Mobile Device Management A Functional Overview

Gopal Tatte[#1], Dr. G. R. Bamnote[#2]

[1#] *ME 1st Yr. Department of Computer Science and Engineering, Sant Gadge Baba Amravati University Prof Ram Meghe Institute of Technology and Research, Badnera, Amravati 444701, Maharashtra, India*
[1]*gmtatte@yahoo.com*

[2#] *Head of Department of Computer Science and Engineering, Sant Gadge Baba Amravati University Prof Ram Meghe Institute of Technology and Research, Badnera, Amravati 444701, Maharashtra, India*
[2]*grbamnote@rediffmail.com*

***Abstract*— Mobile devices are fast evolving and becoming more and more powerful in performance and more convenient to handle with their small form factor (SFF). With these advantages it is fast becoming a preferred device of choice for conducting enterprise functions. Bring your device (BYOD) is a classic example of acceptance by Enterprises to these SFF devices as standard tool for Enterprise functions. With these new devices comes a new challenge of managing these devices in Enterprise networks and applying or ensuring same level of safety and restraints as was applicable to standard enterprise desktops/notebooks. This paper talks about a generic architectural model and core components of Mobile Device Management solution as applied by enterprises to handle these SFF devices in enterprise network.**

***Keywords*— Mobility, Device Management, MDM, BYOD, SFF, Mobile Network, SCMDM**

I. Introduction

MDM (Mobile Device Management) is a wide umbrella acronym that covers whole array of mobility management and security tools. These can be deployed in a premises-based configuration or as a hosted service, managed or otherwise. Primary objective of these tools is to provide with a common management interface for Defining/Identifying devices, to apply policies related to usage, and distribution/managing apps.

With Significant CPU power and processing capacities, new age smart phones are strongly establishing themselves as a strong alternative for cumbersome desktop devices at enterprises. With more and more people bringing in these small form factors (SFF) devices to work, Enterprises are forced to think of these devices as preferred tool for their employees. Also with increasing adaptation of automation in enterprise businesses there is more and more use cases where enterprise provided hand held devices need to be carried in open fields outside enterprise's controlled networks creating serious data and security threats. Significant CPU power, SFF, Intelligent Wireless, and Capacity of broadband networks and abundance of apps availability is a strong convergence for an always connected always on workforce, all in turn forcing need for MDM solutions as an integral part of any Enterprise's network policies.

II. Core Functions

There are three core areas of functionality that should be integral to any comprehensive mobile management solution:

- Enable
- Secure
- Manage

This should be implemented in a process that is simple and efficient for both IT managers and mobile users:

- *Enable - Device Identification*:[2] Provision, the device for use in the corporate environment. This includes providing access to key corporate assets, like email, calendars, critical mobile applications, documents and media content Devices can be either managed i.e. registered with MDM tool as known device with proper authentication and provisioning to enterprise network, or rouge i.e. unknown or un registered devices

- *Secure - Device Connection*:[2] Secure the device and the data that is stored on it and passes through it. Activate appropriate password and access controls, and maintain separation of corporate data from personal data. For MDM controller/gateway to talk to device or for device to talk to MDM controller, there has to be a connection mechanism. This mechanism is typically provided through VPN over Wifi wherein all network traffic from cellular wireless wide area network

- *Device Management*:[2] Manage all devices centrally with real-time access to inventory, configuration and help desk functions. Get prioritized critical information through alerts and notifications that can be fully integrated into enterprise workflow solutions. It's typically performed by pushing group policies after collecting info from the device. These group policies can enable disable any device capability for eg. Switching off the camera once device enters a restricted zone

III. Core Components

Based on the core functions we'd typically have three main components to any MDM solution

- Gateway Server
- Device Enrolment Server
- Device Management Server

Additionally there would be some DB servers, Domain Controllers, Certificate Servers, LOB Servers etc. based on the nature of actual enterprise network. But above three would be where most of the action takes place from MDM perspective.

