White Paper – Mobile Device Management.

Mobile Device Management is the key enabler for secure enterprise mobilization.

New era of mobility needs professional management to obtain full range of benefits.

Life is for sharing.

Management Summary.

Mobility has reached a higher stage of sophistication and customization, which in turn opens the door to an unprecedented range of benefits. Today, mobile workers in remote locations are wirelessly connected to advanced applications with their own devices, such as smartphones or tablet PCs. This leads to a massive expansion of the enterprise environment, higher responsiveness and increased competitiveness.

Enterprises must currently master a multitude of challenges regarding asset diversity, data security, privacy, liability and trust. This increased complexity, which multinational corporations (MNCs) face on an international scale, needs to be handled in an efficient manner. Only so can advanced capabilities be properly deployed in a way that benefits outweigh risks arising from the distributed environment.

Crucial to success are well-defined mobilization strategies and mobility policies; lean telecom management processes; transparency regarding devices and applications as well as company policy compliance, especially with respect to security and privacy. Therefore, Mobile Device Management (MDM) is a key enabler in gaining a competitive edge for the core business. However, it is also a challenge for CIOs who are compelled to embrace the role of business innovators.

In order to achieve the adequate MDM proficiency level either a software-as-a-service (SaaS) or business process outsourcing (BPO) approach can be taken. To avoid the risks and barriers associated with a move to BPO, many companies choose an SaaS model, which includes advice and training from third party consultants. Experienced third parties can advise on MDM best practice; help gain control over assets, services and associated processes; and finally provide support in order to mobilize the entire enterprise with feature-rich, sophisticated MDM systems.

The SaaS approach provides the opportunity to reach best-in-class MDM proficiency within a relatively short timeframe. The customer stays in control of its telecom management processes while taking advantage of involving a knowledgeable third party. SaaS also has the benefit of a “start small, grow big” approach, as it can be first introduced into a few organizational units and then expanded upon successful implementation. Even for companies considering a mid to long-term move to BPO, embarking initially on an SaaS model provides a much better basis for evaluating whether the move to BPO would be valuable and acceptable.

Key issues.

Shift to Mobility 2.0, mobilization of business processes, enhanced competitiveness, increase in mobile workforce, trend toward Bring Your Own Device (BYOD), expansion of the work environment, mobilization strategy, mobility policies, sensitivity to data security, privacy and liability, trust environment, necessity of transparency, challenges for MNCs, MDM proficiency, MDM delivery models, MDM benefits vs. MDM cost, selection criteria for MDM provider.

Who should read this White Paper.

CIOs and CTOs; global, regional, as well as national IT and telecom managers; HR and compliance officers; and procurement executives.

Table of contents.

1. **Mobility is already an indispensable fact of life and is moving to the next stage of development.** 4
   Build Mobility 2.0 into your processes and gain competitive advantage.

2. **Advanced mobility has become complex and needs professional management.** 6
   Effectively handle user differentiation and security needs.

3. **Leading edge MDM solutions enable effective business-process mobilization and complexity management.** 7
   Allow for a tailored application set and a secure environment, while retaining native user experience.
   - 3.1 Key challenges to be solved. 7
   - 3.2 Main MDM approaches. 7
   - 3.3 MDM functionality. 9

4. **Security and native experience determine the MDM approach, while technology drives the MDM delivery model.** 14
   Realistically assess security needs and take advantage of third parties' skills, while staying in control.
   - 4.1 MDM core needs and available approaches. 14
   - 4.2 Defining the deployment strategy. 14
   - 4.3 Selecting an MDM delivery model. 15
   - 4.4 Cost versus benefit considerations. 16

5. **Selecting the appropriate MDM provider requires foresight and knowledgeable analysis.** 18
   Focus on concrete delivery capabilities and benefit from provider advice.
   - 5.1 MDM players. 18
   - 5.2 Outlook. 18
   - 5.3 Selection criteria. 18

1. Mobility is already an indispensable fact of life and is moving to the next stage of development.

Build Mobility 2.0 into your processes and gain competitive advantage.

Mobility has been redefined by user needs and evolving technological capabilities. As it becomes mainstream, differentiated user clusters have emerged: those working in multiple locations within a geographic region, business people who frequently travel abroad, employees working in various areas on company premises as well as those operating from diverse remote locations.

Advances in mobile data technologies, services and software have enabled wireless access to machines and applications. Person-to-person communication complemented by mobile machine-to-machine (M2M) communication has opened up opportunities for an unprecedented redesign of various business processes. This applies to both external processes geared toward customers and suppliers and internal processes such as back-office, design and production.

Today, remote workers – often in very distant locations – expect to have a similar work environment as when working at a stationary location. In parallel, the number of devices continues to substantially increase due to the utilization of multiple devices per user as well as specialized devices for M2M applications. In order to create the user experience required for new usage scenarios and applications, a realm of innovative and powerful terminal devices has emerged. These include smartphones, dedicated terminals and tablet PCs.

This above-described shift to Mobility 2.0 has three major implications:

- A massive expansion of the work environment with core capabilities and critical data distributed to ever-changing locations. In addition to the primary but increasingly difficult task of keeping track of assets, this expansion raises the challenges of ensuring a secure environment and of maintaining an adequate level of homogeneity in terms of business processes and standards.
- An increasingly blurred border between the the work environment and the private domain. This leads to changes in leadership style regarding performance management and company policies, especially concerning the shared use of devices and services for business and private use. Trust between enterprises and employees as well as liability and privacy issues need to be thoroughly reviewed. The shared use of devices can have two forms: company equipment used for private purposes or employee devices used for business purposes, today labeled as “Bring Your Own Device (BYOD)”.
- As a consequence of the first two implications, there is a vital requirement for clear and committed company policies as well as stringent, agile security concepts and sophisticated remote management tools.

MNCs are faced with these mobility developments on a global scale, as they operate in various countries around the world, deploying and shifting resources dynamically between geographical locations. Business processes need to be flexibly replicated in new environments with new operators and partners. Management and international team members who frequently travel abroad depend on reliable, continuously available means of communication.

Overall, mobility is a powerful means for gaining competitive advantage by allowing fast and informed decision-making, efficient processes and flexible work time windows. Therefore, the implementation of mobility should follow a comprehensive approach geared to realizing the full range of advantages as well as balancing the cost-benefit relation.

2. Advanced mobility has become complex and needs professional management.

Effectively handle user differentiation and security needs.

Sourcing, implementing and operating advanced international mobility environments, often combined with fixed line and IT services, is inherently complex. A multitude of providers in different countries offer various services and applications for voice and data aimed at user clusters with different types of needs and roles. Rapidly increasing portfolios of powerful devices are flooding the market with ever-shortened contract durations and lifecycles.

