Enterprise App Stores for Mobile Applications

Development of a Benefits Framework

Full Research Paper

Dr. Daniel Beimborn
University of Bamberg
daniel.beimborn@uni-bamberg.de

Maximilian Palitza
Camelot ITLab GmbH
mpal@camelot-itlab.com

ABSTRACT

Mobile devices and apps have changed the way consumers perceive and use IT. As mobile apps are easy to use and to procure, they have begun to enter the corporate world "under the radar" outside of the control of the IT unit. Employees bring their own mobile devices (BYOD) and apps to do their work – which raises various problems. As a counter-measure, firms have launched BYOD programs and set up Enterprise App Stores (EAS) where their employees can install certified and licensed apps under the firm's control. This paper aims to take a first step in scientifically exploring this new concept of EAS and exploratively develops a benefits framework which can serve as foundation for the conceptualization and empirical investigation of EAS value and adoption by future works.

Keywords

Enterprise App Stores (EAS), Software Distribution, Mobile Apps, BYOD, Benefits

INTRODUCTION

Since the 1980ies, the direction of how IT innovations diffuse into markets has changed. In earlier decades, main innovations happened in the military sector, diffused to industry, and then to consumers. Nowadays, the consumer markets are the main driving force behind IT innovations and consumers bring new innovations to their workplaces, driving the "consumerization of IT" (Moschella, Neal, Taylor and Opperman, 2004). Consumer technologies are often more powerful or user-friendly than enterprise technologies; consequently, employees bring their own devices (BYOD) and software with them to do their work. This trend leads to a decentralization of IT activities, to the creation of "Shadow IT" (Raden, 2005), and to severe problems regarding security, data protection, confidentiality, efficiency etc. (Harris, Ives and Junglas, 2011). For example, employees bring their own Android smartphones, install their own apps, and transfer sensitive customer data to their phone in order to do their work (e.g., manage customer data).

A promising solution for addressing the challenges involved with the consumerization of IT and BYOD, is seen in implementing an Enterprise App Store (EAS) (Gardner, 2011; Hinchcliffe, 2011). By an EAS, firms adopt the concept of public mobile app stores (MAS), such as Google Play or the Apple iOS Store, to the firm-internal environment in order to control the software which runs on their employees' devices. Thus, they can gain back the control over the applications used (and data processed) by their employees. As an example for a corporate-wide successful EAS, *Whirlwind*, which is the EAS of IBM, offers 400 third-party apps and 100 internally developed apps to IBM employees, providing similar features as commercial app stores, such as user rating and feedback, cataloging and search etc. By the end of 2011, Whirlwind had about 35,000 users (Hamblen, 2011).

Our paper contributes to the research of this young concept by developing a framework of potential benefits of EAS. This framework is exploratively developed based on the investigation of existing enterprise app stores and based on interviews with industry experts from this field. In later steps, this benefits framework can be used to inform empirical research on the business value of EAS and on the potentials and inhibitors of EAS adoption and diffusion.

FUNDAMENTALS

Basic Terms

App stores grant users access to apps. Wenzel et al. (2012) define *apps* as software applications that (typically) follow a “transactional” nature[1], are rather simple and low-priced and have single users. They are usually procured by individuals and implemented on an instant usage basis.

Since employees have started to bring their own mobile devices (smartphones, tablets etc.) to work and use it for firm activities, firms seek solutions for getting control about it. One solution, also used for corporate devices, is *Mobile Device Management* (MDM, (Finneran, 2011)). MDM supports centralized control of an entire fleet of smartphones and other mobile devices by applying and ensuring pre-defined configuration settings using an app on the smartphone. This app, the MDM agent, enforces adherence to these settings. Settings include e. g. password length and the deactivation of certain device functions or apps (Hemker, 2012, p. 166). However, MDM systems are not perfectly suitable for BYOD, as they give the IT unit comprehensive control over and insight into a device owned by the employee.

Another potential solution shifts the focus of mobility management from devices to apps and is called *Mobile Application Management (MAM)*. MAM focuses on managing the life cycle of an app from development, procurement, distribution, configuration, and update to the removal of an app (Winthrop, 2011).

In the following, a software system offering these MAM functions will be called Enterprise App Store (EAS). An EAS is defined as a platform for firm-internal distribution of mobile apps. Given the firm-internal nature of an EAS, its offering is limited to apps with a business purpose. The firm’s IT department defines the structures and processes for mobile software distribution and pre-selects those apps that are available in the store. In this way, software can be qualified regarding security and quality standards and according to the IT compliance guidelines defined by the firm.

The following table separates EAS from other concepts of transactional software distribution.

