MSM) can be used to achieve this strategy. With MSM, manufacturers can leverage a range of over-the-air technologies—firmware updating, application management, device analytics, policy management and Type-1 virtualization—both as differentiating features that can strengthen their offerings and as services to their customers. Readers will learn from case studies of how to successfully use MSM to deliver new integrated services.

Whether helping enterprise customers to manage thousands of devices in the field, or making a single consumer happier with their device experience, over-the-air software updating and device management services offer a strategic way for OEMs to differentiate their products and avoid the pitfalls of commoditization. In doing so, OEMs can transform their business and perhaps the entire industry.

Published: October 2013

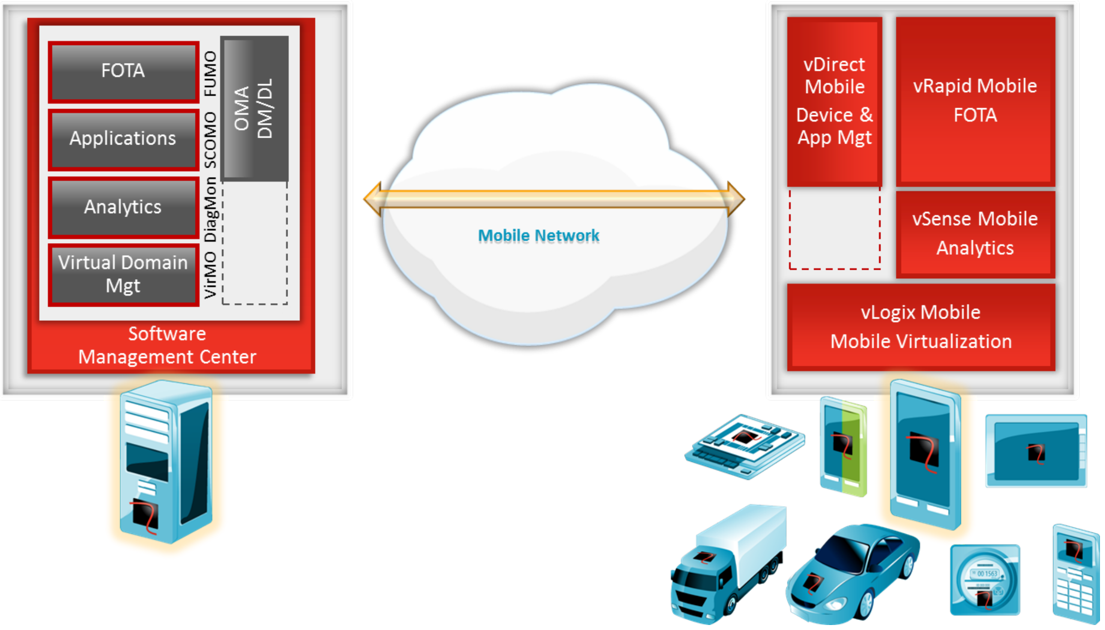
What is Mobile Software Management?

Mobile Software Management (MSM) encompasses a set of technologies and business processes that enable the management of all software assets (firmware, middleware and applications, whether embedded, downloaded or pushed) in mobile devices throughout their lifecycle.

An end-to-end MSM platform includes: 1) a back-end management system from which the OEM can trigger management commands over the air, and 2) client software pre-integrated into the mobile device that receives and performs the management actions. The MSM platform can be installed on-premise or accessed in the cloud in a Software-as-a-Service (SaaS) model.

Within the mobile industry, the most common standards to manage devices and their software are the Open Mobile Alliance Device Management (OMA-DM) standards. Mobile operators and device manufacturers utilize these standards to provision, configure and manage all devices connected to their networks or service in a uniform, secure and scalable way. Over the past five years, these standards are being leveraged beyond telecom to various industries now adopting MSM, including automotive, machine-to-machine (M2M) and consumer electronics. The standards include:

- Device Management (DM) – to bootstrap the device to the network or service, provision subscriber services and configure device settings
- Firmware Update Management Object (FUMO) – to update firmware over-the-air (FOTA) most commonly using delta technology to ensure the smallest update file size
- Software Component Management Object (SCOMO) – to add / remove / update applications
- Lock and Wipe Management Object (LAWMO) – to lock and / or wipe the device to prevent unauthorized access if the device is lost or stolen
- Virtualization Management Object (VirMO) – to create and manage multiple virtual machines running simultaneously on the same mobile device, such as for dual personas in BYOD (Bring Your Own Device)



Architecture of a Mobile Software Management Platform

Published: October 2013

Five MSM Services for Mobile Device OEMs

There are five MSM services that mobile device OEMs can offer to create a differentiated user experience and, in some cases, generate additional revenue streams beyond the hardware sale. These services can transform a hardware manufacturer into a service provider.

1) Firmware Updating: The Foundation of a Successful OEM Service Strategy

The most widely adopted MSM service is Firmware Over-the-Air (FOTA) updating. OEMs use FOTA to update the device's operating system to the newest version containing new features and performance improvements. This expanded service commitment, beyond basic product support during the warranty period, brings many benefits. It reinforces the OEM brand as a service provider, builds long-term customer loyalty, increases user satisfaction, reduces customer care and warranty costs, and enables the OEM to avoid a damaging product recall.

Today, nearly every type of connected device—smart TVs, game consoles, smartphones, tablets, point of sale (POS) devices, cameras, wearable devices including smart watches, chipsets, M2M modules, even cars and agricultural machines—get software updates OTA. It has become an expected feature and OEMs are at a disadvantage if they don't provide new OS versions OTA.

The reason is simple: FOTA is easier, faster, safer and more convenient than updating software with a USB cable via a PC, bringing the device back to a service center for repair, or dispatching a service technician on-site. OTA updates work over any type of cellular or Wi-Fi connection, even through power line communications (PLC) and inside the CAN network of a car. For example, GM, Mercedes-Benz (in the U.S.) and Tesla all use FOTA.

VERTU

Vertu, the world's leading provider of luxury mobile phones, has partnered with Red Bend Software, the industry's foremost supplier of FOTA updating solutions for the mobile market.

Red Bend manages the end-to-end FOTA service, from hosting to delivery of new software updates, via the Red Bend Software Management Center. Red Bend supports Vertu mobile devices across all platforms including the range of Android OS devices such as VERTU Ti, which was launched at the beginning of 2013.

"Vertu customers expect an exceptional level of service and reliability," said Vertu's Head of Software, Mal Minhas. "By working with Red Bend we can ensure that we are able to deliver product software improvements and a premium user experience continuously, with the easiest, fastest and most trusted FOTA updates."

For device users, FOTA ensures device health, reliability and relevancy throughout the product lifecycle. It protects the customer's investment and keeps them productive.

For device OEMs, FOTA represents a positive "touch-point" to make devices continuously better. Each update is a "gift" that engenders anticipation, excitement and gratitude. FOTA is an opportunity to communicate with customers directly to satisfy expectations and delight them.

FOTA also differentiates between branded devices and "no-name" devices. While selling a device with an older OS version may be acceptable for no-name OEMs that just want to "push boxes," not having a FOTA strategy is detrimental to selling premium and mid-range devices in a competitive market. Big brand OEMs that use FOTA include Apple, Samsung, Panasonic, LG Electronics, Sony, Sharp, Lenovo and Toshiba, all of which use FOTA across a variety of products. Increasingly, mid-size and specialized brands are adopting FOTA in order to compete on features, not just price.

The biggest benefit of all for OEMs, though, may be that the same service infrastructure used for FOTA updating can be a springboard for additional integrated services that can create a differentiated user experience and offer real revenue-generating potential.

2) Application Management: A New Revenue Stream for Enterprise Devices

Going beyond operating system updates provided with FOTA, mobile device OEMs can enhance the user experience with management of applications, whether the apps are pre-installed in the device before it ships, discovered and downloaded by users through an OEM-provided app store, or pushed to devices by the OEM. Application management use cases are possible for all types of mobile devices, including M2M devices used in utilities, security, logistics and Telematics, as well as for consumer electronics such as smart TVs and smart refrigerators.

