Whitepaper
Mobile Device Management

ecom Digital Products and Services

A PEPPERL+FUCHS BRAND

Your automation, our passion.

PEPPERL+FUCHS

www.ecom-ex.com

Author: Carl Henderson / Marco Kuhn

Content

Introduction: The modern mobility platform and its challenges

The use of smartphones and tablets as modern enterprise tools allows workers the flexibility to do their work wherever they are in a hazardous location. In addition to enabling mobile working, they also enable safer working practices, increased productivity and are a vital source of information for technicians when completing even the most complex of tasks while on plant.

While there are a wide range of benefits the growth in the use of Windows® 10 and Android™ devices on plant presents IT managers with a range of challenges to overcome if the devices are to be integrated into the corporate network and managed effectively. In addition, working with smartphones and tablets creates a number of data security and protection challenges that need to be overcome.

Depending on the particular enterprise mobility strategy, enterprises can select a large variety of device management models to equip their staff accordingly.

The main management models are:

- **BYOD (Bring Your Own Device)**
  where employees use their personal devices for work purposes although rarely seen in industrial environments
- **COPE (Corporate-Owned, Personally Enabled)**
  a model that allows enterprise owned equipment for personal use
- **COBO (Corporate-Owned, Business Only)**
  an allocation model in which the company's own equipment is made available solely for work tasks
- **COSU (Corporately-Owned Single Use)**
  where devices are locked down in a kiosk mode to perform only a single or small number of permitted tasks

Whether it is the corporate decision to allow BYOD, COPE, COBO or COSU or even a mix of several models, working with mobile devices must in be intuitive and user friendly for the primary device user and at the same time efficient for IT administrators to manage, while ensuring corporate security at the same time.

The standard way to enable smartphones and tablets to be enrolled and integrated into corporate IT effectively and in a secure way is Mobile Device Management (MDM). In addition, MDM systems meet statutory provisions and compliance requirements when working with mobile devices. An example of MDM is Blackberry UEM used internally by Pepperl+Fuchs.

1. Who is this White Paper suitable for?

This White Paper is aimed at Pepperl+Fuchs employees wishing to gain basic knowledge of Mobile Device Management Systems. It shows how MDM software helps IT managers and administrators to ensure security, visibility and control over the use of smartphones and tablets within the enterprise. It is also designed to eliminate any misconceptions and help people understand the role of MDM in our customer's organizations. In our view: An MDM system by no means has to be hard to set up or highly complex in order to perform its tasks with efficiency and reliability and is a must have solution for customers wishing to successfully execute enterprise mobility strategies.

2. What is Mobile Device Management?

Mobile Device Management is the umbrella term for a suite of software-based solutions deployed to deliver the centralized management, the protection of mobile devices and applications such as smartphones, tablets and enterprise applications in the corporate context. An efficient MDM system has intelligent functions to securely integrate the terminal devices into the company's IT infrastructure enabling productive, mobile working that complies with data protection regulations. Mobile Device Management solutions are available as cloud services often paid on subscription as Software as a Service (SaaS) or as on-premises software maintained on internal corporate servers.

3. So what's the difference Between EMM and MDM?

It's no longer just about the smart device. The evolution of enterprise mobility has started to focus more towards the information being secured and not just the mobile device. This means that information is no longer primarily stored on the hardware; instead it often now uploaded to a remotely accessible server or is a cloud back-end solution.

While that's a broad statement to make because there certainly are still solutions available that are still considered MDM solutions by the newer interpretation of the term, they are being phased out in favor of EMM solutions just for the simplicity and security that a total mobile solution offers.

Most EMM solutions in addition to MDM offer Mobile App Management, Mobile Content Management, App Wrapping, Containerization, and other features. This offers an all-encompassing solution that works to cover every aspect of the device.

In this whitepaper we have used the term MDM, because we are basically focused on hardware issues at present. Our solution eMDM is able to support a variety of EMM features as well.

4. Why is Mobile Device Management important?

An MDM system is used mainly for the configuration, enrollment and management of the mobile device estate as well as the protection of corporate data and resources.

Easy enrollment and configuration of mobile significantly reduces the workload of IT department and now widely expected within enterprise. Mobile Device Management makes it possible to execute models such as COPE through the MDM system providing for the integration of the desired devices into the company's IT architecture.

The MDM system handles the staging/deployment of countless mobile devices, saving the administrator from having to remove each device from the box and manually configure all settings and install the business applications. Device staging is extremely simple when the MDM system can be used with Android Zero-Touch. A similar solution to Zero-Touch is Apple's Device Enrollment Program (DEP) or Samsung KNOX Mobile Enrollment (KME).

If the MDM solution also has MAM (Mobile Application Management), the productivity apps can be installed and fully configured on a wide variety of devices from a management console with just a few simple steps.

With the diversity of the mobile devices used and often geographical remoteness of some users it would be particularly challenging for our customers IT department to keep track of versions of mobile operating systems, updates and keep the productivity apps up-to-date without MDM.

MDM also allows access rights, configurations, network settings and guidelines to be distributed and administered centrally.

5. The security is key

An MDM enables enterprise mobility although is importantly also key to the protection of company data. Because only by means Mobile Device Management can the terminal devices be used securely with protection against data loss or even data theft being provided in the event of the device malfunctioning or being lost. With MDM, companies can take immediate emergency action, e.g. locating a lost device via location tracking and deleting company data remotely (remote wipe).

MDM software also enables companies to define and enforce software and data policies as well as user rights according to role of the worker. The appropriate MAM options also make it possible to restrict the use of certain apps on mobile devices via an app filter.

