Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 64 (2015) 274 – 281

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2015 October 7-9, 2015

Ensuring mobile device security and compliance at the workplace

Carsten Kleiner*, Georg Disterer

University of Applied Sciences and Arts, Ricklinger Stadtweg 120, 30459 Hannover, Germany

Abstract

End users urgently request using mobile devices at their workplace. They know these devices from their private life and appreciate functionality and usability, and want to benefit from these advantages at work as well. Limitations and restrictions would not be accepted by them. On the contrary, companies are obliged to employ substantial organizational and technical measures to ensure data security and compliance when allowing to use mobile devices at the workplace. So far, only individual arrangements have been presented addressing single issues in ensuring data security and compliance. However, companies need to follow a comprehensive set of measures addressing all relevant aspects of data security and compliance in order to play it safe. Thus, in this paper at first technical architectures for using mobile devices in enterprise IT are reviewed. Thereafter a set of compliance rules is presented and, as major contribution, technical measures are explained that enable a company to integrate mobile devices into enterprise IT while still complying with these rules comprehensively. Depending on the company context, one or more of the technical architectures have to be chosen impacting the specific technical measures for compliance as elaborated in this paper. Altogether this paper, for the first time, correlates technical architectures for using mobile devices at the workplace with technical measures to assure data security and compliance according to a comprehensive set of rules.

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge

Keywords: Mobile Device, Mobile Applications, Consumerization, Security, Compliance, Mobile Device Management

*Corresponding author. Tel.:+49-511-92961835; fax: +49-511-9296991835.
E-mail address: carsten.kleiner@hs-hannover.de

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge
doi:10.1016/j.procs.2015.08.490

1. Mobile devices at the workplace

Using mobile devices such as smartphones or tablets offers many advantages and has become very popular in private life. The devices get high acceptance, Forrester diagnosed an “explosion” of adoption for them[1]. IDC forecast a 73% growth of shipments from 2013 to 2017 with greater increase for tablets than for smartphones; in 2015 more tablets will be shipped than desktop plus portable PCs[2]. Reasons for this are the features of the devices and the comfort they provide. They are easy to carry and provide access to voice and data services, thereby opening up a wide variety of potential mobile applications, "anytime and anywhere." For many these devices have become an integral part of their private life. The devices offer an outstanding user experience that consists of convincing functionality and emotional reaction to appealing design and user interfaces; in addition, traditional priority of assessing functionality might change to adventuring “Look and Feel”[3].

For companies, Gartner has recognized a dramatic rise in the demand for mobile device applications until 2015, and considers the use of mobile devices in the workplace to be among the ten most important strategic trends[4]. These come along with slogans and phrases such as "… the rise of mobility and the marginalization of the PC“ and "move-and-do“ culture. Using mobile devices for work-related tasks will soon be at 350 million users[1,5]. "Consumerization" describes the diffusion of consumer market devices into business settings. This reverses traditional innovation paths, where new technologies are used at companies first and then users end up also employing them for private needs. With smartphones and tablets, private users are very familiar with the devices, and then bring them into work in the course of "user-driven innovation“[6,7]. According to Forrester, 50% of 18- to 31-year-old and 40% of 32- to 45-year-old workers believe technologies used in their private life are “better” than those in their professional life[8]. Consumers transfer requirements regarding user experience from private to professional life. Thus business requirements are not only driven by functional issues or rules for tax reduction anymore, but by fashion and individual preferences too.

At first glance, using mobile devices for work-related tasks is comparable to the use of notebooks, but using of smartphones and tablets is significantly more complex. These devices are connected with the internet through open channels and networks. Moreover, the devices currently available on the market are very heterogeneous, technical features and configurations are changing fast, and versions of operating systems have short life cycles. The operating systems popular at present – iOS, Windows, and Android – do not provide the reliability and stability known from traditional business systems. Security issues have lower priority for vendors when developing consumer devices than professional devices. Useful functionality for private applications may be inacceptable in business applications.