Following picture depicts high level overview of these components, and how they work with existing infrastructure

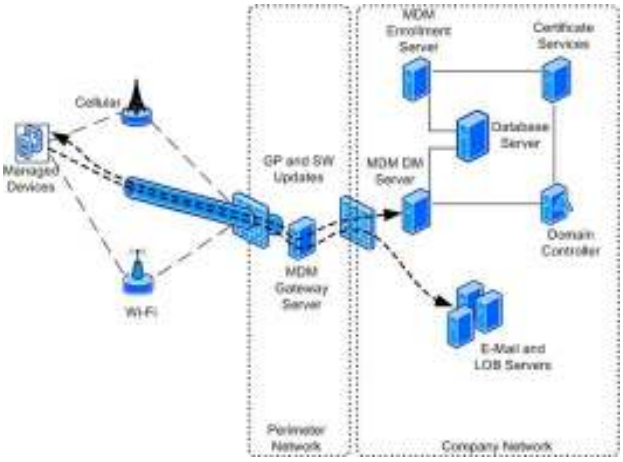

Fig. 1 A high level depiction of a typical MDM solution with its core components. [1]

A. Gateway Server

It's located in DMZ or screened subnet of enterprise network. It provides the way in to Enterprise network for managed device's sessions and provides way out for network and device management communication. It provides…

- Authenticates incoming connection for authorized devices
- Allocates a stable IP address for the device to enable Direct Push updates and support application persistence
- Enables fast resume and reconnect features for devices and applications
- Negotiates keys to encrypt traffic over the Internet

Following illustration shows the detailed architecture of MDM Gateway Server

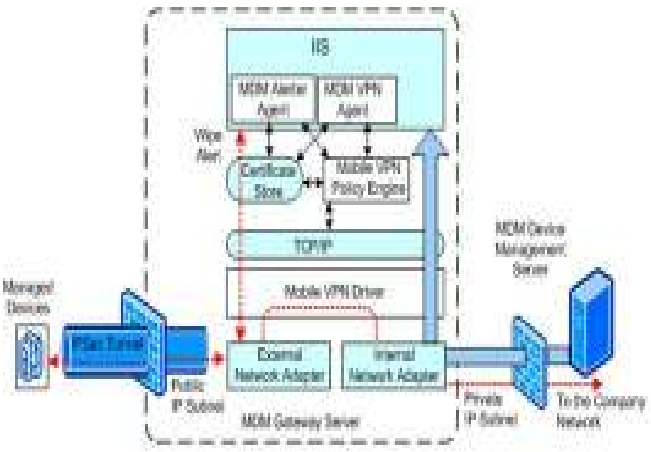

Fig. 2 Architecture of MDM Gateway Server [1]

Gateway Server is the pivotal access point for managed devices. Typically, this server is installed in your perimeter network where a defence-in-depth approach helps protect the network security of your enterprise. MDM Gateway Server is a stand-alone gateway that faces the Internet from inside the perimeter network. Typically, it is not domain-joined and shares no accounts or passwords with your enterprise domain. It does not directly use Active Directory Domain Service, NTLM, or Kerberos access to authenticate devices because these would require Mobile Device Manager (MDM) Gateway Server to be domain-joined or to store domain credentials.

MDM Gateway Server authenticates incoming connection requests by using an offline certificate evaluation process that queries the device machine certificate. It allows an end-to-end SSL session to be maintained between the client application and MDM application servers.

MDM Gateway Server has the following components [1]:

1) Certificate store: MDM uses machine certificates to authenticate Windows Mobile powered devices and MDM Gateway Server and MDM Device Management Server. These certificates are stored in the Windows Certificate Store.

2) MDM VPN agent: The virtual private network (VPN) agent handles communications between MDM Device Management Server and MDM Gateway Server. For MDM Gateway Server, the MDM Gateway Server cannot start communication with servers in the company network. For improved security, the MDM VPN agent does not start connections to MDM Device Management Server.

3) Mobile VPN policy engine: This component establishes and manages the IPsec tunnel to and from the device. It works with the Mobile VPN driver in the networking stack to enable the Mobile VPN client to establish authenticated and encrypted communications over the mobile operator network or through a Wi-Fi network.