Characteristic		**Hardware**	
		Desktop	**Mobile**
Control	**Firm-external**	PaaS market places	Mobile App Stores (MAS) (e.g. Google Play, Apple iOS Store)
	Firm-internal	Software directories (as part of a client management system)	**Enterprise App Stores (EAS)**

Table 1: Means of distributing transactional software[2]

Without an EAS, firms do not have a mechanism to provide pre-qualified mobile apps to their employees which those can use in their work context. According to the table above, EAS can be categorized as merging the ideas of traditional firm-internal software directories and public MAS – providing the functionality of the first and the consumer-oriented user interface and functionality of the latter. Now, employees can use the EAS to choose and install apps that help them to do their work using their own mobile devices, but following the IT compliance guidelines of their firm (cf. Figure 1).

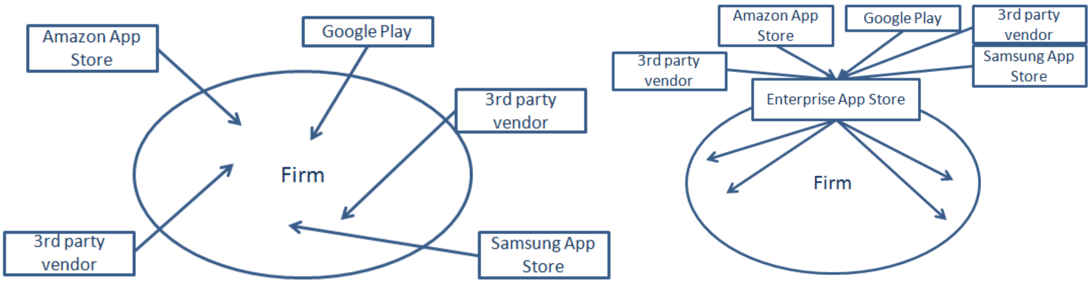

Figure 1. Corporate Scenario without (left) and with (right) Enterprise App Store

[1] Compared to “consultative” software which needs explanation and training before it can be used.
[2] For detailed explanations about these concepts and about their suitability to support BYOD, the reader is referred to the Appendix.

The left side of Figure 1 shows the uncontrolled procurement of apps from various sources by different employees in different parts of the firm, without the IT department having the chance to validate whether the apps follow the firm's compliance standards and security requirements. On the right side, an EAS serves as gate which needs to be passed by apps from external sources (while being tested, certified etc.) before they can be used in a firm-internal environment. We will refer to the first step of this process as "procurement" and to the second step as "distribution" of an app.

DEVELOPING A BENEFITS FRAMEWORK FOR ENTERPRISE APP STORES

Basically, there are three user groups involved with an EAS: (1) the employees/end users, (2) the firm providing the app store to its employees, (3) the app developers/providers[3]. These groups will exploit different benefits that motivate them to implement/use the EAS. Since their decisions are highly interdependent (e.g., if the users do not use the EAS offered by their firm, it will not make sense to implement it), we need to cover all roles and to gain a holistic understanding of this software ecosystem.

First, functionalities of EAS were examined by researching numerous vendors' offerings[4] in this field using all available public sources, e. g. company web sites, magazine articles, video demonstrations etc., to draw the concept of a generic EAS. We identified the following functionalities:

- A user interface resembling well-known MAS interfaces in terms of 'look&feel' and functionality (e. g. personal app portfolio, app directory and search functions, feedback tools) that is accessible using the browser of a desktop computer or mobile device
- Means of communication and social functions, like mailboxes, friend lists, profile pages, boards, blogs or wikis. Could be integrated from the corporate intranet
- Consolidation of app procurement
- License management for external apps. Must support all different licensing models of software that are available on the external market
- Security functions for corporate data that separate the employee's personal data from corporate data on her device by either securing individual apps, creating secured containers on the device, or running another, managed instance of the OS
- Installations of apps that can be triggered centrally (push-installation) or decentrally (pull-installation)
- Updating apps by replacing the old version of an app with the new one in all user portfolios
- Removing an app from single or all devices or from the EAS entirely
- An interface for managing content, users, metadata etc.

We derived the benefits of an EAS from these functionalities using literature on EAS wherever it was applicable[5], but also drawing on related concepts like client management systems, so as to find similarities and to examine whether their benefits were offered by EAS as well. The benefits identified this way were then enriched by conducting semi-structured interviews with involved employees both on the end-user side and on the administration side of an EAS in a global software firm:

- "admin": the previous and the current administrators of the firm's EAS
- "developer": two developers that distribute their apps via the EAS
- "user": two users that have provided feedback on apps in the EAS
- "manager": two managers who use the current EAS and are involved in the development of a new EAS

Together, these four groups provide an "all-round" perspective to systematically examine the potentials of EAS within a company. The interviews, except for the one with Manager2, were conducted over the phone and recorded. First, the interviewees were presented what an EAS is and how it differs from other means of software distribution (cf. Table 1) and what an EAS' main functionalities and their assumed beneficiaries are.