2. Security and compliance risks using mobile devices

Mobile devices are currently at the top of the list of most significant security risks, as demonstrated by a study involving security experts from companies from various sectors[5]. The fundamental values of confidentiality, integrity, and authenticity of business data are particularly threatened. Confidentiality is compromised when unauthorized parties obtain access to sensitive or confidential business information by manipulating devices or intercepting data transmission. Manipulation performed using insufficiently secured devices threatens the integrity of business data. Authenticity is threatened when devices are used to trigger business transactions that cannot be traced without ambiguity. Additionally, important compliance issues are at risk: information systems have to be documented and auditable, certain rules of data security and data retention have to be implemented. In particular, private data of end users must be strictly separated from business data. Mobile devices that are insufficiently secured lead to unauthorized use and modification of data due to deliberate or negligent actions. Also it must be feared that negligent or incautious behavior in private use will be transferred to business use.

Additionally, the level of complexity of the IT when using mobile devices causes additional security risks, sometimes phrased as "Complexity is the enemy of security”[9]. It can be expected that a broad spectrum of devices must be supported, with mobile devices being exchanged more frequently than usually with other devices. Technical and organizational measures have to be in place for cases of lost devices (due to misplacement or theft). Policies and procedures must ensure that the end user will give notice and that locally stored business data can be remotely wiped.

For mobile devices huge numbers of apps are freely available, often infected by malicious functions[10]. The

common use of open channels and networks threatens sensitive or confidential business information. End users often use public hotspots, which are not secured. Because mobile devices are often targeted by attacks, continuous updates of applications, operating systems and even firmware are necessary. Overall, using mobile devices like smartphones or tablets for real business purposes (beyond calling or web browsing) contradict some recent approaches of information management denoted with terms like standardization, consolidation, and reduction of complexity.

3. Concepts and technologies for integration of mobile devices

In order to facilitate the use of mobile devices for business purposes, there are various architectural concepts and corresponding technological solutions possible. These approaches differ in which parts of the applications are running on the mobile devices and on central servers, respectively.

In principle, all approaches are similar to architectures used in classical virtualization solutions. The objective is to isolate business applications from the rest of the mobile system. System environments must be encapsulated so that business data and applications are not exposed to risks. At the same time, it is necessary to retain the popular user interfaces and user experiences. Figure 1 outlines different approaches, represented as variations in the distribution of a business application between mobile device and central company servers. All approaches have been discussed in detail in[11].

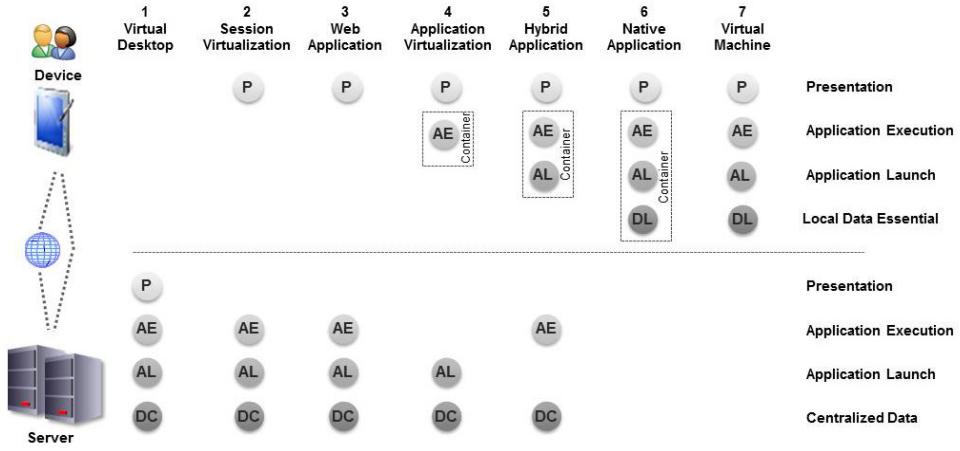

Figure 1: Approaches to Integrate Mobile Devices

Classic three-tier architecture is used for the principle structure of a business application, consisting of a presentation component, an application component, and a data component. An additional distinction between launching and executing applications is required; reasons for this will be explained in the following section. Note that approaches marked “DL” unavoidably require local storage of business data on the device, whereas the others may do so for optimization purposes but don’t have to. Thus, the corresponding aspects of local storage could also be relevant for these approaches.

When using a **virtual desktop** (1), mobile devices launch a virtual machine or a company application on a server in the company network. The user interface is generated on the server and displayed on the device only; user interaction is also processed on the server. Thus, this approach is a mobile variation of terminal servers known from traditional desktop systems. Due to the high bandwidth and low latency requirements this approach may become more interesting in the future with increased connectivity of devices.

