Internet of Things and Cloud Computing
2014; 2(4): 26-31
Published online October 30, 2014 (http://www.sciencepublishinggroup.com/j/iotcc)
doi: 10.11648/j.iotcc.20140204.12

Telecom Namibia enterprise mobile architecture (TNEMA): Bring your own devices

Valerie Garises[1], Jameson Mbale[2, *]

[1]IT Factory, Telecom Namibia, Windhoek, Namibia
[2]Copperbelt University, Department of Computer Science, Kitwe, Zambia

Email address:
garisesv@gmail.com (V. Garises), mbalej@yahoo.com (J. Mbale)

To cite this article:
Valerie Garises, Jameson Mbale. Telecom Namibia Enterprise Mobile Architecture (TNEMA): Bring Your Own Devices. *Internet of Things and Cloud Computing.* Vol. 2, No. 4, 2014, pp. 26-31. doi: 10.11648/j.iotcc.20140204.12

Abstract: In this era, commercialization of IT and enterprise mobility has been envisaged where corporate employees utilized mobile devices such as laptops, smartphones and tablets, to work at anytime, anywhere and from any-device for personal and business purposes. In this way corporates improved productivity, employee retention, flexible work environment, IT value-added to business and reduced running costs. Nevertheless, it also culminated into critical risks to company's systems since employees had uncontrolled access to the infrastructure as such vulnerable to security and data abuse. It was in view of that this work envisaged on the Telecom Namibia Enterprise Mobile Architecture (TNEMA), a system developed to enhance security measures, manage and control the use of bring your own device (BYOD) against the company's infrastructure. The TNEMA architecture composed of five integrated functional components that included: User Interaction, User Mobile Devices, Access Networks, Enterprise Mobility Infrastructure and Enterprise Backend System. The TNEMA architecture security consists of firewalls installed and configured between the components to filter out the malicious and non-corporate operational data. Also, enhanced in the TNEMA are the layers of encryption, authentication and authorization, boundary protection, possible hardening of devices, and mobile device provisioning and management, all contribute to overall security. In addition, TNEMA adequately protects sensitive data using Internet Protocol Security (IPsec) and Virtual Private Network (VPN) that established a secured path between the mobile devices and the Enterprise Mobility Infrastructure and Public Key Infrastructure (PKI) to provide greater control over issuing, renewing, revoking, and managing Secure Sockets Layer (SSL) certificates while still gaining the advantages of using a trusted Certificate Authority (CA).

Keywords: Bring Your -Own Device (BYOD), Enterprise Mobility (EM) ,TNEMA, Mobile Device Management (MDM), Integrated Architecture

1. Introduction

With the consumerisation of Information Technology (IT) enterprise, employees are increasingly on the move. They rely on the ability to work anytime, from anywhere and have access to corporate information without apprehensions for potential compliance, security and cost implications. According to [1], proliferation of mobile devices and applications has led to a new paradigm in the way people work, communicate, collaborate and conduct business. In view of [1], this wave presented businesses of all shapes and sizes with challenges as well as opportunities. This trend is also experienced in Telecom Namibia's customers, employees, and partner engagement. It compels the enterprise adoption of Mobile Information and Communication Technologies (M-ICT) such as laptops, tablets, smart phones and other handheld devices in Telecom Namibia (TN).

Furthermore, [2] stated that the integration of M-ICT to access enterprise information was often called as Enterprise Mobility (EM). The author added that EM enables mobile enterprise users access to information anytime from anywhere through the use of M-ICT. On the other hand, the author said that mobile enterprise was a general term for the companies which decided to use wireless mobile device in order to support critical business functions and provide access to business applications to employees. He stated that in a mobile enterprise employees used mobile devices for work purposes such as checking email, project status, documents, meeting schedule, accounting and to-do lists, etc. These examples are the most common uses with working purpose that an employee might use any or all of them but there were many other mobile applications that a company might have

developed and let their employee work with. Similarly, TN can benefit from embracing EM through employee enablement to access business applications from anywhere, at any time and from any device.

This work centers on development of TNEMA for TN and in particular the technological aspects related to the enterprise applications integration architecture of M-ICT.