The interviews were analyzed using an open coding approach. Single benefit aspects which had been identified through research and – enhanced, detailed, and enforced by the interviews – were aggregated to the categories of the benefits categorization framework, which is given by the following table. It distinguishes between three major benefits dimensions: (1) IT compliance, (2) app life cycle management, and (3) reduction of BYOD Total Cost of Ownership. The "source type"

[3] Moreover, even the EAS itself can be run by a third-party provider as-a-Service for the firm.

[4] Among others, Nukona, OpenPeak, AppCentral, and PartnerPedia.

[5] As of June 2012, we were not able to find literature, neither in German nor English, that focused particularly on the benefits of EAS. We searched the databases of AIS, IEEE, ACM and SpringerLink for „Enterprise App Store" and variations of this term, e. g. "Internal" or "Corporate App Store".

column specifies the origin for each benefit. We differentiate between “Research” (our own findings from the EASs we examined and interviews we conducted) and “Literature” (sources that stated the benefit for EAS or comparable concepts).

				Primary beneficiary		
Category	Sub-category	Benefit item	Source type	User/ employee	Firm	App developer
IT compliance	Reduction of shadow IT (software, hardware, or both)	Usage of apps within firm borders becomes transparent and manageable.	Research		X	
		Internally developed apps can be easily migrated to “official” IT and distributed firm-wide	Research			X
		All private devices are revealed to the IT unit	Research	X	X	
	Data protection / data privacy	Protection of business data on private devices	Research, Literature[1]		X	
		Business data will not be stored on external servers	Research		X	
	Support of license management	Transparency of usage of licenses (cost reduction from consolidation and volume discounts, and easier license management)	Literature[2]		X	
		Avoidance of app vendor claims because of license misuse	Literature[3]		X	
App life cycle management	Develop-ment	Stronger user involvement via feedback on existing apps and idea management regarding new apps support app innovation	Literature[4]		X	X
		Acceleration of development due to usage of EAS security concepts and enhanced user communication	Research		X	X
	Procurement	Economies of scale in app procurement due to a centralized app procurement process	Research		X	X
	Distribution and version management	Easy and efficient distribution of pre-qualified apps	Research		X	
		Centralized and automatable version management by using push concept (only one version in the whole firm, no known bugs and security threats, no incompatibilities)	Literature[5]		X	
	Removal	Selective, flexible and controlled app removal	Research		X	
Reduction of TCO of BYOD program	Centra-lization	EAS is single point of management for all corporate-used mobile hard- and software	Literature[6]		X	
	Standar-dization	Reduced variety of apps reduces maintenance effort	Literature[6]	X	X	

Sources cited:
[1]: (Achten and Pohlmann, 2012; Walter and Dorschel, 2012) ; [2]: (McCarthy and Herger, 2011); [3]: (Gull and Wehrmann, 2009); [4]: (Goul, Marjanovic, Baxley and Vizecky, 2012); [5]: (Schmidt, 2010b); [6]: (David, Schuff and St. Louis, 2002)

Table 2: Dimensions of the EAS Benefits Framework

In the following, we explain the various benefit components and also highlight the necessary conditions that are required to reap the particular benefit.

IT Compliance Benefits

The goal of IT governance it to provide systems and procedures that prevent violations against internal or external rules and regulations (e.g., protection of customer data or intellectual property) (Schmidt, 2010a). An EAS helps contain the uncontrollable usage of private devices and uncontrollable procurement and usage of apps. Thus it does potentially contribute to the following aspects:

- Reduction of shadow IT
- Enabling and ensuring data security on private devices
- Support of app license management, including decentrally purchased apps

Reduction of Shadow IT

"Shadow IT" complements or even substitutes those systems which are centrally provided by the IT unit, usually by the business unit deploying their own systems (Jones, Behrens, Jamieson and Tansley, 2004). Sometimes, employees perceive a gap between their needs and the software and hardware supply delivered by their IT departments. One reason can be a little innovative IT department or an inflexible IT architecture that does not allow to meet the users' requirements in reasonable time (Berbner and Bechtold, 2010, p. 260f). Shadow IT can embrace both software and hardware, and it can be both self-developed or purchased (Rentrop and Zimmermann, 2012). Accordingly, in a mobile context, Shadow IT means employees working with their own mobile devices without their firm's agreement and using self-developed or privately purchased apps for doing their work.