BYOD intensifies this trend. Today's devices, especially smartphones and tablets, have different form factors, various operating systems – like iOS, Android, Windows Mobile, BlackBerry or Symbian – as well as diverse telco and IT capabilities. These complex devices must be integrated into an enterprise environment aimed at structured and optimized processes while keeping costs in mind.

Organizations typically use two types of scenarios to manage mobile device use: the "Enterprise Liability (EL)" scenario – sometimes also referred to as "Corporate Liability (CL)" – and the "Individual Liability (IL)" scenario (Chart 1). In the EL scenario, the enterprise provides its employees with a ready-to-use mobile device and service, remains the device owner, is liable for all data stored on the device and bears the cost for both the device and the service. In the IL scenario employees use their own private mobile device while the liability for the content is distributed between the employee and the enterprise. The employees bear the cost for the device of their choice and the service cost is shared between the enterprise and the employee. In both scenarios the enterprise assumes the responsibility and the cost for MDM. For a dedicated view on BYOD, please refer to our White Paper: "Bring Your Own Device. How to leverage the benefits of mobility while managing costs and security".

Each company within an MNC must take organizational measures when an advanced mobility environment is introduced. Policies need to be implemented that foster efficient work styles and a desired level of business versus private usage. They should simultaneously take national regulations and conditions into account, particularly legislation regarding privacy, which is significantly different between countries. The most crucial aspect, however, is to create a secure environment for the expanded enterprise.

Managing such a complex mobile and IT ecosystem on an international scale is increasingly difficult, both from the sheer amount of resources needed and the highly specialized skills required. Accordingly, "Mobility Initiatives" are at the top of the communication priorities of CIOs. Not surprisingly, telecom consultants and service providers are becoming increasingly overwhelmed with customer inquiries from telecom and IT professionals on topics related to mobility. However, despite being crucial for overall business, telecommunication management is a support function, not the core business of MNCs.

The fundamental first step for overcoming the challenges of mobile complexity is to gain visibility regarding the services and assets, devices and applications as well as to establish policy compliance across the international footprint of the MNC organization. However, according to customer feedback most MNCs lack sufficient transparency to effectively manage their mobile and wireless environments.

Mobile Device Management is an indispensable tool for managing the full spectrum of mobility requirements and options, while providing an appropriate level of protection. Security, particularly on a device that combines personal and business data, is a key issue in today's distributed and diverse work environments. A centralized approach is better able to implement a sophisticated and robust MDM solution, since it is more likely to ensure that an adequate amount of skilled resources and a sufficient budget will be dedicated to this mission-critical task.

BYOD Impacts the Cost for MDM, Devices and Services Differently.

MDM costs are paid by the enterprise, device costs by the employee, while communications cost are shared.

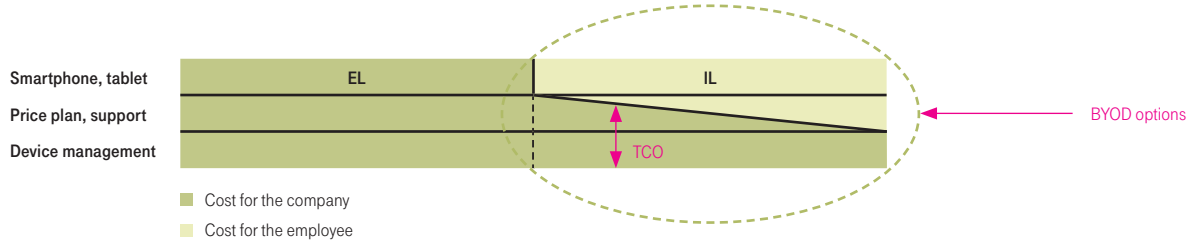


Chart 1

3. Leading edge MDM solutions enable effective business process mobilization and complexity management.

Allow for a tailored application set and a secure environment, while retaining native user experience.

MDM goes far beyond mere device management. It is the essential instrument for implementing an advanced mobility strategy (Chart 2) and enables the comprehensive mobilization of an enterprise's business processes. Based on thoroughly defined mobility policies, MDM allows MNCs to keep track of both hardware and software assets, configure device settings, provide function-specific application sets and manage the data on the devices. Best-in-class MDM ensures that these functionalities are performed in strict accordance with the defined policies in an enhanced security environment. It also provides a platform for both administrators and users to perform these management functions in line with their respective roles.

3.1 Key challenges to be solved.

CIOs are faced with an increasing demand to mobilize the businesses they support. Best-in-class MDM approaches provide solutions for several key challenges:

- Gain an overview by establishing and maintaining a comprehensive and insightful inventory.
- Manage the "universe" of devices to ensure comparable standards and functionalities, across operating systems.
- Enable different business processes by creating tailored sets of function-specific applications, in addition to a common core of general applications.
- Handle business/private coexistence either through a clear separation between the business and private domains or by defining clear procedures for each domain.
- Warrant security by providing the rules and the means and by ascertaining disciplined use.
- Simplify MDM processes by designing versatile and user-friendly systems.
- Keep the cost of mobilization and customization within bounds.

Mobility Strategy Provides the Framework for Defining the Mobility Policy.

The mobility policy drives MDM functionality.

