A GOVERNMENT FRAMEWORK TO ADDRESS IDENTITY, TRUST AND SECURITY IN E-GOVERNMENT: THE CASE OF UAE IDENTITY MANAGEMENT INFRASTRUCTURE

Dr. Ali M. Al-Khouri, Prof.
Emirates Identity Authority/Abu Dhabi, United Arab Emirates
British Institute of Technology & E-commerce, London, UK
Muhammad Farmer, Prof.
British Institute of Technology & E-commerce, London, UK
Jameel Qadri, Research Fellow
British Institute of Technology & E-commerce, London, UK

Abstract

Identity and trust are two important elements that surround any service-providing system. They become more critical when such systems operate in distributed environments and deal with sensitive details. This paper explains how a government-trusted digital infrastructure would address both identification and trust requirements and would support the development of citizen-centric government services. The main contribution of the paper is the presentation of a framework adopted by the government of the United Arab Emirates (UAE) that provides a systematic approach to creating a robust information-sharing system within a secure environment. A model is also presented to explain how synergy among institutions is planned to be achieved and how online users would access web-based government services with a single login using a universal smart identity card.

Keywords: Identity, authentication, E-government, digital infrastructure

Introduction

Communication and Internet technologies have transformed the ways that goods and services are produced and delivered today. Businesses and governments alike all over the world are working towards developing customer/citizen-centric operating models. The use of information and communication technologies to provide and improve private and public sector services, transactions, and interactions has enabled organisations in these sectors to deliver better services and improve the effectiveness and

efficiency of their operations (Asabere et al., 2012; Baumgarten and Chui, 2009; Jones and Williams, 2005; Kärrberg and Liebenau, 2009; Meltzer, 2014).

Such realisations have pushed citizens' expectations to new levels, forcing governments to intensify efforts and investments to enable increased contact with their citizens. Massive large-scale initiatives have been executed in the last two decades by governments in response to such needs and have been labelled with different terminologies such as e-government, smart government, Internet government, digital government, online government and so on. Regardless of what they are labelled with, all such initiatives seek to revolutionise public delivery systems, uphold the development of sustainable communities and promote more transparency and accountability (Atkinson and Castro, 2008).

Among other principal objectives is the desire to bridge the 'digital divide'. This term refers to economic inequality between groups, broadly construed in terms of access to, use of and knowledge of information and communication technologies (Brown et al., 1995; Chinn and Fairlie, 2004). The United Nations e-government surveys are key metrics to benchmark e-government development and guide policies and strategies that can improve overall public service delivery and thereby bridge the digital divide (United Nations, 2012). The UN surveys present systematic assessments of the use of ICT to transform and reform the public sector by enhancing efficiency, effectiveness, transparency, accountability, access to public services and citizen participation in 193 countries. According to the surveys, progress in online service delivery continues in most countries around the world. However, progress with the digital divide is far from satisfactory. Figure 1 depicts that 61% of the world's population still do not have access to the internet.

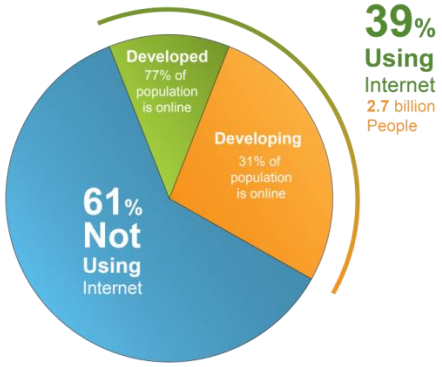

Figure 1: Internet connectivity in developed and developing countries (Source: ITU, 2013).

One of the key findings that emerged from the 2012 survey is that while it is important to continue with service delivery, governments must increasingly rethink their e-government approach by placing greater emphasis on institutional linkages among government structures in a bid to create synergy for inclusive sustainable development. From this standpoint, this paper attempts to outline the framework followed by the government of the United Arab Emirates (UAE) to promote trust, and hence social inclusion, in digital environments. The infrastructure is envisaged to support government transformation plans and to develop a citizen-centric governance structure. The framework represents the UAE government's planned systematic approach to creating a robust information-sharing system within a secure environment. A simplified model is also presented, to explain how synergy among institutions in the UAE is expected to be achieved and how online users would be able to access web-based government services with a single login using universal smart identity cards.