If a firm has defined explicit BYOD regulations and offers certified apps via an EAS, the phenomenon is expected by all of our interviewees to widely disappear. EAS help automate the app distribution process for the user and make it easy to install the tools they need (compared to software directories or other "traditional" forms of software distribution). At the same time, they make app usage on personal devices visible to the IT unit and thus controllable, i.e., they reduce shadow IT. The advantage for employees is that they can proceed in using their mobile devices while knowing that the apps they use are accepted by the firm.

Shadow IT can also consist of internally developed apps which can get wide-spread distribution within the firm without IT unit's approval. Admin2 explained that in the company he works for the EAS substituted half a dozen different software distribution channels which served for the distribution of apps that where self-developed by different parts of the organization: "*We know what apps are out there. If they were in ten different places, tracking which apps have been published would be difficult*". A centralized distribution platform with wider reach to potential users (and corresponding feedback from a broader user base) made it attractive to the firm-internal developers, which then chose the centralized (and controlled) EAS for further distribution. Admin2 named this aspect to be the main benefit of EAS: "*For us, the main benefit was having one location where users can find all apps. […] This is helpful for our internal developers too, as they have one location to publish their apps*". Again, the necessary condition is that the usage of the EAS is not too restrictive. If developers have submitted a solution which then requires weeks or even months for approval, the hidden distribution channels will stay.

Shadow IT is not limited to software though, as the term 'Bring Your Own Device' states. EAS can help illuminate mobile Shadow IT by requiring employees to register any of their own devices they wish to use apps from the EAS on with the EAS in order to facilitate over-the-air app installation (s. below). This will shed light on the devices that were Shadow IT before, giving the IT unit an overview over devices the apps are run on.

Data Protection

Employees using their own devices for work automatically leads to mixing private and corporate data on this device. Since the device does not belong to the firm, the firm loses control over its data (Achten and Pohlmann, 2012). As noted above, one solution could be to include employee-owned devices into the firm's MDM, as it happens with corporate devices. Thus, the IT department would get comprehensive control over the device – but obviously, this will frequently collide with the interests of the actual owners (and has various legal problems, as well (Walter and Dorschel, 2012)[6]).

However, in certain cases firms need to have access to private devices – for example, they need to be able to erase everything remotely if the device has been lost. As consequence, it is suggested to clearly separate private and corporate data on the device (Walter and Dorschel, 2012). We identified three different technical approaches to this:

- Running corporate apps in a container or 'sandbox'
- Running them on a second instance of the OS ('profile')
- 'Wrapping' each app into security policies[7]~~.~~

Each of these three mechanisms fulfills the requirement of data separation and gives the IT department the ability to control the corporate apps and the data involved with them.

Another aspect of data protection is that data might be stored on enterprise-external servers. For instance, if employees use server-side collaboration infrastructures such as Dropbox to keep their work-related documents synchronized, the documents

[6] Particularly in countries with strong labor protection laws, work council rights, etc. such as in Germany.

[7] All those solutions bear also some potential disadvantages: containers and profiles may require a PIN every time the users want to enter the corporate "part" of their device which can be time-consuming. App wrapping requires the IT unit to define and maintain security policies for every single app, a process that is not scalable as such.

are stored on Dropbox servers and are thus out of the company's reach. Providing the employees with an app that offers a functionality they have been missing and that will keep internal data within the company will not only reduce Shadow IT but also eliminate a potential data leak. However, to learn about the employees' needs, the IT unit will need to implement appropriate communication and 'detection' mechanisms (s. 'Development' section below).

Support of License Management

License Management embraces all tasks involved with the usage of licensed software (Gull and Wehrmann, 2009). EAS enable the IT department to get an overview about used and available licenses for each app, for preventing the installation of apps which have no available licenses left, and for efficiently managing renewal cycles. Thus, the EAS increases transparency in the firm's license stock and helps preventing over-licensing (i.e., unnecessary cost) and under-licensing, which can lead to claims from the vendor because employees use apps without having a valid license (Gull and Wehrmann, 2009; Schmidt, 2010b). In other contexts, the monetary benefits of a centralized license management system have shown to be tremendous (McCarthy and Herger, 2011).

An obvious but important requirement is that the firm has employed a centralized license management system which is integrated with the EAS. Further, since the EAS, in contrast to an MDM system, cannot directly access the mobile devices in order to control which software is installed, they must enable the direct installation of the app on the device (without downloading the installation file on the device or on an intermediary desktop computer). If a user orders an app, the EAS assigns a free license to the user and registers the app to the user's portfolio. Then, the installation process can start. If, by contrast, the user had access to the installation file, she could install the app on several of her (or others') devices without the EAS and the license management system becoming aware of it (Jiang, Chen and Mukhopadhyay, 2008).