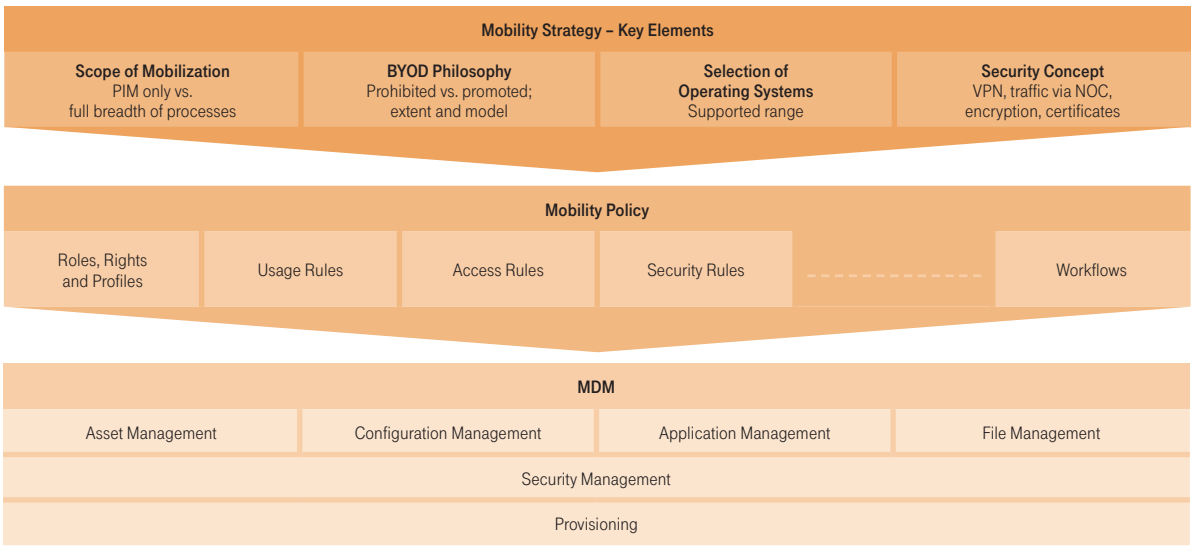


Chart 2

3.2 Main MDM approaches.

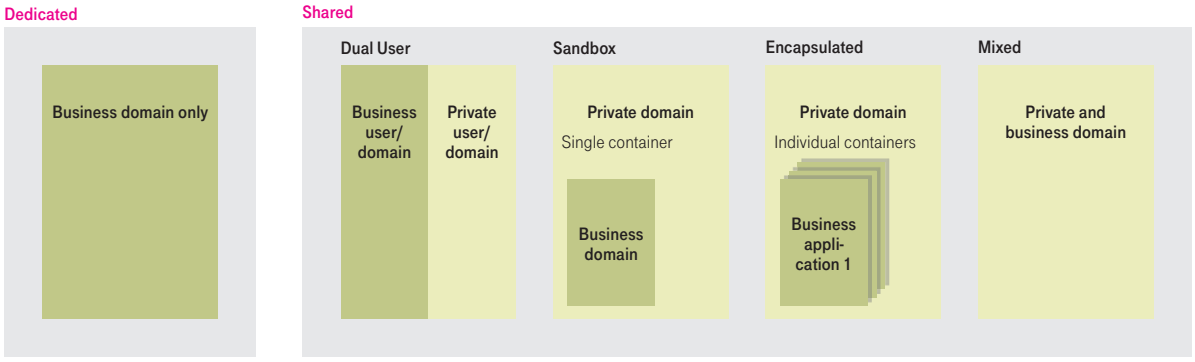
Providers have addressed MDM in several ways, partly influenced by their previous and/or adjacent activity areas. Several MDM approaches have been established in the market, which fall into two broad categories (Chart 3):

- **Dedicated** approaches manage devices aimed only toward business use with provider-defined – usually proprietary – solutions that dictate a predetermined user experience.
- **Shared** approaches manage devices aimed toward both business and private use and apply various methods to handle the two domains:
  - **Dual User** approaches completely separate the business domain from the private domain and manage the business domain only, using a proprietary approach. Such approaches virtually create two devices with no communication between the business and the private domain. The business user experience is typically different from the private user, native experience.
  - **Sandbox** approaches separate the business domain from the private domain by isolating all business data and applications in a container. Primarily the business domain is managed, which implies the compulsory use of a proprietary approach not only for specific applications but also for common business applications like email, calendar, contacts and browser. This prevents a seamless native user experience.
- **Encapsulated** approaches separate individual elements of the business domain from the private domain and manage mainly the business domain. Applications relevant for native user experience can be used both in the business domain and the private domain, ascertaining a quite advanced degree of native user experience. Encapsulated approaches have evolved from mixed approaches and seek an enhanced degree of security.
- **Mixed** approaches provide joint location for the private and business data and applications. Business items are marked and handled accordingly. By building on the functionalities of the respective operating systems, this approach allows for a seamless native user experience.

The main differences between the approaches are the degree of native experience and the security level created by separating the business domain from the private domain.

MDM Vendors Take Very Different MDM Approaches.

Degree of native experience and aspired security are the main differentiators.



- Only business data and applications allowed
- Provider-defined, single user experience

- Complete separation of business and private data and applications
- No communication between business and private domain
- Business domain user experience usually different from native user experience in the private domain

- Isolated location of all business data and applications
- No communication between business and private domain
- Business domain dictates basic applications, thus preventing a seamless native user experience

- Individual isolation of business data and applications
- No communication between business and private domain
- Applications relevant for native user experience can be used both in the business domain and the private domain

- Joint location and protection of business and private data and applications, with markers on business data and applications
- Allows configuration and control of business data across the device without limiting native user experience

Chart 3

3.3 MDM functionality.

Irrespective of the approach taken, MDM systems need to address a set of functionalities in order to create powerful solutions to the key challenges outlined (Charts 4, 6 and 7):

- Asset management
- Device configuration
- Application management
- File management
- Security management
- Provisioning

While most of the MDM functions are "vertical" and relate to particular tasks, security and provisioning are largely "horizontal" functionalities, which mean that they have implications across the whole set of functions. In order to enhance the security or provisioning for specific "vertical" functions, providers may also implement security or provisioning features geared only at these "vertical" functions. For the sake of coherence, these specific security and provisioning features will be treated within the "vertical" function they belong to (Chart 4).

Some MDM vendors incorporate certain Telecom Expense Management (TEM) features in their MDM systems, such as service cost analysis. Other suppliers have full-fledged TEM products for this adjacent market, seamlessly integrating their MDM and TEM solutions.

Best-in-class providers go a step further. They additionally offer mediation platforms which enable the integration of solutions from different vendors, making them accessible with a single sign-on and drawing on a common database.

This White Paper focuses on the functionalities for MDM. For deeper insight into TEM functionalities please refer to our White Paper "Telecom Expense Management. Telecom Expense Management strikes the balance between optimal service and cost".

Best-of-Breed MDM Solutions Provide a Rich Feature Matrix*.

Application management is the crucial vertical function in enterprise mobilization and a key differentiator.

	Vertical Functions			
	Asset Management	**Configuration Management**	**App Management**	**File Management**
	▪ Device inventory ▪ Device registration ▪ Device details ▪ Device retirement ▪ Device designation lost/found ▪ Device ownership status	▪ Device configuration ▪ Device settings (VPN, Wi-Fi, POP/IMAP, SCEP, APN, CalDAV, CardDAV) ▪ Device provisioning	▪ Install, update, uninstall ▪ App settings ▪ Installed apps inventory ▪ On-device inventory	▪ File push ▪ File delete ▪ File restore ▪ File inventory ▪ File wipe ▪ Selective file wipe
Function Specific Security	▪ Device location, lost or stolen (over mobile cells or via GPS)	▪ Device function lockdown (camera, SD-cards, Bluetooth, Wi-Fi)	▪ Secure distribution, updating and withdrawal of in-house applications using certificates ▪ Mandatory presence of mission-critical apps ▪ Preventing from running non-permitted apps via blacklist ▪ Blocking of email access ▪ Allowing /blocking Active Sync ▪ General logs, email client, MDM, certificates logs ▪ Communication history ▪ Usage of voice, SMS, data	▪ File encryption ▪ Mandatory use of data protection
Function Specific Provisioning	▪ Block registration ▪ Device self-registration ▪ Device self-location and mapping		▪ App distribution library ▪ Recommended app store apps ▪ Access control for distributed in-house apps	

* most relevant features

Chart 4

- **Asset management** starts with the registration of all mobile related assets, both hardware and software, including relevant details for each item. It records ownership status and keeps track of lost as well as found devices. Retirement of hardware is also carried out. Such modules often link into the enterprise's accounting systems, which are used for official reporting.

