Enterprise Mobility Management

With EMM, you are choosing a digital future and an unrestricted, secured mobility of the present.

What makes us different?

- European orientation
- Digital expertise
- Proven tradition

- Maximum security for devices, apps, content and personal details

- Innovative
- Simple
- Flexible
- Resilient

- Local support
- Sales partners throughout Europe

- Recognised quality assurance

- EU Data Protection Regulation
- European legal area

- Our EMM is based on a MDM solution developed in Europe, with focus on European standards.
- Various possibilities for system operation, e.g. Cloud or on-premise.
- Genuine multi-client capability, scalable from small to large.
- Standard MDM with possibility for individual enhancement through various EMM modules
- White-labelling of the server and/or client component possible.
- Individual connections can be implemented through numerous web services (API).
- Cloud solution is hosted in secured Tier 3 computer centres in Germany.

Supported Platforms

iOS ANDROID Android Enterprise

Windows 10 Samsung KnOX

Enterprise Mobility Management

EMM Ecosystem

Mobile Device Management

As the leading provider of enterprise mobility solutions, we offer you both individual solutions and all the necessary concepts and components to ensure smooth and straightforward mobile work processes. Our MDM is a key element here.
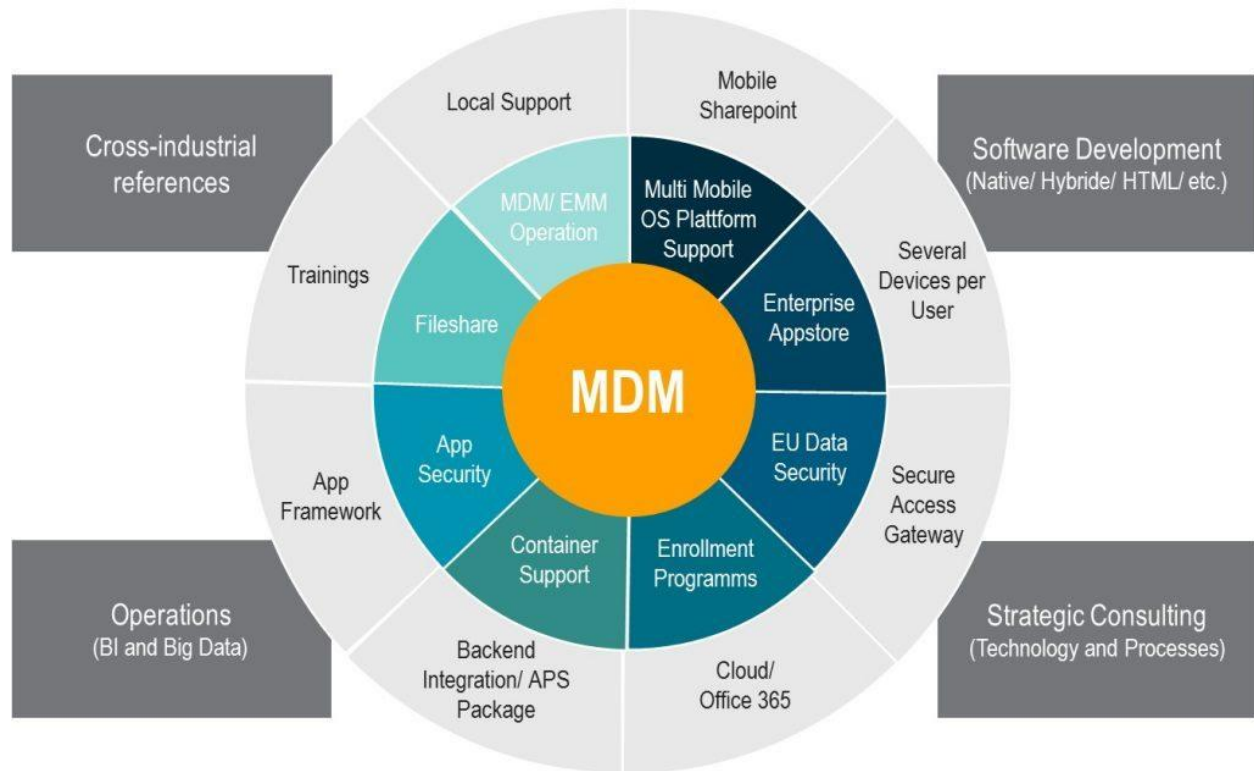
In general, the MDM comprises the following functional groups:

- Roll-out over the air
- Security settings
- Compliance guidelines
- Distribution of device settings
- Distribution of applications and files
- Inventory

MOBILE CONTENT MANAGEMENT

APP SECURITY

Enterprise Mobility Management

Although apps now must comply with security guidelines before they can be published in the various app stores, tests by independent IT security companies show that every second app forwards data to third parties. Do you have the time for the daily testing of the apps that your employees use at your company? We have MAS – European standard mobile app security. Our MAS provides you with access to an application database in which you will find security-relevant ratings of tested apps from diverse app stores. You therefore have a reliable basis when deciding as to whether you rate the app as secure or will place it on your blacklist as being unsafe.

ANDROID MOBILE SECURITY

The Android Mobile Security module provides state-of-the-art protection for Android devices from malware from apps and the Internet. Based on the app of our Austrian partner "IKARUS Security Software GmbH", the following functions can be centrally configured and rolled out using the management interface of our MDM System.

CONTAINER SUPPORT

What does an encrypted container do? It strictly separates your business data (e-mails & attachments, contacts and appointments) from the private sphere of your employees. In the private sphere, your employee can make unlimited use of the mobile terminal, manage their own data and save these (e.g. in a Cloud). You can use a password to protect your company information against unauthorized access and delete it (selectively) as needed. The secure container acts as part of your corporate network and falls under your Administration.

SECURE ACCESS GATEWAY

We offer an approach that limits the number of devices that can access the customer's exchange environment and in addition, makes access dependent on security-relevant device specifications. If a user wishes to access the Exchange Server using a mobile terminal, he or she must identify himself/herself to the firewall. This is done using a "Unique Identifier" (IMEI, serial number, ActiveSync ID, Apple ID). The firewall checks via our Secure Access Gateway, an MDM option, on the MDM server whether the identifier belongs to a terminal that is registered in the MDM. If this is the case, data access will be granted. If not, the device is rejected by the Firewall.

We implement your EMM strategy

- We offer EMM operating models both with Cloud, as well as on premise.
- Different service levels available.
- We create users and devices in your system.
- We work alongside you to define policies and restrictions and then implement them for you in your EMM system.
- You will receive regular reports on the status of your EMM solution and any policy breaches

Enterprise Mobility Management

- Motto: "You use our EMM system, we operate it!"

Savvy

MANY SKILLS. ALL-ROUND SKILLS. THE RIGHT SKILLS.

It is a fact that your business is mobile. Enterprise Mobility is key. Effective management of mobile devices and mobilized processes, as well as optimal integration is essential. Mobile Device Management (MDM) is the key. There are many features and functions. As a leader in enterprise mobility, we can promise you this: Our MDM is the perfect solution, for implementing a successful management of your mobile fleet.

Empathic insights

A PRODUCT IS ONLY GOOD IF IT MEETS YOUR REQUIREMENTS.

The difference between a good product and a better product is not the length of its list of features. After all, many companies know how to program. Rather, it is about complementing technical expertise with insights in and empathy for the users' situation and needs. This requires both an understanding of European business culture and the legal situation and requirements of those who work with the software.

A brick – or a whole building?

Our Enterprise Mobility

If you want to run a successful mobile business, you need to make a fundamental decision: Would you like to put together "only" individual components, or mobilize your entire workflow?

As the leading provider of enterprise mobility solutions, we offer you both individual solutions and all necessary concepts and components to ensure smooth and straightforward mobile work processes. Our MDM is the key element here.

The EMM Product Offered by Aspire Digital is a proprietary software of SEVEN PRINCIPLES Group, Germany.