App life cycle management

As stated above, the life cycle of an app consists of development, procurement, distribution and version management, configuration, and removal (Winthrop, 2011). In this section, we take a closer look how an EAS contributes to each of these steps (except configuration which gains no particular benefits from EAS).

Development

An EAS supports firm-internal app development in three distinct ways, regardless of whether the developer is a professional from the firm's IT unit or a hobby developer. An EAS should offer the same social and communication functions as an MAS does, and like in an MAS users are welcomed to provide their feedback on apps they use. Developers use this user feedback to fix bugs in their apps, improving their quality (Goul et al., 2012), or even develop new apps. Admin2 mentioned the "*submit an app idea*" functionality the EAS in his firm offers. On a certain scale, this feature might even help improve IT/business alignment in this highly consumerization-ridden part of the firm's IT landscape, as it enables users to articulate their need for new mobile functionalities. Admin2 added that administrators provide the developers with usability and design guidelines over the EAS. Manager2 offered an example of how idea management can help preventing Shadow IT and data security issues. It came to the attention of the IT unit that employees have been using Dropbox for sharing and working on corporate documents, not knowing or disregarding the fact that data shared using Dropbox will be stored on Dropbox servers. The IT unit then provided a company-internal Dropbox clone that offers the same features, but will store the files on the company's servers.

EAS also accelerate app development in two ways. Their means of security separate personal and corporate data on the employee's device, providing a secure area (its size ranging between the area of the individual app up to a separate instance of the OS) for the app to run in. This releases the developer of considering security risks his app might encounter, and enables him to focus on improving his apps. Thus, the communication features of the EAS facilitate the knowledge diffusion from administrators to developers regarding any internal coding guidelines apps must adhere to.

Procurement

Since an EAS is the one place within the firm for distributing mobile apps, its use in supporting the procurement of external apps is obvious. An external app procurement process must not only check the app for its safety and acceptability for the EAS, but also gather as much of the firm-internal demand for a particular new app, in order to maximize economies of scale in purchasing this new app. Gathering the demand upfront will prevent or at least reduce a 'Me too' effect that might appear when a new app is available only for limited groups of employees (leaving aside apps for specific tasks or functions, like frontends to the CRM system), eliminating numerous re-orders of this app in smaller quantities.

Distribution and Version Management

MAS enable users to get the apps they want in an easy and efficient way. EAS offer pre-qualified apps fit for business use, enabling employees to easily equip themselves with apps that will help them be more productive, without requiring an extra approval process each time an employee wants to use an app. This eases overhead on the employees‘ managers and the IT unit, who will not have to run the same approval process numerous times. The users’ familiarity with MAS will cause little support effort from the IT unit’s side, as Admin1 noted.

As seen in Table 1, EASs can be seen as client management systems for mobile devices. These tools manage desktop computers remotely by checking e. g. for security breaches and adherence of system settings to corporate policies. Another important feature is their ability to install software automatically on some or all of the computers managed by the client management system, with the administrator having triggered this installation (Schmidt, 2010b). EAS offer the same functionality, ensuring app version consistency across all devices used for business purposes and thereby reducing security risks and maintenance efforts. When a new version of an app is uploaded to the EAS, the EAS checks all users’ app portfolios for this particular app and replaces it automatically (if the developer wants the update to be mandatory) or manually. Developer1 emphasized the importance of this functionality, saying “*For all OS it is important to have an update functionality […] Even without an app like the Apple Store [installed on the device] that checks for available updates on the device, there has to be a mechanism that does just that.*”

This ‘over the air’ installation (i.e., the device is not physically connected to e. g. a desktop computer during the installation) however must be supported by the mobile OS. Simply making the installation file[8] available for download is not sufficient as this would undermine the license management (cf. previous section).

Removal

There are many reasons why an app may need to be removed. Examples include an employee who joins another department, the procurement of a new app that is planned to gradually replace a different app, or a recently discovered data leak in an app. These examples also show the ways of removing an app, as supported by an EAS:

- Removing selectively from one or more devices: The IT unit is able to remove an app and its related data from the employee’s device without interfering with other business or personal apps or data. The license will be returned to the stock (if the license agreement allows this) and is available for use again.
- Removed from the EAS, but not from the devices (i.e., still managed by the IT unit): If an app is going to be, e. g., gradually replaced, it can be locked or hidden in the EAS, making it unavailable from there. It is, however, not removed from the devices, leaving IT capable of managing it, e. g. its security preferences.
- Removed from all devices and the EAS: In this case, an app needs to be removed entirely. It is then locked in the EAS storefront and wiped off of all devices it is installed on. This might be necessary in case a security issue is discovered in an app.