There are several ways that mobile device manufacturers can leverage application management:

Manage OEM Applications Separate from Firmware

Device makers increasingly are developing their own software and applications to create a unique user experience. Some apps may be tied to OEM-specific services that are revenue generating. For OEMs that use open source operating systems, these software assets are beyond the generic OS, and are integrated together by the manufacturer to create the complete firmware version.

However, with MSM, manufacturers can manage their branded apps separate from firmware to leverage the much-faster update cycle for applications. These apps then can be managed as a group or individually, without requiring a complete firmware update. This means a shorter integration and testing cycle.

In addition, new OEM apps can be pushed to devices throughout the device lifecycle, not dependent on users discovering and downloading them from a public app store. This allows OEMs to add new revenue-generating apps and deploy them to the installed base immediately, increasing the OEM's addressable market for its apps and services.

For example, a children's tablet maker may provide a curated app store, or an application for parental control. A refrigerator maker may offer a new app that generates a grocery list based on planned recipes, or ties in directly to a local grocery delivery service. By separating these apps from firmware, the manufacturer can have greater control and realize faster time to market for new app updates and features.

Published: October 2013

For M2M devices, over-the-air application management can be used to deploy incremental functions, such as support for new payment methods. By deploying the new apps incrementally OTA, device makers can send smaller update files which saves bandwidth in data charges.

Offer Application Management to Enterprise Customers

Mobile device OEMs that serve the enterprise market also can benefit from application management, but as a SaaS service to their customers. From the same MSM system used by OEMs to manage their own applications, OEMs can let enterprise customers remotely manage a portion of the device software stack that contains enterprise-specific applications, separate from the OEM's applications and firmware.

To perform application management on enterprise mobile devices such as smartphones and tablets, many CIOs purchase third-party Mobile Application Management (MAM) systems. Such systems can cost $2-5 per month per device. However, with MSM, OEMs can provide integrated MAM as a value-added service to their enterprise customers and capture that ongoing revenue stream directly.

From the enterprise customer's perspective, buying an application management service from the OEM saves time and resources. IT administrators don't need to test and integrate additional MAM software into the device before being deployed to end users. The devices already can be MAM-capable – a simple activation with the OEM turns on the service. From there, enterprise applications can be pushed to the device either in user space or into the firmware, or even in a secure enterprise OS persona, depending on how the OEM has architected the device.

Using MAM to deploy and manage applications over-the-air is less labor-intensive and thus more cost-effective and more scalable than side-loading enterprise apps via a cable or SD card. It also is repeatable, even after device deployment, so that enterprise apps can be added / updated / removed throughout the device lifetime.

Compared to using a public app store such as Google Play for application deployment, an MSM-enabled app management service doesn't depend on users to discover and download applications. The OEM can enable the enterprise to manage apps for individuals and groups. Different users can have different sets of apps pushed to their device.

If an app store is requested, the OEM can use the MSM system to provide a private app store for discovering enterprise-approved apps. In this model, an icon on the device provides access to

Panasonic

Panasonic, a leader in ruggedized computing devices, uses Red Bend Software's market leading Mobile Software Management (MSM) solution in Panasonic's professional-grade Android-powered Toughpad tablets. This gives Panasonic and its enterprise customers the ability to remotely and securely manage their Toughpad devices over the air.

With Red Bend, enterprise applications are protected in a secure zone inside the Toughpad flash memory, ensuring that enterprise applications remain highly secure and tamper-proof.

With Panasonic Toughpad tablets, enterprises have the capability to manage their own applications independently from the tablet's firmware. This includes being able to deploy, remove and update any application efficiently and reliably over the air. In addition, Panasonic can deliver continuous software improvements to its enterprise customers, including keeping the Toughpad up to date with the latest Android version. The solution uses OMA-DM industry standards.

Published: October 2013

some or all of the enterprise's apps that are loaded into the MSM system. "Curated" app stores or catalogs discourage unauthorized device use, and let enterprises select apps they want their employees to use.

This solution is also suited for OEMs that provide special-purpose devices, such as POS tablets, sold to business customers. For example, a POS vendor serving the restaurant industry can offer a private app store with apps it has built or selected from approved partners.