Session Virtualization (2) also provides applications on a central server. Mobile devices launch the application, which causes the server to generate a new dedicated session for each device, which display user interfaces and process user input. Application provisioning like this is also suitable for streaming, as it has a somewhat lower

demand for bandwidth and, especially, latency than a virtual desktop. One advantage is that there is no effort for platform-specific procurement and operation of the applications. Applications are only displayed and not executed on the devices, there is no influence on the mobile systems and no data stored locally. Stable connections to the Internet are necessary for using these applications.

Web applications (3) represent a special kind of session virtualization, discussed here due to its great practical importance, especially for mobile devices[12,13]. Web servers are used for application provisioning, clients use a conventional web browser. The classification shown in Figure 1 is valid, if applications are used for display only, e.g. with classic HTML. When using applications featuring JavaScript or enhanced HTML5 functionality, part of the application logic is executed on the device, thus it must be classified as hybrid application (5). Using standard technologies on both servers and clients means only marginal effort for procurement and operation of applications. Since communication is performed via https, the use of a VPN can be avoided, but solid access controls are necessary to secure data integrity. Bandwidth requirements are comparatively low, therefore applications can be used via WiFi or GSM/UMTS as well.

With **application virtualization**[14] (4), executable applications are provided on central servers. When loading an application, the device downloads the corresponding executable file from the server and then runs it on the device - usually in an isolated area (a.k.a. sandbox or container). The risk of unauthorized access is low. Since devices download executable files, they are always working with the most recent version of the application. Using isolated areas ("container") on the devices lowers the risk of accessing application data by other software. With virtualized applications larger bandwidth is only necessary while loading the applications, after that only low bandwidth is required (if any) and subsequent offline operation is feasible.

Hybrid applications[15] (5) combine some advantages of web applications with those of native applications. Missing functions in web applications are supplemented in hybrid applications with components executed locally on the mobile devices. These components can be implemented with JavaScript or HTML or native programming languages of the devices. In contrast to a pure web application (3) it is possible to use device-specific functions like gesture control. Furthermore, it is somewhat easier to realize offline operation and provide the accustomed look-and-feel. But the technical requirements for the devices are significantly higher than with pure web applications. Furthermore, expenditure increases when trying to support various platforms, even if it is simplified by the use of frameworks like jQuery Mobile, Titanium Mobile, or PhoneGap. Running application components on the devices increase threat potential, because the execution of malware is possible; additional security measures should be implemented.

Native Applications (6) for application provisioning[12] are currently wide-spread in the consumer market. Platform specific versions of applications are produced for each mobile platform. Applications are then provided via the corresponding distribution channel (e.g. App Store, Play Store) and approved by its operator, then downloaded by users and installed locally on mobile devices. A significant advantage of native applications is that users receive applications with a look and feel that is typical for the platform. All specific control options can be accounted for. Additionally, utilization is possible in offline mode when all requisite data is stored locally. Even if offline operation is not being realized (e.g. because data is too big or not up-to-date) operation is possible with low bandwidth. However, the significant integration with the local systems of the devices cause serious problems to separate and isolate business data from private data. Though most current operating systems do offer isolated execution environments for apps, but these systems still allow e.g. critical ways to handle phone numbers. Thus, business and private data can hardly be separated. Remote deletion of data on the device (wipe out) in the event of loss is only possible with a brute-force method, namely restoring the device to the original delivery state. Another big disadvantage to native applications is that specific versions have to be implemented and provisioned for each platform. This requires extensive expertise in various development environments and programming languages. Overall, this dependency on the platform operators and distribution channels represents a significant investment risk.

Virtual Machines (7) expand the idea of application virtualization to platform virtualization[16]. An operating system with embedded application logic is stored on the devices as virtual machine during a dedicated installation process prior to execution. Later on, executions of the virtual machines occur in an area (sandbox or secure container) isolated and secured by the device. This procedure is a well-recognized and established process for desktop systems to secure the execution of third-party applications. Similar concepts are used by recent mobile device platforms such as Blackberry Balance or Samsung Knox specifically designed for business use. The most

important advantage of virtual machines is that applications can be run offline following prior installation. In contrast to application virtualization it is possible to provide various applications simultaneously. Furthermore, the same virtual machine can be used for all common operating systems. Execution in isolated areas on the devices secures the integrity for both business and private data. A complete deletion of company applications and data (wipe out) in the event of loss is easily possible by erasing the whole virtual machine file. The largest disadvantage of virtual machines is that currently there is no universal runtime environment available for various mobile platforms, preventing broad utilization. In light of the tremendous success of virtual machines on desktops, one can count on seeing an increase here in the next years.