In all three cases described above, the EAS provides the IT unit with the flexibility to respond to each situation adequately.

TCO Reduction of a BYOD Program

The third category of EAS benefits links to the effect of EAS on the firm’s IT expenses. We use the Total Cost of Ownership (TCO) analysis, as it incorporates direct and indirect costs of an IT system. Direct cost include procurement and operative cost for hardware and software, e. g. installation, user training and systems maintenance. Indirect costs occur by productivity losses due to unfamiliar IT, down or malfunctioning IT and opportunity costs caused by not choosing a cheaper alternative.

In a BYOD program, employees use their personal devices for business purposes, quasi as a mobile workplace.

[8] e. g. *.apk files for Android and *.ipa files for iOS

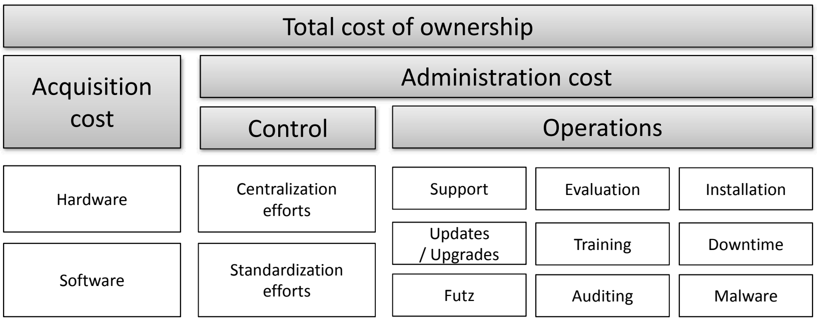

Figure 2: Total Cost of Ownership (David et al., 2002)

David et al. (2002) have proposed a concept for managing the TCO of a desktop computer workplace, and they identified acquisition and administration costs as the main groups of cost factors, with administration cost consisting of control and operations costs. They argue that centralization and standardization of the IT landscape are the two most effective ways to reduce TCO. Centralization means to consolidate software access and hardware management in one location, whereas standardization means reducing the differences in hardware and software of computers used in the firm. Although cost incur for implementing and maintaining means of centralization and standardization, these methods will, in total, lower the TCO by reducing the operations cost, e. g. by enabling remote troubleshooting, reducing downtime due to tested and approved hardware/software combinations, and a smaller knowledge base required for support tasks.

An EAS is the gate for apps from external and, in larger firms, internal sources. It has means of administrating apps, like uploading new versions, removing apps from devices or the EAS altogether, or rolling them out to groups of users. The EAS is also the place to manage corporate sandboxes, partitions and the like on employees‘ devices. As this is done from the EAS backend, the IT unit has all the functionalities required for managing the company’s app portfolio and the devices or sandboxes or OS instances, resp., used for business purposes in one place.

Hardware standardization is not the intention of a BYOD program and hence not in the functional scope of an EAS. Instead, EAS offer standardization of the mobile *software*. The vetting process where all apps need to go through to examine their acceptability for the EAS limits the number of apps that will enter the store to begin with. Afterwards, the MAS-like rating and review system will help to further standardize the portfolio of apps used within the company by promoting those apps with positive reviews. Support efforts will be reduced by e. g. providing app configuration files for every given environment, such as iOS and Android. Also, the limited number of apps available reduces the amount of knowledge that is required for efficient user support. The users benefit from standardization of the app portfolio by being presented not with a confusing number of similar apps for the same purpose, but with a limited selection of well-tested and well-accepted apps.

CONCLUSION

In this paper, we have presented a benefits framework for enterprise app stores (EAS). EAS provide centralized management of mobile apps in a firm-internal environment along with security functionalities to separate corporate and personal data on employee-owned devices. We identified numerous benefits, including:

- Support for IT compliance in enterprise mobility by reducing shadow IT, providing data privacy on personal devices and include apps into license management
- Effective and efficient app life cycle management, supporting app development, procurement, distribution and version management, and removal
- Reducing the TCO of the firm’s BYOD program by providing centralization of hardware and software management and standardization of the firm’s app portfolio

The future development of EAS will need to be tracked; we expect to see them being integrated into full-scale, cross-platform device management tools. Additionally, as their functional scope is currently mostly on native apps (apps that have been programmed for a mobile OS, like Android or iOS), it may shift with the technological and usage paradigms of mobile apps themselves (e. g. web-based apps replacing native apps).