The subsequent sections in this article are structured as follows. We first outline the importance of trust and privacy as key elements for promoting digital inclusion; then, we highlight the importance of identity management as a key pillar for advancing e-government. After this, we provide a short introduction to the status of e-government in the UAE, and move on to delineate the implementation of a national identity management infrastructure in the country. In the subsections, we explain how the identity management infrastructure is envisaged to support electronic service provision and address the elements of authentication, data integrity, confidentiality and non-repudiation. We then explain how the UAE identity management infrastructure will be used to develop a one-stop single registration/login system to access all the services provided by the government. A high-level discussion is also provided on UAE government plans for data integration. Following this, the paper is concluded.

Trust and Privacy

Mayer et al. (1995) defined trust as 'the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party'. Any online service presents challenges in obtaining the trust of people to use the service, especially when people are required to part with sensitive information.

According to Marsh et al. (2009), challenges are significantly greater in e-governance than any other service such as e-commerce because, first of all, government services are often covered by privacy protection legislation that may not apply to commercial services; therefore, government services are subject to a higher level of scrutiny. Second, the nature of the

information involved in an e-government transaction may be more sensitive than that of a commercial transaction. Third, the nature of the information receiver is different in an e-government context: for example, medical records would be considered very sensitive if shared amongst all government agencies. Fourth, the consequences of a breach of privacy may be much greater in an e-government context where, for example, the premature release of economic data might have a profound effect on stock markets, affecting millions of investors.

As a result, any e-government initiative is completely based on how the framework is built to ensure that trust, security and the identity of users are managed and maintained to the highest standard. Electronic commerce research has found trust to be strongly related to information disclosure (Metzger, 2004). A study conducted in 2010 to measure privacy trust in the United States Government found that a majority of respondents did not trust the privacy commitments of the federal government (Ponemon, 2010). Certainly, the level of trust in online services directly affects the willingness of users to share information. It is in this context that an identity management system owned by national government is perceived as fundamental to enhancing the trust infrastructure in a country.

Identity Management: A Question of Responsibility

Identity, according to the *Oxford Dictionary*, is the condition or fact that a person or thing is itself and not something else. Biometric features, detected with the help of technological tools, are one of the best possible ways to establish a person's unique identity; however, details of personal information such as full name, date of birth, home address, and mother's maiden name have been widely used instead in both the pre and post-Internet eras. Nonetheless, biometric methods of identity are now being increasingly used across the globe.

Identity remains at the centre of all public and private sector information and financial transactions across digital infrastructures. However, there are important differences between government bodies and commercial organisations in terms of responsibilities, the amount of data retained and the duration of retention. The aim of a government body taking part in an e-service should ideally be to encourage every citizen, and other users, to register with the service so that it can be delivered effectively and efficiently; private organisations direct their efforts only at potential customers who can bring commercial benefit. Moreover, the information retained by government departments will most likely be held for longer than that retained by private or commercial organisations because citizens rarely wish to sever relations with government bodies. As a result, identity records, identity management, and related privacy concerns become even more

challenging for government bodies. For an e-government service to be effective and successful, the service provider must be in a position to verify and authenticate the identity of users. The UAE's identity management infrastructure is the one-stop answer.

First, let us discuss e-government status in the UAE, and then move on to consider the identity management infrastructure setup in the country to support e-government transformation.

UAE E-government

The UAE government has developed multiple short and long-term e-government strategies to support more effective and efficient digital governance models and to deliver modern services to its diverse customer base along a multitude of delivery channels (Al-Khouri, 2012). The UAE e-government strategy is part of a comprehensive and integrated system, involving different government entities, that aims to improve government services and make them available through innovative channels on a 24/7 basis (TRA, 2013). In less than a decade, the UAE e-government strategy has made rapid progress, setting an example of popular and effective e-government to support development, and has obtained a positive response from its citizens.

