Technology and Investment, 2013, 4, 7-12
http://dx.doi.org/10.4236/ti.2013.41002 Published Online February 2013 (http://www.scirp.org/journal/ti)

Identity and Mobility in a Digital World

Ali M. Al-Khouri
Emirates Identity Authority, Abu Dhabi, UAE
Email: ali.alkhouri@emiratesid.ae

Received October 22, 2012; revised November 20, 2012; accepted November 27, 2012

ABSTRACT

Mobile identity management has attracted the attention of both the public and private sectors in the last few years. In the context of service delivery, modern mobile communication networks offer more convenient approaches to developing citizen-centric applications. However, taking into consideration the need for compelling user authentication and identification, secure communication in mobile environments remains a challenging matter. This article explores the potential role of government-issued smart identity cards in leveraging and enabling a more trusted mobile communication base. It delves into the identity management infrastructure program in the United Arab Emirates (UAE) and how the smart identity card and overall system architecture have been designed to enable trusted and secure transactions for both physical and virtual mobile communications.

Keywords: Identity Management; Mobile Identity; National Authentication Infrastructure; Wireless PKI; Identity Provider; UAE

1. Introduction

Now more than ever, the world is transitioning drastically to digital spheres, in which the best possible use is made of digital technologies. Our transition to the digital world has been rapid and innovative, and it is now shifting us towards a more converged existence. It was not too long ago that discrete devices worked in isolation, but now they are ubiquitous and provide us with a seamless experience in service delivery that can be accessed virtually from anywhere and at anytime. For example, one could submit a service request on the Web, follow and track the delivery progress using a landline on IVR, call a contact center and update the request, provide additional information at a kiosk, pay using a credit card from a mobile phone, and receive the physical goods at the designated location and a confirmation of delivery via SMS. This is the reality of a converged digital world.

In this digital domain, all facets of mobile identity management are gaining wider attention from both the public and private sectors. Their significance lies in their contribution towards providing trust for transactions in user-centric applications and their impact on the overall context of service delivery [1]. However, this is not as tranquil as it may sound. The primary challenge is that mobile identity management systems need to be multilaterally secure and allow appropriate user access to data, while enabling privacy and anonymity [2].

Referring to the specificity of the mobile services field in modern networks, Srirama *et al*. (2006) state that there are some "characteristics unique to the mobile paradigm, the increased complexity of emerging handheld devices, the greater sensitivity to security and load related problems in wireless infrastructure and increased complexities of scale" [3]. This implies that we first need to have unified identification criteria that allow us to identify mobile and virtual individuals [2]. The role of an "identity provider" is crucial to confirm the credibility of the parties participating in a service or transaction [2]. It should provide sufficient credentials for service providers' relying parties to explicitly authenticate mobile users, thus enabling trust in the transactions being made securely.

In this article, we examine the role that a national identity infrastructure could play in the facilitation of mobile environments, with specific reference to the United Arab Emirates (UAE). In light of the current shortcomings in the existing literature about government practices in the field, we attempt to create government-published content to support the current body of knowledge that could support the development of both the practice and research fields.

This article is structured as follows: Section 2 provides a short overview of the role of identity, in light of converging digital technologies; Section 3 introduces the UAE's digital identity management infrastructure; Section 4 briefly describes the UAE's identity system and its service eco-system; Section 5 provides an overview of the digital ID profile and how it helps in establishing trust in the e-transactions; Section 6 presents how the

UAE identity management system supports mobility, both from individual and enterprise perspectives; Section 7 looks at some government plans that attempt to integrate mobile phones with its national identity management infrastructure to improve the accessibility of its services; and finally, Section 8 concludes with some perspectives.

2. Convergence of Digital Technologies

Digital convergence is an evolving reality. A key point is that this convergence is not just limited to technology, but also outreaches to user experiences. User interfaces, information, and services are all converging into computer-mediated systems that are independent of the communication channel and the device or communication tool (see also **Figure 1**). The user is geographically unbound and may interact, communicate, collaborate, and share information in many new and different ways.

Unquestionably, the body (entity) of central focus in digital environments is the person seeking the service, or in other words, the transaction initiator. Different stakeholders in this transaction lend their support, and the service provider delivers the requested service and ensures service fulfillment. A more revolutionary form of business operations may strike out when an irrefutable identity is made available for the service seeker, who is actually anonymous in the digital world.

Our digital world spreads across several threads, but they all meet in their needs for identification. In other words, the underlying enabler to our digital world is identity, which is:

- Uniform across multiple channels of communication;
- Standardized and usable in all contexts of identity verification;
- Issued by a *trusted identity provider* that enables authentication on demand across various communica tion channels.

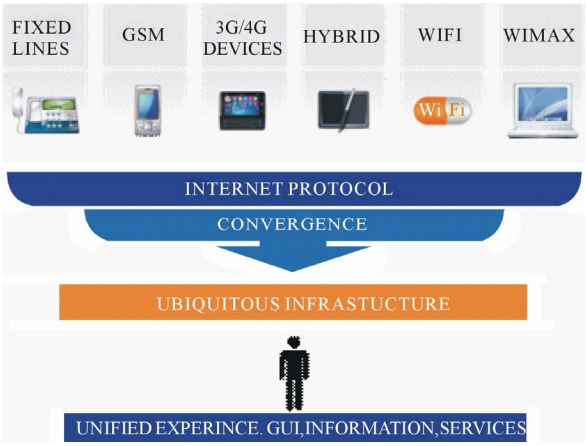

Figure 1. Convergence of digital technologies and citizen interfaces.