2. Background

In the past TN supported and even encouraged employees to work remotely by issuing corporate laptops and mobile phones for corporate email, voice calls and enabling intranet, email and business applications access via VPN. Today, the demand for mobile and wireless technologies in TN is pervasive thus many employees are now using consumer devices such as smartphones, tablets and laptops to support business productivity—a trend called consumerisation. TN employees are acting as a catalyst for change by using their personal devices and third-party applications for work purposes, leading to what has been labelled by experts as the "consumerisation of IT".

Historically, TN provided multiple mobile devices to employees as staff benefit but due to the high management costs the company resolute to provide an ICT allowance instead of company funded equipment. Henceforth, the employees can choose the package that suit within their ICT allowances and buy any type of device(s) according to their preference. This phenomenon is often referred to as Bring or Buy Your Own Device (BYOD).

The BYOD programme in TN focuses on reducing costs without proper fore thought of how to manage network resources, devices, employees and how IT Department should integrate these new devices in terms of support like access and security. Furthermore, the BYOD poses challenges as well as the opportunities that were not taken into consideration. This business problem resulted by BYOD phenomenon is presented in the next Section.

3. Statement of the Problem

Since the introduction of BYOD, TN employees own multiple mobile devices such as: laptop computers, smart phones, tablets and demand for mobility on their devices. TN employees bring their privately owned devices to work, access various mobile applications for personal and corporate use. Subsequently, the consumerisation of IT extends the reach of the company's wired and wireless information infrastructure. Therefore, the personal devices operate outside of the company IT architecture by doing so the company information also becomes more vulnerable to security breaches outside the perimeter.

[3] reported that the top concerns for BYOD were related to security in particular device, data breach, mobile data and application security. In view of the above, employee mobility increases risks of unauthorised exposure to sensitive and critical corporate data. It also creates many challenges for TN's IT Division forcing them to rethink traditional methods of providing computing services, ensuring information security and controlling the use of enterprise technologies. Furthermore, the degree and extent of risks to company was not known and could pose serious threats to corporate data on the mobile devices within TN. This situation has created dilemma for TN IT management who needed to maintain corporate data security, while enabling more devices and functionality. Consequently, they were under pressure to find the right balance between end-user demands, mobile platform diversity and security requirements.

In response to some of the abovementioned requirements the IT division opted for a Mobile Device Management (MDM) solution to secure, manage and control the BYOD devices and mainly to protect the corporate data on the mobile devices. According to [4], MDM solutions bring features like data encryption, remote data wipe to iOS and Android smartphones thus focuses only at device level. The author further stated that Mobile Application Management (MAM) arose as a popular alternative with features that allowed IT to manage selected business applications deployed to mobile devices by providing deployment tools, application-level encryption, and single-sign-on. In view of [5], both MDM and MAM solutions focuses only management devices and applications and does not address integration of M-ICT into business. Hence, the need for EM which comprised of technology solutions that could manage the increasing array of mobile devices, applications, data, secure access to enterprise infrastructure. Given this situation, the researcher has been motivated to carry out this research.

4. Literature Review

[6] Defined mobility as the application of mobile and wireless technology to enable communication, information access, and business transactions from any device, from anyone, from anywhere, at any time. In the same way, this study provides enterprise application integration architecture for TN that enables employees to access corporate resources using company provided and privately owned devices irrespective of their physical at any time. Furthermore, [1] described that EM was built on a foundation of processes and technologies allowing full access and instrumented insight to all organisational resources. The author added that the results improved adaptability, access, and interaction amongst employees, customers, partners, and suppliers, independent of their location. In addition the author stated that the mobile enterprise was an emerging organisational form that resulted in a paradigm shift of how business was done.

[7] stated that the mobile industry was changing at a rapid pace and so was the behavior of employees which used mobile technologies. They further said that one has to look at the technology trends by market, the competitive landscape, and the mobile worker adoption trends. In addition, [5] reported that 28 % of their workforce was currently using personal devices for work-related tasks, and this percentage was expected to rise to 35 % by mid-2013. Similarly, TN observed

that employees today were increasingly tech-savvy and self-empowered. They typical owned an assortment of laptops, smartphones, tablets and PCs that were often more advanced than what the company could offer. Hence, this trend forced TN to embrace "bring your own device" or BYOD trend to improve productivity, employee retention, enhanced mobility, a more flexible work environment and improved IT value to the business.