The UAE, according to the UN E-government Survey 2012, was ranked 1st among Gulf Cooperation Council (GCC) countries, 5th in Asia, and 28th in the world for e-government performance. The report says that the UAE's world ranking of 28th (with an E-government Development Index of 0.7344) is especially notable because the country advanced 21 ranking points in two years. The report goes on to draw an interesting comparison between Norway, which is 8th in the table, and the UAE, concluding that the UAE has achieved the same level of online services as Norway based on population and GDP per capita:

'The rapid progress made by the UAE is a best practice case highlighting how effective e-government can help support development. With double the population and three quarters the GDP per capita, the UAE has achieved around the same level of online services as those offered in Norway, a global leader at 8th position.' (UN E-government Survey 2012)

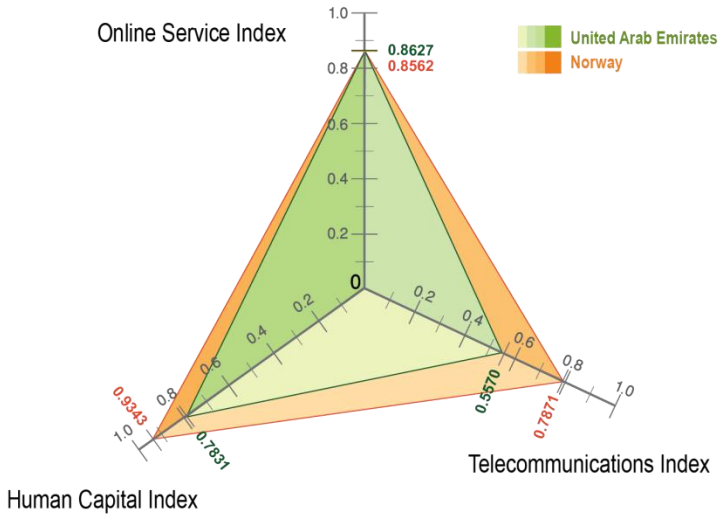

Figure 2: Comparison between e-government in the UAE and Norway (Source: UN Survey, 2012)

The e-government initiatives in the UAE are completely in alignment with the general principles of the UAE Government's strategic cycles for the period to 2021. Among other things, the strategies strive for integrated policies, effective coordination and cooperation among federal entities, the delivery of high-quality, customer-centric and integrated government services, the promotion of efficient resource management and the enhancement of transparent and accountable governance mechanisms (TRA, 2012; UAE, 2011; UAE-NA, 2012). A trusted government identity management infrastructure is one of the principal building block imperatives that the UAE government has initiated to enable e-government transformation, as we discuss next.

UAE National Identity Management Infrastructure

In 2004, the UAE government launched a national identity management infrastructure programme with a mission to facilitate the identification and verification of UAE nationals and foreign residents. The programme is designed to offer a solution to the identity and trust concerns of the e-infrastructure by providing trusted, secure and advanced identity cards, and by maintaining and updating the population register of the UAE. The key role of the e-infrastructure is to build the confidence level of users, who can then interact with government entities in a trust network.

The infrastructure's capability to establish a secure and trusted bi-directional information pathway between service providers and users will ensure the cyber-security and privacy of users. They will no longer need to register for individual services provided by different departments; instead,

they can use a single login facility with their national digital identity card. In effect, the UAE's identity authentication and verification services will act as a trusted partner between the service provider and user. However, bearing in mind that not all users are techno-literate and any technological solutions provided and explained by the UAE government may not fully convince them to share their personal information, a need is felt to apply other approaches to increase the level of confidence among e-service users, so that their willingness to share information is raised to a level where they feel secure and satisfied. These other approaches fall beyond the scope of this paper, and will be investigated in the future as an extension to it.