Limitations of this paper

Although the theoretical benefits of EAS have been described and researched to the best of our knowledge and on the available literature on this or similar topics, the following limitations apply to this paper: First, the data and experience or knowledge base regarding app stores is limited, yet. Public sources do not offer detailed information about each vendor's EAS. Our interviewees all work in the same company which is using its own EAS that is limited in functionality compared to the set of EAS functionalities drafted in this paper. The second limitation is the lack of empirical, scientifically sound evidence available on EAS, so the benefits outlined above are yet to be proven in reality.

Outlook: Future Research on Enterprise App Stores

So far, the benefits of EAS have been identified. In this paper, however, the potential disadvantages that come with an EAS have not been mentioned, which is another important area of research on EAS. For example, the presence of an EAS might involuntarily cause, contrary to what we argued above, app variation instead of standardization. The ease of procurement, also on a larger scale, might spark uncoordinated app purchasing, leading to exactly the opposite of what was intended to be achieved.

Another direction of EAS research will be to develop an adoption model that helps to understand the attitudes and behaviors of both firms and users and that will guide empirical research of the EAS phenomenon. The challenge will be to integrate the different adoption models for users, developers, and the firm that actually implements and runs the EAS. As already argued above, the benefits (and other decision determinants) of these three entities are highly interdependent. The adoption decision of one entity is a decision determinant of the others. Moreover, from the firm's perspective it is not only about adopting an EAS, but also on how to optimally design it (or: 'which features to adopt'). Doing a simultaneous empirical investigation of EAS adoption both at the firm level and at the user level will help to deeply understand the dynamics and inhibitors for successful EAS implementation and roll-out. These results will be highly valuable for firms that look for BYOD and EAS strategies, but also for the 'market' which includes independent vendors that develop business apps and will be interested to place their offerings in EAS of larger firms and even EAS providers that run the whole enterprise app store for a company and thus become another intermediary link of the increasingly complex value chain for providing users with the software they need – and want – to do their work.

REFERENCES

1. Achten, O. M., and Pohlmann, N. (2012) Sichere Apps (Secure Apps), *Datenschutz und Datensicherheit*, 36, 3, 161–164.
2. Beimborn, D., Miletzki, T., and Wenzel, S. (2011) Platform-as-a-Service, *Business & Information Systems Engineering*, 3, 6, 381-384.
3. Berbner, R., and Bechtold, J. (2010) Innovationsmanagement als elementarer Bestandteil des IT-Managements (Innovation Management as Elementary Part of IT Management), in Frank Keuper, Marc Schomann and Klaus Zimmermann (Eds.) *Innovatives IT-Management (Innovative IT Management)*, Gabler, Wiesbaden, 257–274.
4. Buxmann, P., Hess, T., and Lehmann, S. (2008) Software as a Service, *Wirtschaftsinformatik*, 50, 6, 500–503.
5. David, J. S., Schuff, D., and St. Louis, R. (2002) Managing your total IT cost of ownership, *Communications of the ACM*, 45, 1, 101–106.
6. Finneran, M. (2011) BYOD Requires Mobile Device Management, InformationWeek, http://www.informationweek.com/mobility/business/byod-requires-mobile-device-management/229402912, as of 22 Feb 2013.
7. Gardner, D. (2011) App stores - They're not just for consumers any more, as more enterprises adopt the model to support mobile work, http://www.zdnet.com/blog/gardner/app-stores-theyre-not-just-for-consumers-any-more-as-more-enterprises-adopt-the-model-to-support-mobile-work/4366, as of 28 Jun 2012.
8. Goul, M., Marjanovic, O., Baxley, S., and Vizecky, K. (2012) Managing the Enterprise Business Intelligence App Store: Sentiment Analysis Supported Requirements Engineering, in *45th Hawaii International Conference on System Sciences*, Maui, 4168–4177.
9. Gull, D., and Wehrmann, A. (2009) Optimized Software Licensing – Combining License Types in a License Portfolio, *Business & Information Systems Engineering*, 1, 4, 277-288.
10. Hamblen, M. (2011) IBM opens up smartphone, tablet support for its workers, ComputerWorld, http://www.computerworld.com/s/article/9221289/IBM_opens_up_smartphone_tablet_support_for_its_workers?taxonomyId=75&pageNumber=1, as of 04 Jun 2012.
11. Harris, J. G., Ives, B., and Junglas, I. (2011) The Genie Is Out of the Bottle: Managing the Infiltration of Consumer IT Into the Workforce, Accenture.