  State-of-the-art asset management modules consist of a unique, exhaustive asset database. This enables proactive, sophisticated asset portfolio analysis and management. User preference patterns can be derived and adjustments to the portfolio proposed, while obsolete and unused devices can be discarded. Specific security provisions allow for location of lost or stolen devices via the base stations in the mobile network or via GPS. With such systems, asset management functions can be easily performed both by the administrator and the user, e.g. registration of new devices or location of lost or stolen ones.

- **Device configuration** provides and updates the settings for the heterogeneous "universe" of mobile devices, smartphones and tablets, thus creating a largely harmonized configuration base across various devices and operating systems. This includes settings for Wi-Fi access, VPN integration, APN assignment, POP/MAP allocation as well as protocol selection, e.g. SCEP, CalDAV, CardDAV.

  Advanced configuration systems interact with the asset management database in order to provide relevant configuration parameters for each item, which are then processed for the advanced asset analysis. Specific security features allow for the lock-down of certain functionalities on devices. For example, cameras, SD cards, Bluetooth communication or Wi-Fi access can be prohibited.

- **Application management** distributes and replaces applications to the mobile and dispersed workforce. They are installed with the requested settings and configurations (e.g. for the corporate email account), updated and, when necessary, uninstalled.

  True, effective and efficient mobilization that dramatically extends the reach of the enterprise is only possible with MDM. It is the key enabler for mobilizing business processes, by supporting with a mandatory set of applications – which ensures a standardized core of business tools – and optional applications which further facilitate the business processes and their environment.

  Best-in-class application management modules create a thorough overview of the applications available on each device through on-device inventories. Advanced security features, such as those based on certificates that are dedicated to application management, create a highly protected environment for the secure distribution, updating and withdrawal of the application. These systems guarantee the availability of all mission-critical, mandatory applications, both general and business-function specific, to every user group (Chart 5).

  Once installed, features like whitelists and blacklists ensure that only desired applications are run on the devices by preventing the launch of any unwanted applications. According to the provisions of the respective mobility policy several kinds of actions can be taken, spanning from alerts and messages to both the user and administrator, to blocking of emails and synchronizations or even wiping the devices.

Versatile Mobile Enterprise Applications Platforms are User Targeted.

Each user group has access to general enterprise as well as business-function specific applications.

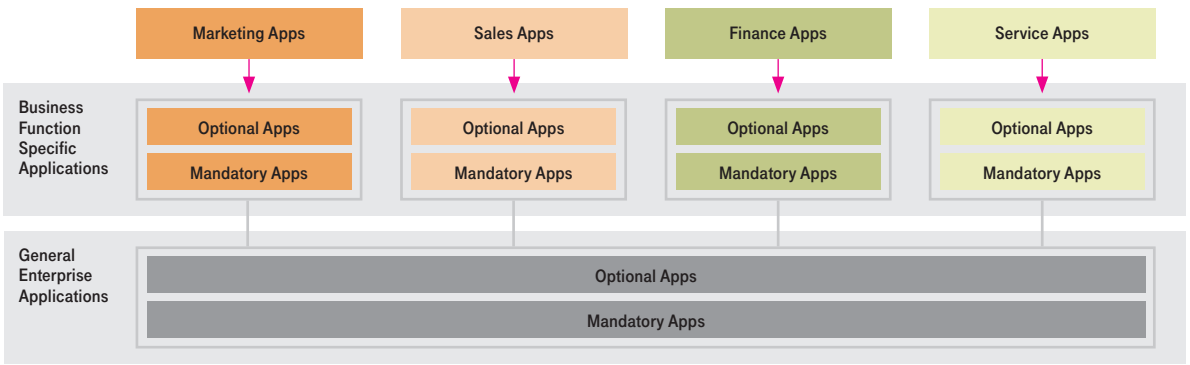


Chart 5

Additionally, history logs for all types of communication can be generated and stored, e.g. email, calls, SMS or data exchange. These features are highly sensitive as they touch enterprise security on one hand and personal privacy on the other. Different countries have different philosophies on how to strike the balance between the two areas. Accordingly, various regulations apply even if there is a core standard of legislation for certain regions like the EU. Therefore, the specific policies in each country need to be thoroughly analyzed and taken into account when configuring advanced security features.

Scenarios in which both enterprise and private applications are located and used on a device, e.g. in a BYOD case, require special attention. Not only do applications from the enterprise sphere need to be strictly separated from applications in the private domain, it also has to be ensured that applications from one domain do not access data from the other. As an example, advanced modules prevent content from the business email application from being copied to the concurrently running private email application.

Similarly, emergencies, such as when a device is lost, stolen or suspected of a fraud attack, need special treatment. Malicious use of business applications must be prevented by blocking or even by wiping these applications. Wiping particularly needs to be handled very carefully when enterprise and private applications are collocated. It has to respect the liability that the enterprise assumes for the private domain as outlined in the mobility policy and related rules. While selective wiping is possible with advanced systems, policy provisions could also lead to a complete wiping of the private applications.

With leading application management modules, provisioning includes application distribution libraries or dedicated enterprise application stores, which allow employees to comfortably access general as well as dedicated application sets (Chart 5). These contain both mandatory and optional applications. In the most sophisticated systems the employee is given access only to a shop targeted to specific business functions and roles. This consists of applications only relevant to his or her profile.

- **File management** takes care of storing, securing, retrieving, restoring and deleting files. It is a basic function, but it deals with one of the most valuable resources companies have: enterprise data. These data contain the know-how of the company as well as information entrusted to the enterprise by third parties, e.g. customers and partners.

Apart from general safety measures for protecting the entire environment, state-of-the-art file management modules provide a means of securing individual documents or sets of data. A crucial function of such modules is the ability to react in the emergency cases mentioned above, i.e. lost or stolen devices or fraud suspicion. As with applications, data is remotely wiped, either selectively for devices with mixed business and private use, or even totally. The selected course of action for mixed-use devices such as those in a BYOD scenario depends on the mobility policy and the level of liability taken by the enterprise for the private data on the device.

Best-of-Breed MDM Solutions Provide a Rich Feature Matrix*.

Security management, both general and function-specific, is critical for implementing enterprise mobilization.