Security Measures of the Infrastructure

The UAE National Population Register is the main database for all personal profile information of UAE citizens, immigrants, and GCC citizens living in the country. The database stores biometric and personal information to establish a registered person's unique identity. The personal profile information of an individual is stored on a universal national smart ID card, which has personal information such as full name, date of birth, main and secondary addresses and occupation. The ID card provides a single secure document with public key infrastructure (PKI) enabled digital certificate and anti-fraud features. The national ID card service, and the population register, managed by Emirates ID, seek to achieve, among other strategic objectives, the management and maintenance of several population databases at a reduced cost, and to provide the digital infrastructure required to deliver the e-services of the e-government plan effectively and securely.

The UAE national ID card architecture is designed to deal securely with the risk-prone transaction of critical information. The architecture, based on layered environments, takes into consideration critical concerns such as the privacy and protection of personal information, user authentication and validation, system user trust building and accountability, and government policies. The architecture provides a solution to handle the enrolment and management of information and profiles within the population register in a secure environment. This environment is linked with other support environments for internal business operations; for example, communication on Internet channels via SMS and email, or obtaining data on e-forms which eventually become part of the population register. The support environment lies in the Internet zone, whereas the identity infrastructure operates in a secure non-Internet zone.

This configuration protects the population register from being exposed to possible external attacks. As stated above, the ID cards and the database servers are PKI-activated, and are therefore protected from network attacks such as man-in-the-middle, sniffing, tampering, and denial-of-

service. The PKI environment of the solution architecture is connected to the network zone where PKI entrusted security management is deployed. The PKI and certificate authority (CA) server, consisting of a digital certificate and synchronisation server hosting an Oracle database, authenticates any device on the network and regularly replicates the stored data to avoid any threat of loss and intentional or accidental data alteration.

Thus, the infrastructure offers the four main security features that any secured network should have for high-risk systems and applications. These are: authentication, data integrity, confidentiality and non-repudiation. This robust security and identity mechanism is important in order to build the required level of trust between the citizen on one side of the UAE's identity infrastructure and the government on the other in the G2C e-government model (Al-Khouri, 2013).

It is also important to ensure that if the value of a major data element changes, such a change is propagated across all enterprise systems. There are different components with close interaction in the population register system. They share web services which ensure that any change in personal data is accounted for in each of the dependent components. Further, any changes are communicated through secure channels using digital certificates and internal key management. The foregoing discussion identifies areas such as data protection, unauthorised sharing of, or access to, personal information, and the robust deployment of an identity management system, which have been addressed in the UAE by sound expertise and technological support.

Single Sign On: Synergy among Different Government Entities

Typically, government is a much more complex entity than any commercial or non-commercial organisation in terms of the number of service-providing departments and agencies and the tiered structure of these bodies. There are different stakeholders across government departments and agencies, with some unique, and some shared, interests and needs. However, from a user's point of view, government is seen as a single source for providing different services. This view of government as a single source is accentuated by the online presence of government services.

In pre-Internet days, citizens had to go to different physical offices for different services, or send postal mail to different offices at different physical locations; but as we have moved from 'brick' to 'click' offices, perceptions have changed. The user does not see, or is unwilling to see, the complexity of the processes involved in delivering the services. For him/her, the services are seen as originating from a single entity and from a single cyber-location.

Communication within departments is still not as robust as it seems from the outside. There are still gaps in setting up comprehensive

interoperability among different government entities, with the gaps based on the nature and functionality of the entities. The challenge that remains is how to deliver services to the user as his/her agenda requires. The *modus operandi* of the entire system of e-governance needs to be conceived and designed carefully because government is a much more complex entity than any commercial organisation. The two design approaches to provide services are explained below.

The first approach is to provide e-services to each user through individual departments. Each department will require its user to submit personal information details and will then have to register him/her for the service. The department will be required to verify and authenticate the user before providing any information and/or service. This means that each department will be required to develop its own digital infrastructure for identification, verification and authentication. The responsibility for privacy, data protection, and loss of information will be completely owned by that department. Given the number of departments and agencies providing different services, to what extent will a user be willing to submit details for different services?