12. Hemker, T. (2012) „Ich brauche das!“ — Mobile Geräte im Unternehmenseinsatz (I need that! - Mobile Devices in an Corporate Context), *Datenschutz und Datensicherheit*, 36, 3, 165–168.
13. Hinchcliffe, D. (2011) Enterprise app stores arrive; IT departments nonplussed, http://www.zdnet.com/blog/hinchcliffe/enterprise-app-stores-arrive-it-departments-nonplussed/1549?tag=search-results-rivers;item15, as of 28 Jun 2012.
14. Jiang, B., Chen, P.-Y., and Mukhopadhyay, T. (2008) Software Licensing: Pay-Per-Use versus Perpetual, *SSRN Electronic Journal*.
15. Jones, D., Behrens, S., Jamieson, K., and Tansley, E. (2004) The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation, in *ACIS 2004 Proceedings*.
16. Keizer, G. (2011) Google pulls 22 more malicious Android apps from Market, ComputerWorld, http://www.computerworld.com/s/article/9222595/Google_pulls_22_more_malicious_Android_apps_from_Market, as of 21 Mar 2012.
17. McCarthy, M. A., and Herger, L. M. (2011) Managing Software Assets in a Global Enterprise, in *2011 IEEE International Conference on Services Computing*, Washington DC, 560–567.
18. Moschella, D., Neal, D., Taylor, J., and Opperman, P. (2004) The ‘Consumerization’ of Information Technology, http://lef.csc.com/assets/192/download, as of 04 Jun 2012.
19. Raden, N. (2005) Shadow IT: A Lesson for BI, http://www.information-management.com/bissues/20051001/2600021-1.html, as of 12 Feb 2013.
20. Rentrop, C., and Zimmermann, S. (2012) Shadow IT - Management and Control of unofficial IT, in *The Sixth International Conference on Digital Society (ICDS)*, Valencia, Spain, 98–102.
21. Schmidt, W. (2010a) IT-Governance, in Jürgen Hofmann and Werner Schmidt (Eds.) *Masterkurs IT-Management*, Vieweg+Teubner, Wiesbaden, 355–403.
22. Schmidt, W. (2010b) Management von Anwendungssystemen, in Jürgen Hofmann and Werner Schmidt (Eds.) *Masterkurs IT-Management*, Vieweg+Teubner, Wiesbaden, 225–286.
23. Thurm, S., and Kane, Y. I. (2010) Your Apps Are Watching You, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html, as of 04 Nov 2012.
24. Walter, T., and Dorschel, J. (2012) Mobile Device Management - Rechtliche Fragen (Mobile Device Management - Legal Questions), *Wirtschaftsinformatik & Management*, 4, 3, 22–26.
25. Wenzel, S., Faisst, W., Burkard, C., and Buxmann, P. (2012) New Sales and Buying Models in the Internet: App Store Model for Enterprise Application Software, in *Multikonferenz Wirtschaftsinformatik* Braunschweig, Germany.
26. Winthrop, P. (2011) Mobile Application Management vs. Mobile Device Management, http://theemf.org/2011/05/18/mobile-application-management-vs-mobile-device-management/, as of 29 Mar 2012.

APPENDIX

Different Forms of Transactional Software Distribution

	Description	**Usability in a mobile BYOD context**
PaaS, APaaS	On-demand software, or Software as a Service (SaaS), is provided over the internet. The vendor is hosting and maintaining the software, while the user accesses it via browser (Buxmann, Hess and Lehmann, 2008). App Stores for SaaS business software are part of an on-demand development platform (Platform as a Service, PaaS). A platform based on a core application is called APaaS (Application-based platform as a service).Software developed on an APaaS enables the customer to tailor the system to its needs. (Beimborn, Miletzki and Wenzel, 2011)	Because on-demand software is used in the web browser, (Buxmann et al., 2008), it could be used in a mobile device browser, however, the small screens of mobile devices limit its usability.
Software Directories	Software directories are the part of client management systems that is visible to the user. They offer him or her software that have been preselected by the IT unit and can be selected for installation (Schmidt, 2010b).	Currently, software directories support only desktop software. The pre-selection and approval by the IT unit guarantee high reliability and security of the software. According to Table 1, EAS can be seen as software directories or client management systems for mobile devices.
Mobile App stores (MAS)	Mobile App Stores (MAS) are widely known from the consumer world, with the Google Play Store for Google's mobile OS Android as a well-known example. Google Play is accessible via desktop computers and mobile devices and allows the user to browse apps and to add them to their app portfolio, installing them automatically on a device they registered for their account.	MAS' target audience are personal users. In Google Play there does not seem to be a lot of quality control, as cases of apps that were removed due to their malicious content (Keizer, 2011) show. Also, apps from MAS might be reading personal data from the device and sending them to unknown recipients (Thurm and Kane, 2010). Thus, apps from MAS should not be allowed to mingle with corporate data.

Table 3: Alternative forms of transactional software distribution