4) MDM Alerter agent: The Alerter agent notifies the device that pending Open Mobile Alliance Device Management (OMA DM) commands are waiting, such as a device wipe. The Alerter agent then notifies the device to start an OMA session. The managed device communicates with MDM Device Management Server through the usual mechanisms and then retrieves the command.

5) Mobile VPN driver: The Mobile VPN driver manages network communications with the device. It checks that data coming from the device is valid and that the device has a valid IPsec Security Association (SA). If the connection is valid, the data is forwarded. If the connection is not valid, the data is discarded or is moved up the network stack to the Mobile VPN policy engine to negotiate a new connection.

B. Enrolment Server

Enrolment Server provides the services that are required to enable a Windows Mobile powered device to join the managed device environment.

The following illustration shows the architecture of MDM Enrolment Server.

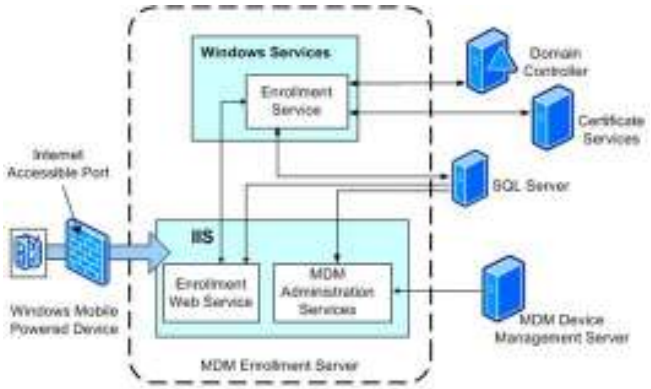

Fig. 3 Architecture of MDM Enrolment Server [1]

The MDM Enrolment Server has the following components: [1]

1) Administration services: This collection of Web services is functionally similar to the administration services on MDM Device Management Server. Because the Enrolment Web service uses TCP port 443, the Administration Services uses other TCP ports that the administrator can configure.

2) Enrolment Web service: Internet Information Services (IIS) hosts this Web service that manages incoming requests from Mobile devices to enrol in the managed infrastructure. After the Enrolment Web service receives a request, the service manages later communications with the Mobile device until it becomes a domain-joined managed device. Then, MDM Gateway Server handles the communications.

3) Enrolment service: This Windows service handles all communications to enterprises Active Directory Domain Service and PKI infrastructure. Enrolment Server provides a protected over the air (OTA) process to request and retrieve

certificates for devices. To help protect against malicious attacks, MDM Enrolment Server may use shared-secret encryption to perform protected enrolment over non secure connections, such as public General Packet Radio Service (GPRS), or other mobile data networks. This lets users enrol their device without having to cradle it and without having physical access to the enterprise network.

C. Device Management Server

Device Management Server provides the services necessary to interface the management infrastructure servers and services of an enterprise with MDM Gateway Server in the perimeter network. MDM Device Management Server transforms protocols that are used within enterprise to Open Mobile Alliance Device Management (OMA DM). This enables to manage Mobile devices in a manner similar to how we manage portable and desktop computers for an enterprise.

Device management includes the following tasks:

- Application distribution
- Group Policy application
- Firmware inventory
- Device wipe

The following illustration shows the detailed architecture of MDM Device Management Server.