The second approach is to create a one-stop single registration/login system for an integrated approach to all the services provided by the government. The single login agency or department will be responsible for identifying, verifying, and authenticating each user, who will be required to share personal information only once. The agency will own, and therefore be responsibility for, the user's personal information. This second approach has many advantages, such as: a) the cost and complexity in maintaining and managing the personal data will be reduced; b) compatibility problems associated with using different identity technologies and standards will be circumvented; and c) the user will not have to register for any new service that might be introduced after his/her registration. This is the model adopted in the UAE in a unique 7+1 architecture (see Figure 3).

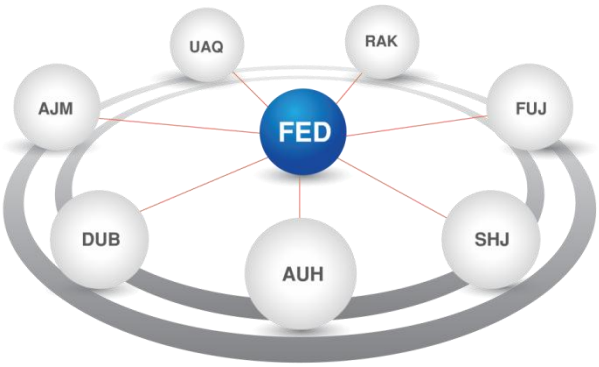

Figure 3: UAE federal and local e-government 7+1 architecture

Each Emirate caters to its citizens and residents by offering localised government. Each e-government authority aggregates the e-services into an Emirates Government Portal, thus enabling a single window for services on the web for each Emirate. The UAE identity management infrastructure is capable of providing a central shared authentication service and supporting infrastructure for authenticating a user and directing him/her to different departmental services, independent of the standards they use, and covers a wide range of requirements for delivering e-services. With the national ID card and population register database at the back end, the framework provides a robust solution. Identification and authentication will be carried out automatically at the login centre, and the user will then be directed to the pool of cloud services offered by different departments. In turn, e-government authority (the government services aggregator) is managed using the *national validation gateway* set up for this purpose by the Emirates ID authority. The e-government authority acts as the proxy for the ID authentication provided by the validation gateway, and further accords access to different government departments. The following simple model illustrates the logical position of the UAE's identity management infrastructure in the information flow.

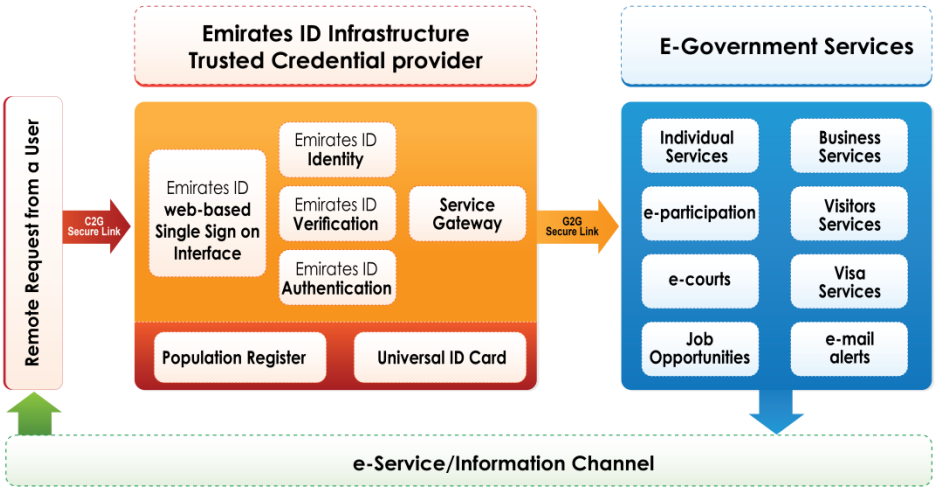

Figure 4: Emirates ID's user authentication model

A remote user wanting to use a government service will establish a secure connection with the e-government's web interface to provide his/her details. The service provider submits the ID credentials from the card to Emirates ID's identity management system. This will identify, verify and authenticate the user. The government service provider can alternatively allow the user to use his/her ID-linked user name and password to log in.