According to [8], the number of mobile devices now outpaced humans on this planet, it was estimated that there were 7.3 billion devices in the world in 2012 compared with just fewer than 7 billion people. In support, [9] noted that a major shift to mobility had been the main technological focus of IT development, was a new network structure, a facilitator of business activity and that more than 5 billion mobile service subscriptions supported approximately 80% of the world's population that communicated on the go. In the case of Namibia, [6] announced that they had reached 2,042 million active subscribers in 2012 which accounts for 10% increase to the previous financial year. In view of [10], the recorded population of 2,324 million people in Namibia demonstrated that the growth of mobile subscribers versus population was also observable in the Namibian mobile consumer market. Looking at these statistics unleashed a multitude of potential opportunities to communicate and collaborate with customers, employees, and partners in TN.

[11] stated that mobile communications could enable organisations to take advantage of a number of benefits including connectivity, flexibility and interactivity. They said that these benefits contributed to increased efficiency and effectiveness of fundamental activities in an organisation and helped to transform business processes. In the same manner, TN enhanced the ways employees communicate and collaborated. For instance, greater access to their email and calendars along with voice, video and messaging applications such as Microsoft Lync facilitates employee-to-employee (E2E) communication in TN. Furthermore, TN grants remote access to content such as dashboard reports and enterprise applications such CRM, SAP, using mobile devices allowed employees to take full advantage of their out-of-office time. Hence, an employee whose work was field-based by design to spend their working hours out of the office M-ICT enhances their productivity by bringing the office assets to the field.

5. Current Usage of M-ICT

There is a lot that needs to be done in order to militate against the high risk of sensitive information leakage from the company due to amount of corporate documents being accessed from mobile devices. The fact that there is no control over the access of data through the mobile devices makes the company information insecure. Without control measures in place renders the system susceptible and a lot of sensitive and classified information becomes exposed and accessible to people who are not supposed to have that information.

This study was conducted in Namibia in the city of Windhoek and Telecom Namibia a parastatal company was taken as a case study.

The sample population of eighty (80) staff was drawn from the five departments of Telecom Namibia company across the country. According to authors in [12] they pointed out that if the population was less than 100, do not sample, survey the entire population. They further highlighted that, if the population size was around 500, sample 100. From their guidelines, hence this work sample size of eighty (80) employees which was regarded sufficient and true representative of the whole population.

The research employed a non-experimental research design that was descriptive in nature. [13] stated that non-experimental designs were mainly used in descriptive studies in which the units that had been selected to take part in the research were measured on all the relevant variables at a specific time. In light of [13], this study used the descriptive research strategy, which described the relationship between the uses of mobile devices, applications, and the possible threats it may bring into the company. Therefore, the questionnaire data was analysed by using descriptive statistics to determine the breadth of the M-ICT and develop an integrated enterprise application architecture. The research results present the variety of mobile devices, operating systems (OS), applications and usage preferences of the sample population. Furthermore it provided better understanding of the benefits and risks which guided the development of an integrated enterprise application integration strategy to enhance the mobile communication in TN.

The summary of the major findings based on this work were:

- 51% of the respondents owned laptop computers either company provided or privately,
- 7% owned desktop computers,
- 52% of the respondents have Apple tablets,
- 52% of respondents have Samsung smartphones,
- 51% of the respondents have Android smartphone operating systems,
- 24% of the respondents use their tablets on reading personal email,
- 21% of the respondents use their smartphone on send or receiving instant messaging / social media,
- 76% of the respondents use their smartphones and tablets for about an equal amount for work and personal reasons,
- 60% downloaded 1-5 applications on their tablets and smartphones,
- 60% use their mobile devices to access/interact through email,
- 60% use mobile websites to access/interact through emails,
- 62% spend less than 1 hour browsing on their mobile devices,
- 33% spend less than 1 hour outside of the office environment,
- 75% of the respondents agreed on the risk of sensitive information leaking from the company,
- 81% of the respondents did not get IT Factory support for their mobile phones,
- 54% of respondents were dissatisfied with the IT support

they received.