	Vertical Functions			
	Asset Management	**Configuration Management**	**App Management**	**File Management**
Overall Security	▪ Password and encryption policy (phone, SD-cards, internal storage) ▪ Password enforcement ▪ Overall wipe ▪ Selective wipe enterprise configuration & settings (Wi-Fi, VPN, certificates) ▪ Selective wipe enterprise app profiles ▪ Selective wipe enterprise email/PIM ▪ Selective wipe SMS ▪ Lock ▪ Lockdown (camera, app install, safari, YouTube, iTunes, content) ▪ Passcode to unlock		▪ Unlock ▪ Remote lock and wipe ▪ Silent enforcement of profiles update and security ▪ Wakeup client/forced device check-in ▪ Virus scan ▪ Backup snapshot ▪ Active Sync connection monitor ▪ Version or compliance ▪ Certificate distribution ▪ Corporate certificate authority protection ▪ Root detection ▪ Allow/block actions by OS type	

* most relevant features

Chart 6

- **Security management** provides a safe environment across all MDM management modules. It addresses the main risks of enterprise mobilization, which inherently result from the massively expanded business environment. While application management provides the rich universe of necessary mobile applications, security management removes the main barriers to their implementation. It gives both functional and IT C-level management the required degree of confidence for pursuing business mobilization.

  High performance security management modules ensure that general access to the mobile environment is only possible through elaborate passwords, which are changed at regular intervals (Chart 6). Sophisticated encryption algorithms are used to protect all elements in the business domain and, where applicable, also in the private domain.

  A key function of the security management modules is to foster and enforce security and protection measures set out in the mobility policy. Beyond the compulsory use of passwords, this includes “silent” updates of profiles and security settings as well as monitoring of versions and compliance. State-of-the-art security management modules proactively examine the risk environment and the security posture of the user. Attempts to circumvent security measures are also detected and countermeasures are initiated.

To diminish the damage in case of loss or accidents, such systems periodically create back-ups and synchronize the data and applications according to predefined sync policies. If a device has been lost or stolen, or if fraud tampering is suspected, the security management modules swiftly react with measures corresponding to the level of threat. Actions range from blocking certain functions and prohibiting sync processes at the hardware as well as software level to selectively or fully wiping the data, applications, settings and other data on the devices.

Powerful security management ensures the highest security level for each device type. Accordingly, when users migrate across various devices, this provides a similar high level of security for each specific device.

Best-of-Breed MDM Solutions Provide a Rich Feature Matrix*.

Provisioning lays the foundation for user friendly, lean, flexible processes.

	Vertical Functions			
	Asset Management	**Configuration Management**	**App Management**	**File Management**
Overall Provisioning	▪ Central web-based console across operating systems ▪ Role-based access ▪ Remote access ▪ Per device actions ▪ Group actions ▪ End user self-service (by invitation)		▪ Remote device lock, unlock, wipe ▪ Self lock/wipe by user ▪ Send message ▪ Certificate distribution for Exchange, Wi-Fi, VPN ▪ Auto-enrollment and renewal of certificates	

* most relevant features

Chart 7

- **Provisioning** enables the involved parties to perform actions for using the functions of the various MDM modules. It is aimed at structuring and simplifying the tasks. Provisioning also manages the inherent complexity resulting from the requirements of administrators and end users: rich functionality and enhanced handling friendliness. Up-to-date provisioning allows various roles to be defined and provides differentiated access based on those roles (Chart 7). It thereby permits administrators to control the most critical actions while end users receive their own set of actions. This creates a win-win situation: end users save time and are more flexible, while less effort is required from administrators.

  An additional level of flexibility is introduced by provisioning systems that enable remote and over-the-air (OTA) service. This gives both the administrator and end user the possibility to take action independent of the location of the device. The ultimate freedom for the end user is achieved by systems that allow self-service through the mobile device itself.

But cost saving in this self-service ecosystem will only be achieved if servicing by the end user is as efficient as that performed by the administrator. Clumsy and inefficient systems that need extensive training and expert support will offset any potential savings.

Advanced provisioning systems make it possible for administrators to service both individual and groups of devices across operating systems via web-based consoles (Chart 8). Messages can be sent and wake-up client alerts can be activated. Additionally, end users can perform a wide range of management functions aimed at their own devices.

Beyond the efficiency aspect for administrators and users, user friendliness is a crucial factor for the acceptance of MDM, contributing significantly to the willingness to comply with the mobility policy.

Provisioning Lays the Foundation for User Friendly Processes.

In flexible systems, both administrators and end users can perform MDM functions.

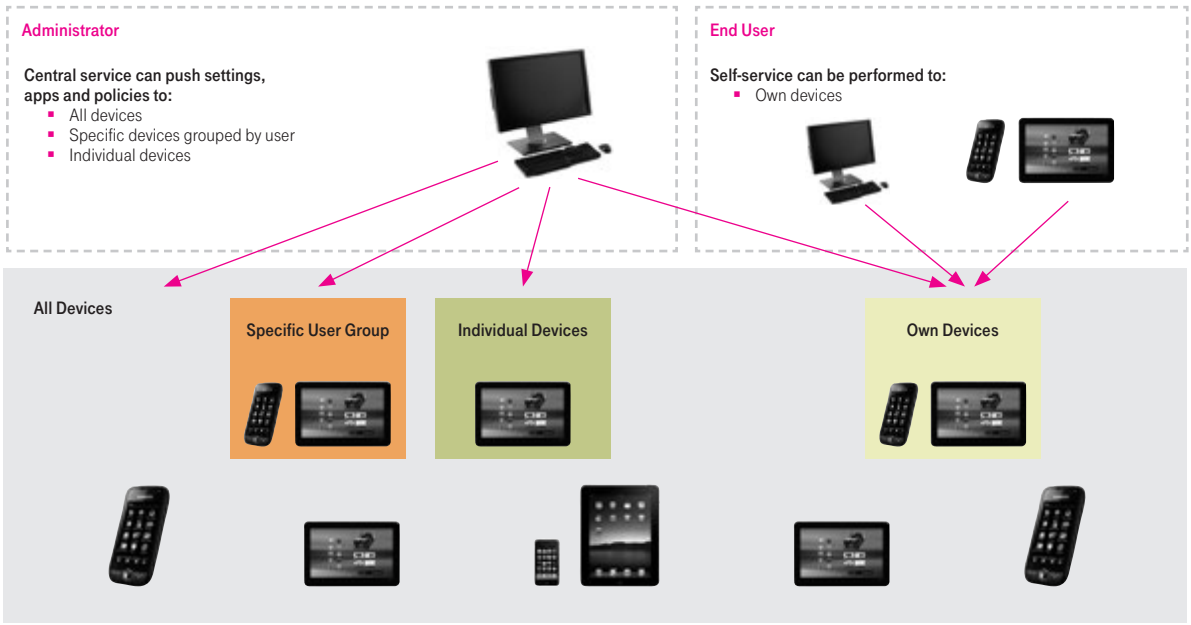


Chart 8

4. Security and native experience determine the MDM approach, while technology drives the MDM delivery model.

Realistically assess the security needs and take advantage of third parties' skills, while staying in control.