An additional benefit is that using MSM to provide a private app store means the OEM does not necessarily need to become "Google Certified," which can be prohibitively expensive and unnecessary if access to public apps is not required for the target market.

3) Device Analytics: Improve the User Experience with Real-Time Data

As mobile devices become richer with features and functionality, understanding how devices are actually used is key to improving the mobile user experience and creating differentiated products and services. With MSM, OEMs can leverage an on-device agent to collect, monitor and analyze device usage, software performance and application behavior from the perspective of the user and device in the field. This insight can be used to improve the next firmware version or as inspiration when designing the next product.

For OEMs becoming service providers, collecting analytics information can be augmented with device "self-care" features, where users are prompted to take actions that may improve device performance, like deleting unused apps or files, or switching off apps that use a lot of data.

In addition, proactive self-care can reduce customer support costs and even reduce the number of devices being returned because they "don't work" when in fact the problem arises from user error or lack of knowledge. This phenomenon is known in the telecom industry as "no fault found."

NTT DOCOMO and Red Bend Software have jointly developed a product that addresses the risk of lost smartphones.

DOCOMO's Omakase remote lock application uses Red Bend's vDirect Mobile® device management software to provide peace of mind by halting access to personal information.

If someone loses an Omakase-equipped Android smartphone, he or she can prevent unauthorized access simply by contacting DOCOMO and having the device remotely locked.

おまかせロック
If you lose your mobile phone:
0120-005-250 (9 a.m. to 8 p.m.)
I just realized I don' t have my mobile phone!
The caller is verified to be the subscriber over the phone and then the mobile phone is locked by a remote operation.

Image Source: NTT DOCOMO

Analytics also can be offered as a service to enterprises. Enterprises can access real-time analytics data about application usage and performance from their employees and networked devices, gaining insight into productivity and reducing customer support calls. The MSM system can display reports and real-time status for a single user / device or groups of users / devices, and monitor trends over time. Such reports can include: software and application inventory and usage statistics, application network consumption and resource utilization, mobile usage behavior patterns and trends, device performance and application crashes.

For M2M devices used in manufacturing, retail, health care, utilities, transportation and logistics, analytics can be a particularly valuable service offering. It can report on device network coverage, and can prevent downtime.

4) Policy Management: Control Access and Ensure Security of Resources

Policy management is another service that OEMs can offer to enterprise and consumer customers as a differentiator from other hardware providers.

In BYOD, policy management enables enterprises to control employee access to corporate resources. It is also beneficial for devices used in services industries like telecom and utilities, for preventing unauthorized use.

Like MAM, many CIOs purchase Enterprise Mobile Device Management (E-MDM) systems in order to manage policies on enterprise-connected devices. These over-the-top EMDM providers charge enterprises $2-5 per device per month for policy management.

With MSM, OEMs can eliminate the need for third parties and offer integrated MDM services directly to enterprise customers as a value-added service. Policy management services can enforce the use of passwords and encryption, and can turn off functions such as the camera and Wi-Fi.

One common service is Lock and Wipe. If the device is lost or stolen, the enterprise can use the OEM-provided MSM system to lock and / or wipe the device instantly, thereby protecting access to the corporate network.

Lock and Wipe services also can be offered to consumers on a variety of consumer electronics devices, as a way to protect personal information and even to deter theft. For example, a digital picture frame vendor can offer a Lock and Wipe service in the event the frame is stolen to ensure privacy of the consumer's photos. Or, a Lock and Wipe service could be offered to car owners in case their vehicle is stolen to protect access to applications and personal content stored in the IVI system.

Sierra Wireless, which has adopted Red Bend's vRapid Mobile® FOTA client and vDirect Mobile® DM client since 2007, also licensed Red Bend's vLogix Mobile® for use in its AirPrime™ embedded wireless modules. Sierra Wireless' customers can extend their investment in apps written for 2G networks as they upgrade to 3G networks.

With vLogix Mobile integrated into AirPrime 3G modules, M2M app providers now have access, on a 3G device, to the industry-leading Open AT® Application Framework, originally designed for 2G networks. Red Bend's virtualization solution allows AirPrime customers to reduce costs and time to market by enabling the reuse of 2G software and apps when migrating to 3G.