After authentication, the user will be connected to the gateway service, enabling him or her to visit a service of interest. The Emirates ID authentication system provides an identity federation service to the government service providers. The e-government portal uses this token and serves as the proxy required to handle the identification requirements of the different participating departments. Any further request from the same user in the same session will be handled directly by the service provider without a need for a second authentication. However, when the session is terminated, the authentication process will have to be reinitialised in order to access the e-services.

Data Integration Model

Data integrity is guaranteed by the digital signature that accompanies the data written into the smart card. This signature from the national identity management infrastructure can be verified online to assure the card data reader that the card is genuinely issued by Emirates ID and that the data has not been tampered with. PIN, biometric and digital certificate validation assure multiple factors of authentication on the remote channels. A transaction signed using digital certificates provides non-repudiation trust to the service provider. Since a transaction is carried out between the service provider and the service seeker on the basis of digital identity, confidentiality remains with the entities involved in the transaction, with no data held by the national identity management infrastructure. This explains how the UAE government has addressed areas such as data protection, unauthorised sharing of, or access to, personal information, and the robust deployment of an identity management system to support e-government infrastructure.

It is also worth noting that the UAE has been able to run a successful alpha test of the processes, integrating different ministerial bodies securely with the identity management system and the back-end databases. The test system uses 3-tier database-oriented middleware architecture, providing communication between the secured back-end identity management database and the web-based front-end application. Under test conditions, the system has shown that the proposed architecture is resilient at adapting to changing conditions and abrupt disruptions. The system is set up in a *high available* mode, with disaster recovery in place. The system is scalable, and is designed for easy upgrades.

Security measures are in place for the continual assessment and monitoring of the system against security risks and threats. The system is fully compliant with ISO standards and guidelines. The population register is on an isolated network and is not connected to the outside world. Internal security measures and controls are in place for internal resources access. The UAE's informational infrastructure has put in place mechanisms, such as an

audit trail, validation rules that permit changes, and user names and passwords, that provide secure administration of the back-end and front-end applications. These security mechanisms safeguard the personal information of users against improper information alteration or destruction.

Conclusion and Future Work

In order to make e-government effective and inclusive, users of the information infrastructure of the country expect reliable security for their transactions to be in place. On the other hand, the expectation of government entities is that the users of their respective systems are authentic and legally entitled to be using the systems. A trust model with a strong identity management system is needed.

In this paper we have analysed the UAE's preparedness, in terms of resources and digital infrastructure, to facilitate communication between users of e-services and service providers. The identity verification and authentication services will relieve a number of challenges faced by e-service providers while dealing with users' personal information. At the same time, the system will enrich the experience of users, by raising the level of trust they have in the way their personal information is handled and by allowing them to use different services with a single login. The system significantly enhances the ability to deliver e-services and drive the e-transformation of the country. Such a transformation contributes to the higher productivity and transparency of government service operations, which in turn provides a business-friendly environment, resulting in stronger national growth.

As an extension to this research paper, we will investigate and analyse mechanisms to improve the trust between users and government agencies with respect to e-governance and examine the potential for improving the integration and security of the systems. We will also discuss how interoperability could be enhanced to reduce redundancies.

References:

Al-Khouri, A.M. (2012). eGovernment Strategies: The Case of the United Arab Emirates, European Journal of ePractice, No. 17, pp. 126-150.

Al-Khouri, A.M. (2013). Connected Government: UAE Government Integration Strategy. Business and Management Horizons, Vol. 1, No. 1, pp.74-95.

Al-Khouri, A.M. (2014). Digital Identity: Transforming GCC Economies, Research, Innovation and Entrepreneurship Reforms in Gulf Cooperation Council (GCC) Countries, Journal of Innovation: Management, Policy & Practice, Vol. 16, No. 2, pp. 3594-3617.