In conclusion, the more parts of the applications are executed on the mobile devices (in Figure 1 from left to right)

- … the better the applications can be tailored to the platform's specific user interface.
- … the easier implementation is on server side, because less application logic has to be implemented there.
- … the easier application installation and maintenance becomes on the device, because the platforms' existing distribution channels can be used.
- … the easier is an implementation of offline-capable applications.
- … the more important and difficult it becomes to ensure data security on the devices, as there is high threat potential.
- … the more complex is implementing, installing and maintaining of applications, as several platforms have to be accounted for. For each platform, special development expertise is required, specific applications have to be implemented, and server-side software must be capable of handling different clients.

Pros and cons of the different approaches counterbalance each other and should be measured carefully. Development efforts will be significantly lower with the solutions Virtual Desktop, Session Virtualization, Web Application, and Virtual Machines (no. 1 through 3 and no. 7 in Figure 1), as a single implementation can be used for multiple platforms. Conversely, the necessities of a stable and permanent internet connection and the restricted options for tailoring to platform-specific user interfaces represent significant disadvantages. In any case, ensuring privacy of users' data on the devices against company access remains challenging.

4. Technological measures to support security and compliance

Most requirements for secure integration of mobile devices are directly specified in national laws (e.g. Bundesdatenschutzgesetz in Germany) or can be derived from standards such as ISO 27000 or COBiT. In the following section we assume that the enterprise IT satisfies all those requirements, i.e. only requirements necessitated by mobile devices are considered. Conceptually requirements have been presented in[11], so we focus on technological measures.

Currently, architectures according to no.5 or 6 in Figure 1 are very popular when using mobile devices, both in private as well as company settings. Companies usually complement these architectures by employing so-called "Mobile Device Management Software" (MDM software) which consists a client and a server component. Together these two components provide several of the technological measures required for company use of mobile devices. Details will be discussed in this section together with other measures that are not provided by MDM software.

4.1. Mobile devices

All measures can only be successful if the devices itself are not compromised, e.g. screen scraping or leaking information via clipboard is prevented. Antivirus software can account for that[10], but has to be maintained and kept active. This can be supported by MDM software. **Physical security** of the devices is difficult to achieve by technical measures, but has rather to be implemented by organizational measures to ensure user awareness. Additionally, user diligence and notification procedures in case of device loss have to be declared.

To achieve **access control** user authentication on the device has to be activated. It requires enforcement of sufficiently complex passphrases or unlock patterns or usage of biometrics, signature cards or token. The desired security level has to be balanced against the necessary effort to be achieved. Otherwise security measures might be undermined by e.g. writing down overly long passphrases. When devices have to be serviced or repaired additional tasks are necessary, e.g. previously resetting them to delivery status and recovering from a backup after completion of servicing. In addition, access control on application level is required to control access to programs and data and ensure that in case of surmounted admission control only non-critical interactions (e.g. phone calls or private zone access) on the device are possible. This can be achieved by separation of private and work zones either on system level (such as Blackberry Balance) or by using different virtual machines on the device. In enterprise applications access control has to be integrated into central access control systems (cf. 4.2) and should preferably use possession-based techniques.

Dissemination control is primarily achieved by data encryption on the device and during transmission. Communication with central enterprise systems is secured by end-to-end encrypted protocols or encrypting VPNs. Local data encryption is automatically used on some platforms, but sufficient secrecy of decryption information can mostly not be controlled. Thus, additionally an encryption of application and data on the device with company controlled keys is necessary. Encrypted containers for single applications as well as groups of applications (for common usage of data) are typically provided by MDM systems. Data must also not be copied illegitimate, e.g. by unwanted screenshots or clipboard access. Thus clipboards should be disabled in enterprise applications or (if that is not acceptable for usability reasons) data to be copied should be restricted or encrypted. Similarly, accidental or intentional data leakage by using popular cloud or messenger services has to be prevented. Such services should be irreversibly disabled for enterprise data or alternatively be impeded by using proprietary data formats which such services typically do not automatically operate on. For cases of theft or loss of a device a complete remote wipe of enterprise data from the device and a remote factory reset have to be possible. This functionality may be offered by device platforms and/or by MDM systems. For legal reasons private data on the device must be excluded from wiping.