"Red Bend enables us to simultaneously support two operating environments in our AirPrime SL808x devices, helping our customers to reduce the cost of transitioning to newer 3G networks without requiring them to rewrite existing applications designed for 2G," said Pierre Teyssier, Senior Vice President of Engineering, M2M Embedded Solutions for Sierra Wireless.

5) Type-1 Virtualization: Support Two Operating Systems on a Single Device

Virtualization technology is being adopted in mobile devices in order to run multiple operating systems simultaneously, separately and securely on the same hardware platform. One use case is to lower costs and increase time to market by extending the investment in legacy software but without requiring a change to hardware. This enables OEMs to retain customers longer.

In another use case, hardware manufacturers no longer need to wait for replacement cycles in order to sell another device to an existing customer. They can sell a second “virtual” device on the same product. Using the MSM system, a second OS can be deployed over the air. Or using the MSM system, a dormant OS can be activated over the air.

Dual-persona mobile devices represent huge potential for the next-generation of smart devices. The most effective way to create a device with dual personas is to use a Type-1 hypervisor that is integrated into the hardware. It provides the strongest security and highest performance for multiple OSes sharing the same hardware resources, without delaying time to market.

Dual-persona devices have great appeal to consumers. For example, a dual-persona tablet can separate a parent’s virtual tablet from a child’s virtual tablet. If the child unknowingly downloads a malicious application, it cannot affect the parent’s virtual tablet. This is particularly valuable for enterprise devices, where the work persona requires strong security, such as for BYOD.

For enterprises, virtualization is the ultimate solution for IT departments wanting complete control. By enabling the enterprise to deploy and maintain their own, completely separate OS on the device, OEMs can offer enterprises the same level of security as if employees use two physically different devices.

At the same time, dual-persona devices also meet the employee’s need to maintain privacy on devices that are being managed by IT. The IT administrator has no visibility, access or control over the personal OS.

Red Bend’s TRUE™ Solution for BYOD uses Red Bend’s vLogix Mobile Type-1 hypervisor along with Red Bend’s full Mobile Software Management capabilities to create a dual-persona smartphone or tablet that can be managed OTA by both the OEM (personal persona) and the IT administrator (work persona). The solution recently won First Place in the CTIA E-Tech awards in the Enterprise Solution – Security, Fraud & Privacy category.

Summary

Mobile device manufacturers can quickly and easily establish high-value, one-to-one customer relationships, build differentiated products and create ongoing revenue streams using Mobile Software Management (MSM) services.

With MSM, forward-thinking manufacturers can use their hardware products as platforms from which to deliver value-added services. By offering MSM services such as firmware updating, application management, device analytics, policy management and dual-personas, OEMs can stand out from the competition and avoid commoditization.

By integrating over-the-air management capabilities into their device offering, OEMs have the ability to capture revenue that today is being captured by third-party, over-the-top providers. Device manufacturers that adopt MSM can transform their businesses and change the dynamics of their industries.

About Red Bend Software

Red Bend® Software, the leader in Mobile Software Management (MSM) with more than 1.75 billion Red Bend-Enabled™ devices, makes mobile devices and services continuously better in a rapidly changing world. Red Bend is the only company that provides standards-based products and solutions for software management, device management, and mobile virtualization that work on any mobile phone and connected device uniformly, efficiently, and securely over the air. Red Bend enables its customers to stay competitive in a fast-moving market by helping them deliver high-value services on an increasing number of connected devices with growing software complexity. More than 80 leading device manufacturers, mobile operators, semiconductor vendors and automotive companies worldwide trust Red Bend with their most important assets—the mobile and connected devices their consumers depend on.

For more information about Red Bend's MSM solution, visit:
http://www.redbend.com/en/products-solutions/software-management

Corporate Headquarters
400 Totten Pond Road
Suite 130
Waltham, MA 02451 USA
Tel: +1-781-890-2090

Korea
6th Fl, MISO Bldg., 890-47,
Daechi-dong, Gangnam-gu
Seoul, 135-839 Korea
Tel: +82-2-2051-3482

Published: October 2013