4.1 MDM core needs and suitable approaches.

Choosing the suitable MDM approach (Chart 9) for an enterprise depends on the specific challenges the company faces and the resulting key elements of the selected mobility strategy:

- **Scope of mobilization**, ranging from only mobilizing functions like email, calendar, tasks lists and personal address books (Personal Information Management – PIM), to fully mobilizing the business processes with access to company resources such as directories, CRM and ERP systems.
- **BYOD philosophy**, stating whether and to what extent the BYOD model is promoted by the enterprise.
- **Choice of operating systems**, resulting from the scope of mobilization and the BYOD philosophy, and setting the range of systems to be supported.
- **Security aspirations**, specifying whether internal traffic should be routed through a VPN or a Network Operation Center (NOC), if files and messages should be encrypted or if applications should be validated through certificates.

When choosing a suitable MDM approach, these considerations will lead to a careful evaluation of two main drivers: the demand for security on one hand and the need for native user experience on the other.

Companies faced with extreme security concerns might tend toward the dedicated, the dual user or the sandbox approach. With the dedicated approach, the company policy aims at allowing only business applications and data on the devices. Technical settings are configured accordingly, nevertheless preventing private data or applications have in practice encountered certain limitations. The employees are faced with a single, company selected "take it and you cannot leave it" user experience.

The dual user approach addresses the security concerns of the enterprise by completely separating the business domain from the private domain. Depending on the selected solution, it may give users the possibility to enjoy some native experience both in the business and the private domain, but it obliges them to act in two different worlds. For the sandbox approach, where the business domain is isolated in a container or sandbox, proprietary applications are mostly used in the business domain, which differ from the applications in the private domain.

All three approaches do not satisfy the increasing requirement of today's workforce for "native experience", i.e. for using widely accepted devices and applications in the consumer market also for the business domain. Therefore, companies choosing these approaches may forgo the benefits such trends imply: increased employee satisfaction and productivity.

Companies willing to accept a variety of devices and applications will opt for the encapsulated or mixed approach, in which the business domain and the private domain are jointly located and core applications are shared. The security level is determined by the functionality of the various operating systems, complemented to a certain extent by the MDM tools. Some manufacturers have migrated from the mixed to the encapsulated approach in order to enhance security. Protection levels provided by these shared approaches have been substantially increased through continuous development of operating systems, as well as increasing sophistication of MDM tools.

Accordingly, security conscious companies must continuously watch this progress and carefully reassess how such shared approaches from different MDM providers fit their actual security needs. By reacting flexibly to user needs and advances in MDM technology, farsighted CIOs have proactively embraced the new role they are expected to fulfill – that of an enabler and business innovator.

4.2 Defining the deployment strategy.

Enterprises considering introducing leading edge MDM systems should embrace a carefully planned and phased approach. Three steps are advisable on the way to full-fledged MDM implementation, which supports advanced mobilization:

- **Consult** – Analyze MDM best practice cases, dedicated White Papers as well as MDM system presentations and documentations.
- **Manage** – Gain governance over assets, services and associated processes as well as transparency of all elements of Total Cost of Ownership. This can be achieved by introducing TEM tools and using basic MDM features, thus gaining control over ordering and deployment processes, inventories and cost visibility.
- **Mobilize** – Develop comprehensive mobilization strategies defining the entire enterprise mobilization ecosystem along the key elements outlined. Implement advanced, feature-rich MDM systems with sophisticated application management and security management modules, which are based on flexible provisioning platforms.

Along this path enterprises should tap into the knowledge of analysts, operators and MDM providers, who are constantly at the leading edge of developments in this field.

4.3 Selecting an MDM delivery model.

A major decision faced by managers is to choose an MDM delivery model that is best suited to their company. MDM is a deeply technical universe. It needs specialized resources across a broad area of technologies, which is driven to a large extent by the various operating systems. Therefore, contrary to adjacent markets like TEM, enterprises have not developed their own MDM tools but have looked to third parties for MDM support.

Depending on the make-or-buy options in three key areas – people, tools and operation – three main models have been established in the market:

- **Licensed** Own experts, third party tools, own operations
- **SaaS** Own experts trained and advised by third party consultants, third party tools, third party operations
- **BPO** Third party experts, third party tools, third party operations

On the **generic level**, involving third parties in the key areas has several advantages, which include:

- **Better service** – MDM providers have specialized knowledge and can allocate sufficient resources with the required skills to design powerful, feature-rich solutions, which cannot be economically developed by a single customer.
- **Increased efficiency** – Permanent exposure to the processes of different customers and telecom operators as well as continuous improvement efforts position MDM providers much further down the learning curve. Therefore, they are able to drive extremely efficient processes and run highly reliable IT operations.
- **Speed of implementation** – Adding a new customer to an existing operation is easily achieved by the MDM provider, whether it is a shared system or a customer specific instance. Thus MDM can be introduced to individual units or entire organizations, taking into account the particular circumstances of the customer. This allows for a swift move to a higher level of MDM proficiency.

Mobility Strategy Choices Will Determine the MDM Approach.

Trade-offs between security and native experience are the main drivers.