The findings from this study indicated a positive trend that laptop computers usage was still the leading mobile devices followed by the smartphones and tablets. It was noticed that Android OS was dominant among the mobile operating systems. In terms of user activity majority of respondents used tablets for reading email while they used smartphones for instant messaging and social networking. High number of respondents indicated that they used their smartphones and tablets for about an equal amount for work and personal reasons. Furthermore, respondents downloaded various mobile applications on their tablets and smartphones. Respondents used their mobile devices to interact mainly through emails and mobile websites. In addition, it was recorded that employees spend less than an hour on Internet browsing from their mobile devices. Majority of the respondents agreed that there was a risk of information leakage from the company through the use of mobile devices. Most respondents indicated that they did not receive any mobile support from IT Department.

6. Proposed TNEMA

Based on the findings of this work, it was evident that majority of employees owned multiple mobile devices with variety of OS, mobile applications and used it for both personal and work purposes. Furthermore, respondents indicated low usage with enterprise applications was attributed by little access to these systems from their mobile devices. This stressed more the need for M-ICT integration in TN to make enterprise applications accessible from mobile devices to empower employees and to reap the benefits of TNEMA.

Subsequently, the study recommended device agonistic enterprise application integration architecture to ensure data integrity through secured enterprise mobility infrastructure. Below is high-level design of proposed TNEMA in Figure 1.

6.1. High Level Design of TNEMA Components

- *User Interaction Spectrum* are communication channel among the different groups to enhance communication and collaboration such E2E, B2E, B2C, B2B, etc. irrespective of their physical location aimed at improvement of customer responsiveness, employee productivity and operational efficiencies [14]. This taxonomy is scalable and flexible to accommodate more communication channels.
- *User Mobile Devices* are mobile devices, including smartphones, tablets, laptop computers and other equipment that support multiple radio connectivity such as cellular and Wi-Fi. They also host voice and data applications on general purpose operating system (OS) environments such as Apple iOS, Android, RIM Blackberry, Windows Phone and others.
- *Access Networks* are mobile communication networks provided by cellular service providers such MTC, TN Mobile and Wi-Fi access systems e.g. public hotspots, which provide data, network connectivity [10]. Whether service provider or corporately controlled, these networks provide "mobility" through wireless data network access and "immediacy" that enables use of TN enterprise applications from anywhere and anytime [1]. Typically, TN is using wireless LAN within the campus area network which provides access between offices, buildings and towns thus can leverage on the existing Wi-Fi infrastructure.
- *Enterprise Mobility Infrastructure* provides the enterprise connection for all communications with user mobile devices. It includes call control to establish data connections with authorized mobile devices. Applications may be hosted here, or proxies/gateways may be provided to interact with mobile devices security applications and to route TN enterprise services traffic. Hence, the Enterprise Mobility Infrastructure (EMI) will secure, mediate, and manage the interaction between TN enterprise services and authorized mobile devices, applications and users. User requests for service are always routed to and handled by enterprise mediation; authentication and authorization decisions for access to secure data and services are made in the enterprise. The main component of the enterprise mobility infrastructure is the Mobile Enterprise Application Platform (MEAP) or mobile middleware with cross-form mobile development tools. MEAP as a platform includes following capabilities:
- Comprehensive integration capabilities – Connectivity to corporate systems such as SAP, CRM, Billing, etc.
- Mobile Application Development – Integrated Development Environment (IDE) for building mobile applications.
- (MDM) capabilities – Support for device provisioning, secure transmission of data, remote configuration, mobile asset tracking, policy identification and adaptation, etc.
- (MAM) capabilities – Support for provisioning and access control to mobile applications used in business settings (configuration settings, user authentication, push notification services, application usage analytics, etc.)
- Enterprise Backend Systems are the existing and evolving enterprise services provided for all TN users, including mobile users using enterprise applications. TN enterprise services include applications such as voice communications with evolved derivatives such as presence, chat, and conferencing using Microsoft Lync; email using Microsoft Exchange; corporate data via file servers; Intranet via Microsoft SharePoint; ERP using SAP; CRM/Billing via Huawei CBS, CTalk Call Centre and Track IT Helpdesk.