6. The core role of MDM

6.1 Quick and intuitive enrollment and integration of mobile devices into corporate IT:

Time-saving integration of company-owned smartphones and tablets – thanks to MDM, the devices can be completely configured with just a simple steps with apps and policies distributed and managed from a central location anywhere in the world.

6.2 Back-up of company data and compliance with data protection:

With important features such as the strict partition of private and enterprise owned data, password requests and remote data wiping, MDM ensures that employees work with their mobile devices in compliance with the GDPR and that company data are fully protected.

7. Who needs an MDM solution?

The selection and use of an MDM solution has become standard practice for all enterprises wishing to ensure adequate data protection (GDPR compliance) and secure integration of the devices into their IT architecture.

For companies who use smartphones and tablets, an MDM system is recommended where there are 20 or more mobile employees, even if they only read business emails or use WLAN on their mobile devices.

8. What criteria is expected from MDM solutions?

To ensure the productivity of mobile workers and safeguard enterprise security as well as ease the burden on the IT department, the MDM system should meet the following minimum criteria:

8.1 Cross-platform solution

An MDM solution should support multiple operating systems and hardware platforms and ideally be able to use the native functions of the respective device manufacturer – e.g. the separation of business and private contacts from iOS 11.3 upwards or the Work Profiles on Android Enterprise.

8.2 Simple and Intuitive

The MDM platform must be easy to configure for the administrator with minimum effort. It should also integrate seamlessly into the company's existing IT infrastructure and Active Directory. This makes it easy to adopt roles and rights and minimize effort and expense.

8.3 Centralized set-up and configuration of the devices

It should be possible for policies, profiles and certificates to be configured centrally in a management console and be sent to the appropriate devices via mouse click. Check whether the MDM system supports Android Zero-Touch or Samsung Knox Mobile Enrollment.

8.4 Comprehensive Mobile Security

The MDM system must reliably protect the company data, the terminal devices and the connections between the mobile devices and corporate resources. In order to comply with the security aspect, the MDM solution therefore has features for password security enforcement, data encryption and blocking individual device features (e.g. file downloads or screen mirroring). In addition, the MDM system must enable the location and blocking of devices as well as the remote wipe of all data or only the company data should a device become lost or stolen.

8.5 Remote support and maintenance

If diverse locations are to be managed centrally, it is practical if updates, data, apps and configurations can be carried out and delivered centrally via MDM console.

9. The addition of MAM to the MDM stack

It is also an advantage if an MDM solution also has MAM functions. Mobile Application Management is about applying security and certain settings directly to apps. For example, MDM options can help ensure that an application can be encrypted and password-protected or can be deleted or uninstalled remotely. With MAM, administrators can distribute apps to mobile devices and fully configure them.

9.1 Data protection, security & compliance thanks to MDM

Data protection requirements have been on the increase for years. Since the entry into force of the EU General Data Protection Regulation (GDPR), which dictates the controllers of personal data must put in place appropriate technical and organizational measures to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data. An MDM solution helps companies to meet the requirements of the GDPR and their own compliance guidelines.

9.2 Mobile data protection is a must

As smartphones and tablets used in a company have access to the same data and resources as a standard desktop PC and servers, data protection also needs to be extended to the mobile devices. Therefore it is imperative mobile devices are securely integrated into the company networks and that security leaks or breaches can be ruled out.

9.3 Data protection through Mobile Device Management

The MDM system provides for GDPR-compliant separation of private and business data on mobile devices. Security measures and policies are enforced and monitored in a uniform way via the MDM console. For example, corporate password security policies become mandatory in order to protect systems against unauthorized access. User profile, email account, VPN and WLAN access are configured automatically.

9.4 Device allocation models need specific security measures

In COBO (Corporate-Owned, Business Only) and COPE (Corporate-Owned, Personally Enabled) scenarios, the devices must be operated in a fully managed mode where Android devices in Fully Managed Mode (also known as Work Managed Device). Android devices, separate work profile from personal data, In the event of a device being lost, the business area of the relevant terminal device can immediately be deleted remotely.

10. What ecom instruments GmbH offers?

Since summer 2019 ecom offers a new product range named "Digital Products and Services". One possibility for our customers is to apply for a service called "eMDM". This service can be ordered pre-installed at time of ordering the hardware. So the customer doesn't need to enroll their device, and can use the advantages of an MDM system instantly on.

If a customer already has their own MDM system, he can apply for a service named eCSL which enrolls his devices into his MDM as well. Compatibility of requested ecom hardware and existing customer MDM solution needs to be tested and verified for each request separately.

All other services are available for a large range of ecom products. Please get in contact with your local sales representative to get more info or visit www.ecom-ex.com/eDS.

11. References

https://developers.google.com
https://www.samsungknox.com
https://www.cortado.com

Your automation, our passion.

Explosion Protection

- Intrinsic Safety Barriers
- Signal Conditioners
- FieldConnex® Fieldbus
- Remote I/O Systems
- Electrical Ex Equipment
- Purge and Pressurization
- Industrial HMI
- Mobile Computing and Communications
- HART Interface Solutions
- Surge Protection
- Wireless Solutions
- Level Measurement

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- Fieldbus Modules
- AS-Interface
- Identification Systems
- Displays and Signal Processing
- Connectivity

Pepperl+Fuchs Quality
Download our latest policy here:

www.pepperl-fuchs.com/quality

PEPPERL+FUCHS

www.pepperl-fuchs.com
Subject to modifications · © Pepperl+Fuchs
Author: Carl Henderson / Marco Kuhn / 04|2019