Asabere, N.Y., Oppong, D. And Kusi-Sarpong, S. (2012). A Review of the Roles and Importance of Information and Communication Technologies

(ICTs) in Supply Chain Management (SCM) of Organizations in Supply Chain Management (SCM) of Organizations Organizations and Companies. International Journal of Computer Science and Network (IJCSN), Vol 1, No. 4, pp. 70-78.

Atkinson, R.D. and Castro, D. (2008). Digital Quality of Life. The Information Technology and Innovation Foundation. pp. 137–145. http://www.itif.org/files/DQOL-14.pdf

Baumgarten, J. and Chui, M. (2009). Mckinsey Quarterly. https://www. mckinseyquarterly. com/E-government_20_2408.

Brown, R.H., Barram, D.J. and Irving, L. (1995) Falling through the net: A survey of the have nots in rural and urban America. U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA). http://www.ntia.doc.gov/ntiahome/fallingthru.html

Chinn, M.D. and Fairlie, R.W. (2004). The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration. Economic Growth Center. http://www.econ.yale.edu/ growth_pdf/cdp881.pdf

Crawford, S.P. (2011). The New Digital Divide. The New York Times. http://www.nytimes.com/2011/12/04/opinion/sunday/internet-access-and-the-new-divide.html?pagewanted=all&_r=0

Department of Economic and Social Affairs (2012). E-Government Survey 2012. United Nations: New York.

International Telecommunication Union - ITU (2013). The World in 2013: ICT Facts and Figures. http://www.itu.int/en/ITU-D/Statistics/Documents /facts/ICTFactsFigures2013-e.pdf

Jones, A. and Williams, L. (2005). Public Services and ICT - Final Report: How can ICT Help Improve Quality, Choice and Efficiency in Public Services?. The Work Foundation, London. http://www.theworkfoundation. com/ downloadpublication/report/111_111_public services and ict final report.pdf

Kärrberg, P. and Liebenau, J. (2009). Enterprise Efficiency in the Use of ICT in China, France, Germany, Great Britain, India, Japan & the USA. London School of Economics. http://eprints.lse.ac.uk/42760/1/EnterpriseEfficiencyInTheUseOfICT.pdf

Marsh, S., Patrick, A.S. and Briggs, P. (2007). Social Issues of Trust and Digital Government. In: Information Security and Ethics: Concepts, Methodologies, Tools, and Applications. IGI Global, Hershey, Pennsylvania, USA, pp. 2892-2904. ISBN 9781599049373

Mayer, R. C., Davis, J.H. and Schoorman, F.D. (1995). An Integrative Model of Organizational Trust, The Academy of Management Review (20) 3, pp. 709-734.

Meltzer, J. (2014). Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-sized Enterprises and Developing Countries, (Working Paper 69), Global Economy Development, The Brookings Institution, Washington, DC. http://www.brookings.edu /~/media/research/files/papers/2014/02/internet international trade meltzer/ 02 international trade version 2

Metzger, M. J. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce, Journal of Computer-Mediated Communication, vol. 9, No. 4.

Ponemon (2010). 2010 Privacy Trust Study of the United States Government. http://www.privacylives.com/wp-content/uploads/2010/07/ ponemon-2010-privacy-trust-study-of-us-govt-06302010.pdf

Telecommunication Regulatory Authority - TRA (2012). UAE eGovernment Strategy 2012-2014. http://government.ae/documents/10138/98433/ eGov_Strategy_01-04-2012_Ar_new.pdf?version=1.0

Telecommunications Regulatory Authority - TRA (2013) mGovernement Road Map. http://government.ae/documents/10138/84716/mgovroadmap Finaldraft-v1-on+website+30122013.pdf/d98eac48-4f6a-4324-9763-210f52f695ae

UAE (2011). Highlights of the U.A.E. Government Strategy 2011-2013 http://government.ae/documents/10138/220393/Highlights+of+the+UAE+Government+Strategy+2011+-2013.pdf?version=1.0

UAE National Agenda – UAE-NA (2012). http://government.ae/web/guest/ uaenationalagenda.