7. Security

Security infrastructure of proposed enterprise mobile infrastructure ensures secure access between mobile devices, access networks, TN enterprise services and data. Henceforth,

as depicted in Figure 1, security consists of firewalls between the access networks, Enterprise Mobility Infrastructure and backend systems. Furthermore, layers of encryption, authentication and authorization, boundary protection, possible hardening of devices, and mobile device provisioning and management all contribute to the overall security. In order to adequately protect sensitive information, the following cryptographic principles apply:

- To cross open access networks, two layers of approved commercial cryptography are required. One of these layers will be an Internet Protocol Security (IPsec) Virtual Private Network (VPN) which establishes a secured path between the mobile devices and the Enterprise Mobility Infrastructure. The other one is Public Key Infrastructure (PKI) to provide greater control over issuing, renewing, revoking, and managing Secure Sockets Layer (SSL) certificates while still gaining the advantages of using a trusted CA (Certificate Authority).
- The implementation of the two layers must be independent. Using two independent layers reduces the potential for compromise of classified or sensitive information in case of implementation errors.
- TN-issued PKI credentials should be used for mutual authentication in both layers. The mobile devices connect to the enterprise with layered encryption and authentication.
- All data between employees' mobile device and the Enterprise Mobility Infrastructure is protected in an IPsec VPN tunnel. The IPSec VPN connection must be established before connections to enterprise services are permitted. The VPN Gateway serves as the main entry point into the Enterprise Mobility Infrastructure and authenticates requested VPN associations using the Internet Key Exchange (IKE) protocol. A VPN client that cannot be identified or authenticated is denied access to the Enterprise Mobility Infrastructure and to all enterprise services.
- Within the VPN tunnel, application traffic is encrypted to provide an additional layer of protection. The inner layer may depend on the applications or services being used.

8. Conclusion

It is clear from the results of this work that the use of M-ICT in TN is widespread among the employees. However, the lack of M-ICT integration for TN enterprise services is undesirable. Moreover, the study highlights inadequate M-ICT support provided by IT Department. It is, therefore, important for TN IT management to provide a unified and secure TNEMA as illustrated in Figure 1 to address the issues of heterogonous device, application management and security for multiple devices per user environments.