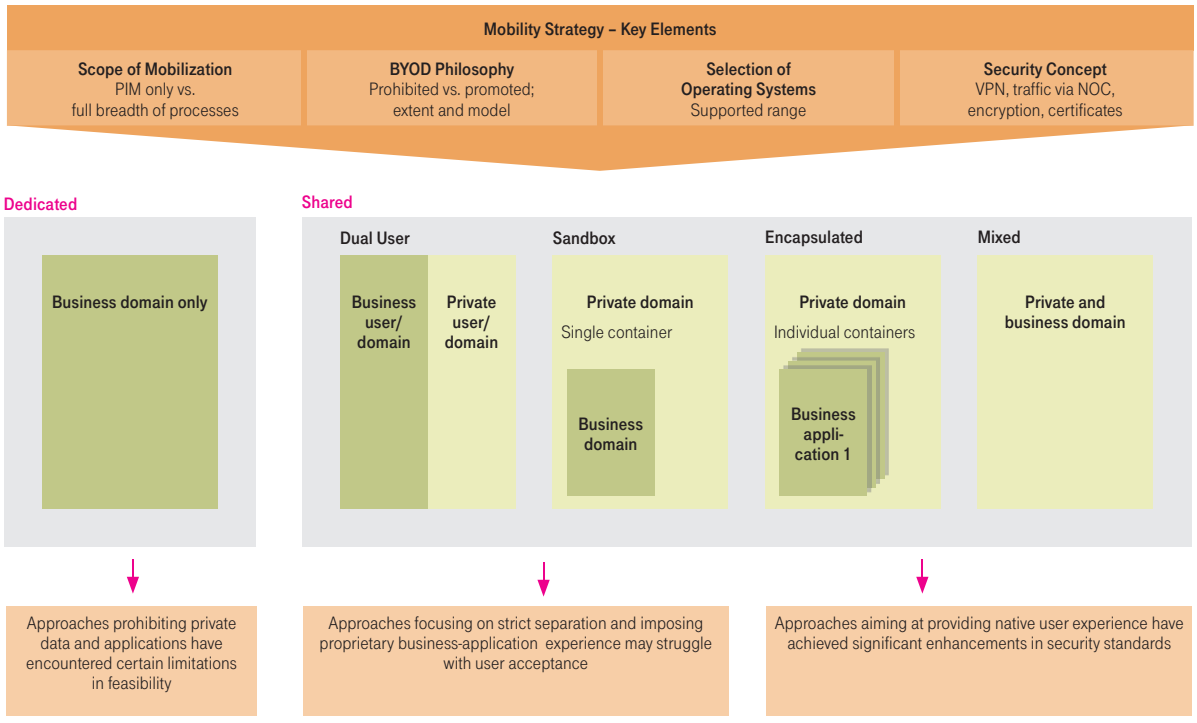


Chart 9

- **Focus** – The adoption of SaaS or BPO will free up resources allowing reallocation within the customer organization. Both situations will allow the company to concentrate on adding value by focusing on the core business. Adoption of BPO might mean that most of the MDM related resources would be transferred to the MDM provider; however, this will still contribute to an enhanced focus.

Nevertheless, there are some **cautions** that should be considered when involving third parties:

- **Dependency** – With an increasing degree of involvement by third parties, comprehensive and clear SLAs must be committed in order to ensure the same level of comfort as with the enterprise's own operations.
- **Remaining MDM activities** – Even when going as far as BPO, there are still MDM activities to be performed by the customer. These include provisioning relevant MDM data (e.g. invoices, information on organizational structure and cost centers), evaluating reports and recommendations, initiating actions and monitoring the performance of the MDM provider. Where special service levels for mission-critical activities may be required, some actions might need to be kept in-house. An example of this is when device replacement must be performed within a very short time, for instance an hour. Here, the first level support functions might need to stay with the customer.
- **Data protection and liability** – Since considerable insight can be gained from the data of each user and severe actions can be undertaken on individual devices, tailored data protection, liability agreements and review processes must be implemented when involving third parties for MDM. Various levels of sensitivity shown in different countries (for example USA vs. Germany) toward data privacy and security issues must be taken into account.
- **Personnel issues** – In order to reach acceptance and support for BPO, it is necessary to develop clear, convincing personnel concepts. These should take into account a possible reallocation within the customer organization and a potential transfer to the third party. They must be discussed and agreed upon at an early planning stage.

On the **company specific level**, choosing the appropriate operational model largely depends on the time pressure the company faces for mastering a competitive mobile enterprise environment. This requires the company to perform a thorough analysis, which MDM providers are willing to support with their expertise.

Nevertheless, a clear trend has been recognized: Reaching the best-in-class level within a reasonable time frame can best be achieved by adopting the SaaS or BPO operating models. To avoid the risks and barriers associated with a move to BPO, many companies decide on an SaaS model. This gives the opportunity to reach best-in-class MDM proficiency within the customer organization. It offers the advantages of involving a third party, while leaving the customer in control of telecom management processes.

SaaS also has the advantage of a "start small, grow big" approach. Prudent companies "start small" by launching MDM implementation first in one or a small number of units or countries, often with only a limited set of data and a core set of MDM elements. Once having achieved convincing results, they "grow big", deploying MDM across the entire footprint with a high level of data granularity and an extended set of MDM elements.

Even for companies considering a mid to long-term move to BPO, embarking initially on an SaaS model provides a much better basis for evaluating whether the move to BPO would be valuable and acceptable. Implementing MDM is always a journey, which needs to be carefully planned and undertaken with a reliable partner.

4.4 Cost versus benefit considerations.

Uncertainty about cost is one of the major reasons why companies hesitate to embark on an operating model with significant involvement of a third party, e.g. the SaaS or BPO models.

However, the main factor that must be considered is that MDM enables enterprise mobilization, which is a strategic step in the development of an enterprise, with all associated benefits of faster reaction to customer demands, streamlined internal processes and increased productivity. Nevertheless, weighing all these benefits – including BYOD cost considerations – against the costs of introducing MDM would provide a rather imbalanced perspective.

By narrowing the focus on costs and cost savings closely related to MDM, some MDM providers show savings estimations that need to be carefully interpreted in order to avoid confusing MDM savings with TEM savings. As devices used for mobilized business processes, like smartphones and tablets, show an increasing resemblance to PCs, useful analogies can be drawn from the experience of the PC industry.

Advanced MDM Systems Allow Substantial Cost Savings Beyond Mobilization Benefits.

Savings are driven by remote and user self-administration features as well as sophisticated interaction capabilities.

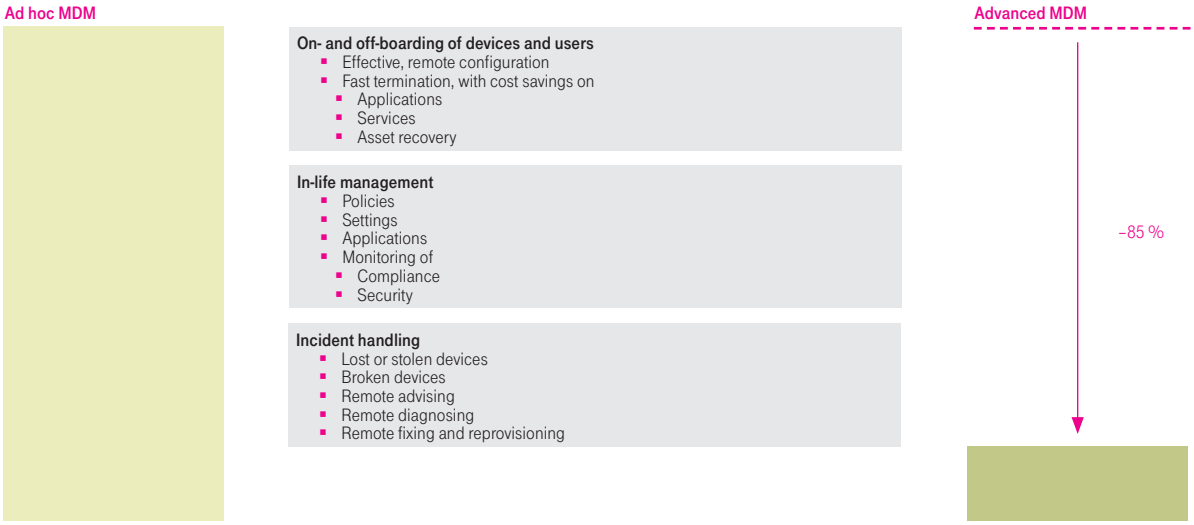


Chart 10

Sound savings estimations both in the mobile and PC markets compare the cost of ad hoc device management with the cost of advanced systems and evaluate the savings in several process-oriented categories (Chart 10):

- **On- and off-boarding** of devices and users through effective, remote configuration and fast termination with cost savings on applications, services and asset recovery.
- **In-life management** of policies, settings and applications, monitoring of compliance and security.
- **Incident handling** for lost, stolen or broken devices, remote advising, diagnosing, fixing and re-provisioning.