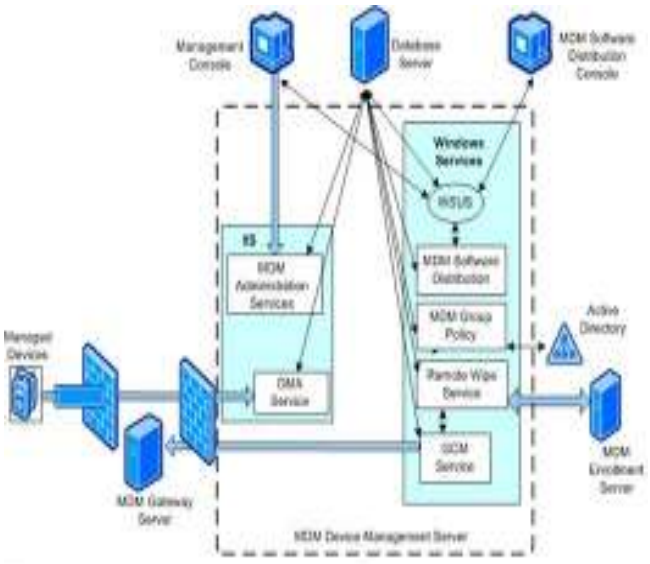

Fig. 4 Architecture of MDM Device Management Server [1]

MDM Device Management Server has the following components: [1]

1) Administration services: These Web services manage the administration tasks received from Mobile Device Manager (MDM) Console. When commands are received, the relevant service translates them into OMA DM tasks and then stores them in the relevant MDM database.

2) OMA service: This Web service works as an OMA proxy and enables the managed device to use OMA DM to communicate with MDM. This method provides more secure communication with systems in your enterprise network. The OMA service converts tasks from the MDM database into OMA DM commands and then sends them to the managed device for execution. When the device has completed the commands, the OMA service updates the database with the device status.

This service supports load balance arrays of MDM Device Management Server that provides a scalable architecture. You can use an appliance or the native Windows Network Load Balancer (WNLB) capability to load balance these arrays.

3) MDM software distribution: This service provides the interface to Windows Server Update Services (WSUS). All external communications use the standard WSUS interfaces. Therefore, no update to the WSUS servers is required.

4) Group Policy service: This service communicates with the Group Policy service on your enterprise domain controllers. This service determines the Resultant Set of Policies (RSOP) from the Active Directory Domain Service for each device object in the domain. The service translates Group Policy settings into tasks and then stores them in the MDM database. The OMA service processes them and applies them to a device the next time that the device connects.

5) Remote Wipe service: This service manages the command to wipe data from a managed device. This service is notified when a device has been wiped or the wipe command has expired. The service then does several things:

- It communicates with a domain controller to remove the Active Directory Domain Service object for the device.
- It communicates with the MDM Enrolment Server to revoke the device certificate and delete its account from Active Directory.
- It updates MDM Gateway Server and databases so that the device cannot connect to the system by using its previous credentials. The device can complete the enrolment process again if it has to re-join the managed environment.

6) Gateway Central Manager (GCM) service: This service helps overcome the difficulty of configuring a computer that is running MDM Gateway Server in the perimeter network in a more secure manner. The GCM service communicates configuration changes and updates to MDM Gateway Server. This communication is pushed through an SSL connection from MDM Device Management Server on the enterprise network to the management IIS instance on MDM Gateway Server.

IV. STANDARDS

Typical MDM is based on several open industry standards for mobile devices

- TCP/IP
- Open Mobile Alliance Device Management (OMA DM)
- IPsec and Internet Key Exchange Protocol Version 2 (IKEv2)
- IKEv2 Mobility and Multihoming (MOBIKE) protocol
- Software Component Management Object (SCOMO)

ACKNOWLEDGMENT

I'd like to thank Dr. G. R. Bamnote (Dean Faculty of Computer Science and Engineering Sant Gadge Baba Amravati University, Head ME Computer Science and Engineering Department PRMITR Badnera, Amravati) for his guidance and support in preparing this paper.

REFERENCES

[1] Architecture Guide for System Center MDM, Microsoft Corporation
[2] The 2011 Mobile Device Management Challenge - Defusing Mobile Anarchy in the Enterprise, Robin Layland and Joanie Wexter
[3] Best Practices: Extending Enterprise Applications to Mobile Devices – The Architecture Journal, Kulathumani Hariharan
[4] OMA Web site: http://openmobilealliance.org/
[5] SCOMO http://technical.openmobilealliance.org/Technical/Comments.aspx
[6] For the Internet Engineering Task Force (IETF) specification, see Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture, at this IETF Web site: http://www.ietf.org/