Input control does not require any measures since devices are typically tied uniquely to a single person so that access to enterprise applications can be traced. For **order control** in addition to dissemination control access to enterprise data has to be restricted to legitimate applications. Most mobile platforms ensure that automatically by allowing data access only to applications that created data. MDM system containers can additionally be used to take care of common data access. **Availability control** is supported by backup runs that have to be executed and verified periodically. User-controlled backups need to be simple as well as encrypted, but must not be stored on insecure storage devices. Specifically automated backups stored on servers of the platform vendor are not acceptable. Since recovery processes tend to be complicated, availability control should be ensured by centrally controlled backups.

Compliance with the requirement for **separation of data** is similar to order control in that a clear separation of data access between (groups of) applications is implemented locally by configuration or supported by MDM systems. Measures employed for dissemination control also take care of separation of data.

Achieving certain requirements by MDM software has limitations and drawbacks as desired functionality may be limited by the features provided by the native operating system (e.g. a certain complexity of a device passphrase can only be guaranteed if supported by the operating system and made accessible to the MDM client). Proprietary operating systems are dependent on features offered by the vendor which incurs significant risks particularly for future versions of the OS - as influence on the vendor is very limited. In addition all features offered through the MDM client are not implemented on OS level but rather on application level, thus security problems on OS level can often not be discovered let alone prevented. Thus integrity of the device operating system is of utmost importance.

Table 1. Technical measures on mobile devices (MDM provided functionality).

	Physical Security	Access control	Dissemination control	Input control	Order control	Availability control	Separation of Data
Specific application	Primary						
Application authentication		Primary		Secondary			
Specific measures in		Primary	Primary		Secondary		Secondary

enterprise application							
Client-side encryption							Primary
Device authentication		Primary		Secondary			
Backup and Recovery		Secondary				Primary	
Anti-virus software	Secondary	Secondary	Secondary		Secondary		Secondary
VPN client			Primary				
Encrypted containers			Primary		Primary		Primary
Remote wipe receiver			Primary				
Private and work zone		Primary	Primary		Secondary		Primary

4.2. Central computing systems

To ensure **physical security** well-established measures such as multi-level security gateways and port restrictions are required to provide access for mobile devices to the company network (via VPNs). **Access control** is provided by secure authentication schemes on access points for mobile devices to the company network. This is usually implemented by VPNs which may use password-secured and certificate-based authentication, also taking care of data encryption during transmission. In addition, authentication on application level can be used if demanded.

Dissemination control requires additional technology in central systems. This includes e.g. definition of mobile applications for enterprise use (incl. anti-virus software and modified versions of standard mobile applications) to provision these from central systems. In addition, the definition of common security zones for groups of mobile applications is necessary as well as remote-wipe functions. Encrypted data transmission is also required. All of these requirements can usually be satisfied by server components of MDM software.

Input control for mobile devices requires logging of local activities, already provided by central computing systems. In addition, the assignment of mobile devices to user profiles needs to be managed in central systems. This is provided by MDM systems which should be capable to connect to existing identity management systems.

Order control demands central configuration of which data may be used by which mobile applications and in which mode (e.g. read, write, delete). In addition integrity and recency control of devices and their applications needs to be centrally initiated and managed. This is typically provided by platform vendors and/or MDM software.

Availability control needs centrally scheduled and initiated backups of local data and requires corresponding software. Backups should not impede standard usage of the devices, e.g. only be executed if sufficient bandwidth is available. Usually such software will also provide restore capabilities on new or repaired hardware. Usage of these tools will most likely require deeper IT knowledge. For cases of theft or loss a sufficient number of reserve devices has to be kept in stock to reduce downtimes. If devices contain only copies of central data backups of the devices are not required as the new or repaired devices can be provisioned by the MDM software with all required data and applications. Synchronization of data can be implemented in the (mobile) applications or automatically provided by using a capable underlying database system. **Separation of data** does not require any additional measures.

Table 2. Technical measures in central computing systems (MDM provided functionality).