All savings categories are mainly driven by advanced features in the provisioning modules. These allow for remote administrator actions, user self-administration, as well as comprehensive and sophisticated interactions in each of the MDM modules dealing with configurations, applications and security. This helps reduce time, both on the user and expert side, in addition to a reduction in wasted assets. Estimations from MDM providers and PC experts point to saving potentials of up to 85%.

When considering a long-term partnership, competent MDM providers draw up a business case to set the cost baseline and evaluate the expected savings. These are then weighed against the expected MDM cost. Based on ROI considerations, proficient companies evaluate the whole context of mobility, of which MDM is a central part, capturing both benefits and TCO. The underlying business case involves detailed analysis as well as combined effort from both the MDM provider and the company.

5. Selecting the appropriate MDM provider requires foresight and knowledgeable analysis.

Focus on concrete delivery capabilities and benefit from provider advice.

5.1 MDM players.

Within the highly fragmented MDM market, three categories of MDM providers with various target customers, competencies, capabilities, track records and geographical reach can be identified:

- **MDM focused providers** – Due to the high complexity of MDM, particularly in the areas of data and mobile communication, numerous specialized providers emerged in the early market stages. They typically came from a dedicated service area, such as device management for fixed-line voice and data services, PC and notebook management or MDM for mobile services. Today, however, in order to meet customer expectations they need to cover a comprehensive range of telecommunication and IT devices, services and applications. Several MDM providers have diversified into other applications like TEM by capitalizing on their existing customer relationship. Thus, a highly fragmented landscape forms today's market.
- **System integrators** – Mostly as part of large outsourcing deals, system integrators have been driven to offer MDM services. While the scale of the deals has allowed them to develop their own MDM services, many system integrators increasingly offer "vendor agnostic" MDM services by integrating solutions from various MDM suppliers. They do this for two main reasons. The first is to draw on an extended and differentiated portfolio of specialized MDM services. The second is to comply with requests from customers who have built a track record with services from certain MDM focused providers, which they want to keep when going the extra mile toward the BPO model.
- **Telecom operators** – Increasingly, telecom operators have entered the MDM arena. This has developed from their role as a supplier of a wide range of devices as well as their natural position as a generator of data that is required for MDM, in regard to services and applications. In contrast, other MDM providers and system integrators rely on data they receive from customers or from telecom operators. Like system integrators, telecom operators can offer both self-designed MDM services and services that are incorporated from several MDM providers.

5.2 Outlook.

Before selecting an MDM provider, farsighted managers should take into account some main evolutions in the MDM market:

- **Increased customer focus on MDM** – With the ever-growing importance of telecommunications across business, especially for the mobilization of processes and applications on an international scale, MDM has become one of the top priorities of CIOs.
- **Sophistication of solutions** – The high priority of MDM is matched by high demands regarding the capabilities and impact of MDM. Customers expect a rich set of relevant features in horizontal as well as in vertical MDM solutions, targeted at specific industries.
- **Consolidation of the markets** – To fulfill customer requirements for advanced solutions and wide international presence, and in order to finance R&D and increase capacities, smaller players will find it necessary to merge. System integrators and telecom operators wanting to swiftly become significant players in the MDM market will aim at acquiring smaller companies with specific expertise. Additionally, larger and smaller players will tend to cooperate, allowing the former to offer a broader portfolio and opening sales channels to the latter that will leverage them internationally.

5.3 Selection criteria.

As already indicated, international enterprises increasingly consider implementing the SaaS and BPO models. These are companies with large fleets in numerous countries and various user clusters in terms of services, applications and usage patterns. Successfully pursuing these models depends on building a long-standing relationship with a skilled and reliable MDM partner. In identifying such a partner, the following capabilities need to be evaluated:

- **Targeted functionality** – Including full asset visibility such as the possibility to track their physical existence; the ability to easily configure mobile devices, smartphones and tablets with different operating systems; secure distribution of general and function-specific applications via enterprise application stores; prevention of malicious use of business applications; blacklisting and blocking of unwanted applications; secure data storage, access and transfer; creating a secure environment by fostering or enforcing security measures; providing protection through passwords and encryption algorithms; generating back-ups; taking appropriate emergency actions like blocking and selective or full wiping; user friendly, web-based interfaces servicing multiple operating systems; remote and over-the-air capabilities and suitable self-service options.

- **Safe design** – Based on established standards and secure platforms. It should be able to integrate different services in addition to MDM and link into the enterprise's accounting systems.
- **Comprehensive support** – Both in fast, result-oriented implementation and dedicated operational support with a single point of contact, backed by a team of experts who are available 24/7 and committed to specific SLAs.
- **Wide reach** – In terms of regional presence with the required skills and manpower, as well as having the international and local industry knowledge to deal with operators and suppliers.
- **Broad experience** – Capable of working closely with the MNC on translating business needs into mobility requirements; undertaking Proofs of Concepts and showing a proven track record in implementing numerous MDM solutions with various or specialized requirements as well as a stable, long-standing customer base.
- **Sound stability** – Relying on committed and trustworthy stakeholders on the owner, expert, and management side and drawing on profitable business and adequate financing.

The criteria mentioned above are useful for performing an educated screening of the numerous providers in the MDM market. A final selection process will need to analyze in detail an enterprise's future telecommunication needs and the required telecom management activities. These have to be compared to the individual capabilities of a selected set of MDM providers.

Key steps of the final selection process are:

- Formulate future telecommunication needs
- Set the MDM proficiency ambition level
- Select an MDM delivery model
- Establish a short-list of potential MDM providers
- Perform sound analysis to establish a reliable cost and service-level baseline
- Determine the MDM provider of choice

For in-depth advice that would allow joint development of a detailed MDM specification, please get in touch with your Deutsche Telekom, International Businesses Unit MNC Global Account Manager or contact us at: **www.multinationals.telekom.com**

We look forward to supporting you!

Imprint

Address:
Deutsche Telekom AG
Multinational Corporations
Landgrabenweg 151
53227 Bonn, Germany
Email: multinational.corporations@telekom.de

www.multinationals.telekom.com
Please use our contact forms for questions about the company or products and services provided by our business areas.

Pictures:
Deutsche Telekom AG

Life is for sharing.