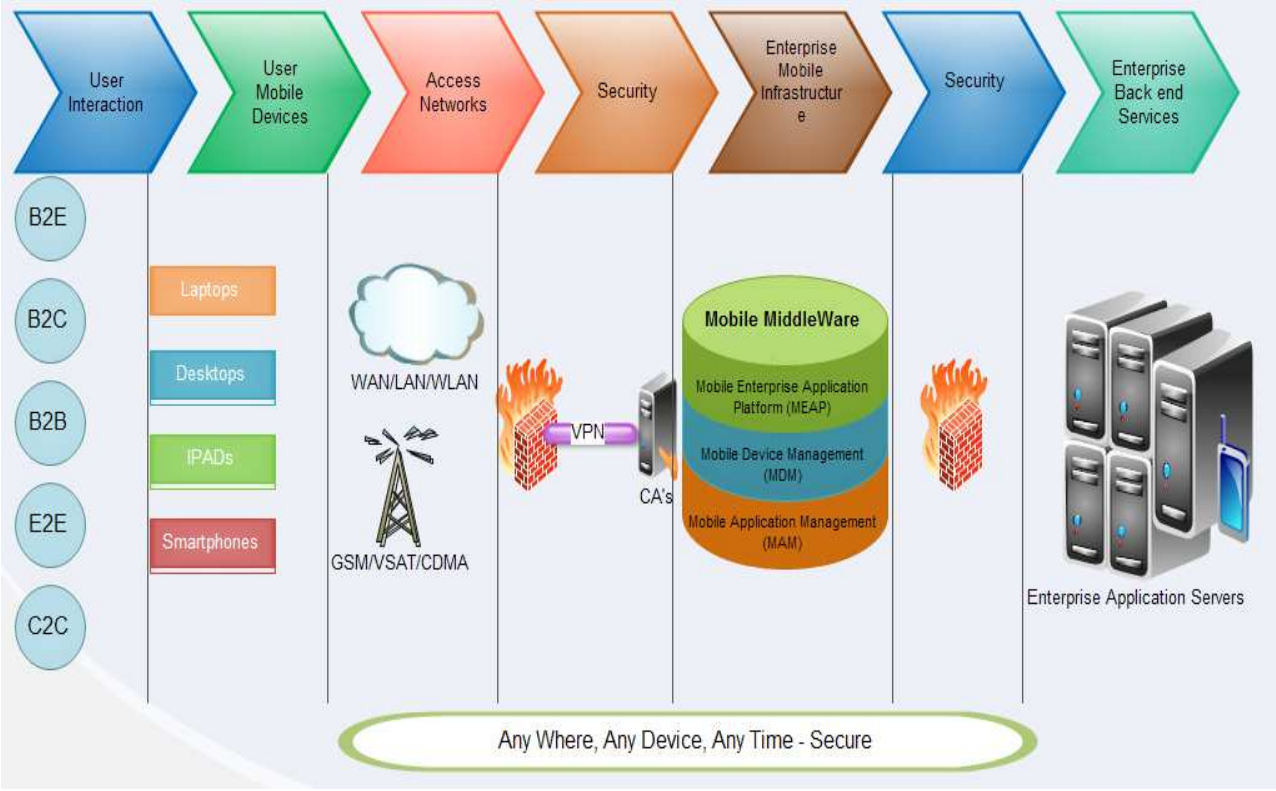

Figure 1. *High Level Design of TNEMA.*

Acknowledgements

We wish to acknowledge and thank the Telecom Namibia which is sponsoring the TNEMA project.

References

[1] Basole, R.C., (2008). Enterprise mobility: Researching a new paradigm. Information Knowledge Systems Management 7 (1). IOS Press

[2] Basole R. C., (2007). Strategic planning for enterprise mobility: A readiness-centric approach. Keystone, CO, USA, Association for Information Systems.

[3] Ernst and Young. (2013). Bring your own device: Security and risk considerations for your mobile device program. Retrieved on 15 January 2014 from www.ey.com/Publication/vwLUAssets/EY_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

[4] Muneer S., Sharma C. (2008). Enterprise mobile product strategy using scenario planning. Information Knowledge Systems Management 7, 211–224. IOS Press

[5] Price Water house Coopers. 2010. Bring your own device: Agility through consistent delivery. Retrieved on November 2013 from http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/BYOD-1-2011.pdf

[6] MTC (2013, March 27). MTC Namibia celebrates strong annual results; positions for 2012. Windhoek. Namibia

[7] Tao, J. & Chen, X., 2010. Web Service Based Enterprise Mobile Information System. Nanjing, Jiangsu, China, IEEE Computer Society, pp. 320-323.

[8] Kakihara, M., & Sørensen, C. (2002). Post-Modern Professionals Work and Mobile Technology. In Proceedings of the Paper presented at the New Ways of Working in IS: 25th Information Systems Research Seminar in Scandinavia (IRIS25)

[9] Krishnan, S. (2013). Enterprise mobility putting people first. Retrieved on 3rd December 2013 from www.pwc.in/en_IN/in/.../enterprise-mobility-putting-people-first.pdf

[10] World Bank (2011). World Development Indicators (WDI) database. Washington, DC: Author.

[11] Kornak, A., Teutloff, J., Welin-Berger, M. (2004). Enterprise Guide to Gaining Business Value from Mobile Technologies. John Wiley & Sons.

[12] Leedy, P.D., and Ormrod, J.E., (2010). Practical Research: Planning and Design, 10th Edition: New Jersey, USA.

[13] Maree, K., (2007). *First Steps in Research*, Pretoria, Van Schaik Publishers.

[14] Kietzman, J., Planggera, K., Eaton, B., Heilgenberg, K., Pitt, L., & Berthon, P., (2013). Mobility at work: A typology of mobile communities of practice and contextual ambidexterity. Journal of Strategic Information Systems. 3, 1-2