	Physical Security	Access control	Dissemination control	Input control	Order control	Availability control	Separation of Data
Role-based access		Primary					
Device: Backup & Recovery Management						Primary	
Data synchronization						Primary	Primary
Security Information & Event Management	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary
Application authentication		Secondary					
Allocation & provision-ing of SW for devices			Primary			Secondary	

Configuration & provisioning security zones on devices			Primary		Secondary	Secondary	
Device management	Primary			Secondary			
Identity management		Primary		Secondary			
VPN server	Primary	Primary					
Remote wipe initiator			Primary				
Device integrity check	Secondary				Secondary		
Secure online storage			Secondary		Secondary		Primary

Well-established security procedures which are continuously reviewed should also be applied when integrating mobile devices into enterprise systems. Threats and risks definitely increase with mobile devices compared with centralized IT systems only[10]. In addition, the number and heterogeneity of platforms and devices increases significantly which in turn make attack detection more difficult. Thus the importance of "Security Information and Event Management" (SIEM) systems, which provide continuous monitoring and detection of even complex attacks increases. While those tools are available off-the-shelf in principle, a meaningful configuration and extension of these systems to be useful for the company will most likely require consulting expenses.

5. Conclusion

Mobile devices such as smartphones and tablets offer huge functionality coupled with high convenience; usage is well-known to most employees from their private domain. Consequently, such devices should also be used in enterprise information systems. However, significant technological as well as organizational measures are required to achieve acceptable levels of security and compliance. Based on the choice of technical architecture to integrate mobile devices into enterprise information systems this paper presents technical measures for a comprehensive set of security and compliance goals. For managing mobile devices, it seems necessary to use MDM systems to secure network access, manage heterogeneity of devices, provision software sets to the devices and keep devices and applications recent. Using MDM systems is only one building block for integrating mobile devices into enterprise systems securely. But also beyond MDM other technological as well as organizational measures are necessary as presented in this paper.

References

1 Schadler T, McCarthy JC. Mobile Is The New Face Of Engagement - CIOs Must Plan Now For New Systems. Forrester (Edt.); 2012.
2 IDC (Hrsg.). Tablet shipments forecast to top total PC shipments. www.idc.com/getdoc. jsp?containerId = prUS 24314413 2013
3 Bechinie M, Murtinger M, Tscheligi M. Strategisches Experience Management. Praxis der Wirtschaftsinformatik HMD 2013; 294: 87-96.
4 Gartner (Edt.). Hot Research Circle: Hot Topic Survey Results; 2012.
5 Deloitte (Edt.). Raising the Bar - TMT Global Security Study. 2011.
6 Györy A. Cleven A, Uebernickel F, Brenner W. Exploring the Shadows: IT Governance Approaches to User-Driven Innovation. Proc. of the 20th European Conference on Information Systems ECIS; 2012; p. 1-12.
7 Harris M, Patten K, Regan E, Fjermesat J. Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?, Proc. of the 18th Americas Conference on Information Systems AMCIS; 2012; p. 1-7.
8 Gray, B. Building A Bring-Your-Own-Device (BYOD) Program. Forrester Research (Hrsg.); 2012
9 Johnson K. Mobility/BYOD Security Survey. SANS Institute (Edt.); 2012.
10 Bundesamt für Sicherheit in der Informationstechnik BSI (Edt.). Sicheres mobiles Arbeiten - Problemstellung, Technische Voraussetzungen und Lösungswege anhand der Anforderungen für mobile Endgeräte in der Bundesverwaltung 2014.
11 Disterer G, Kleiner C. Mobile Endgeräte im Unternehmen. Wiesbaden: Springer Vieweg; 2014.
12 Charland A, Leroux B.. Mobile application development: web vs. native, Communications of the ACM 2011; 54: 49-53.
13 Anthes, G. HTML5 leads a web revolution. Communications of the ACM 2012; 55: 16-17.
14 Subar S. Mobile virtualization. www.visionmobile.com/blog/2010/06/mobile-virtualization-coming-to-a-smartphone-near-you; 2010.
15 Christ AM. Bridging the Mobile App Gap, Sigma Journal - Inside the Digital Ecosystem; 2011. p. 27-32.
16 Texiwell N. Get Your OS from VMware: Mobile Virtualization Platform. www.virtualizationpractice.com/get-your-os-from-vmware-mobile-virtualization-platform-11080; 2011.