In reality, there are multiple providers of identity for any given entity, all jostling for space, which enable cross verification and authentication over diverse services. Thus, as long as the services are virtual, inter-dependent identity verification can suffice. Yet, with real services like physical goods, secure communication enablement, and financial transactions, higher trust requirements are needed for the completion of the transactions.

With such needs in mind and in an attempt to build the infrastructure for digital economies, many governments worldwide have awoken to the need to provide trusted and ubiquitous identities to their citizens [4-6]. In a space with multiple identity providers, government-issued identity credentials stand to become the most trusted construct. The issue that remains with such an identity is usability, which is fraught with risks of impersonation and identity theft. These risks have been addressed in other countries, as some have implemented, and many others are in the process of setting up, a *national authentication infrastructure* to provide seamless identification that bridges multiple service channels to enhance users' experiences and enable secure digital transactions [7].

3. UAE Digital Identity System

UAE has set a clear vision for digital identity issuance in the country. **Figure 2** depicts the smart identity card issued by the UAE to all of its citizens and residents. This comes as part of its national identity management program (also referred to as national identity management infrastructure) that was launched in mid-2005. In the seven short years since its launch, UAE has been a leading country in the Middle East and Africa in issuing more than 8.5 million digital certificates to its population. This represents 96% of its total population—99.9% of the citizens and 95% of the expatriate resident population. The digital identity provided by the UAE is composed of a set of credentials delivered in the form of a smart card, which includes a unique national identification number, biometric data (fingerprints), and a pair of PKI digital

Figure 2. UAE smart identity card.

certificates—one for authentication and another for signature (see also [8]).

4. UAE ID and Service Eco-System

The secure credentials issued by the UAE national identity management infrastructure are designed to support their use by the citizens and residents in both physical and digital environments. Smart identity cards with digital credentials are provided to facilitate government and public sector service delivery transactions, from across manned counters to transactions on the web. This is supported by multi-factor authentication capabilities and advanced identity verification mechanisms. **Figure 3** shows the context of the national identity card and the service eco-system in the UAE.

5. UAE National ID Card and Trust Establishment

The UAE national identity card is a smart combi-card with both contact and contactless communication capabilities. The card is an instrument that is packaged to carry the physical identity details of the cardholder, along with the digital ID profile, in the smart chip. The digital ID profile consists of:

1) A unique national identity number (IDN);
2) Biometrics (fingerprints);
3) A pair of digital certificates issued from the population certification authority (CA) of the public key infrastructure set up for this purpose.

Whenever a card is presented in any electronic (remote) transaction, the online validation center (*i.e.*, national authentication centre) validates the card by verifying its authenticity and the expiry date of the card. Whenever personal data is read from the card, the data is presented with the Emirates Identity Authority's digital signature confirming that the data on the card has not been tampered with. That the cardholder is who he/she claims to be is established using multiple factors of authentication, including a PIN verification and biometric verification.

A software development kit (SDK) is available on the government's Internet portal to promote usage and integration of the identity card with service providers' systems in both the government and public sectors. An applet is also available online for cardholders to download onto their personal computers to register themselves and use certain e-services that require strong authentication. These are but a few examples of the identity card's uses for which the SDK and the card applet have supported the development of auto-ID and mobile applications. Thus, the UAE national ID card establishes trust in the virtual, digital world and enables online transactions.

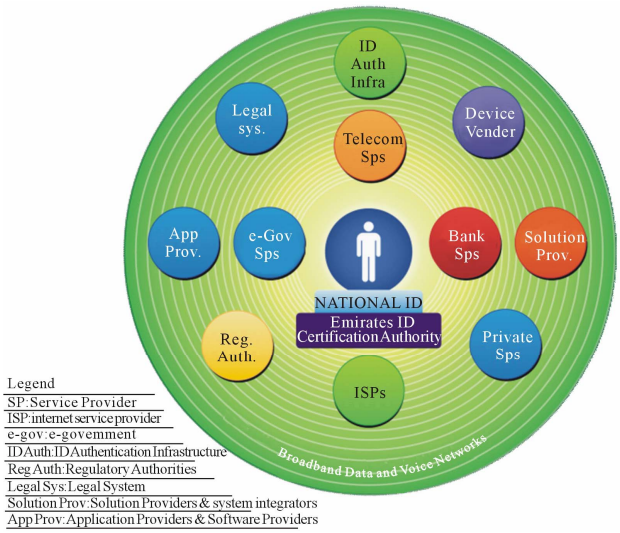

Figure 3. Identity and service eco-system.

6. Enabling Mobile Transactions

It is important to note here that the term mobility transcends individuals, enterprises, and the government. Each entity attempts to reach out to its respective stakeholders and be "available" at all times and over different communication media. Let us look at mobility from both individual and enterprise perspectives.

6.1. Individual Mobility

As mentioned earlier, individuals in the UAE are provided with smart cards that carry trusted identity credentials issued by the government. The digital identity associated with verifiable credentials is now available in the cardholder's wallet. This enables the individuals to present their IDs and credentials on demand to gain access to government or private sector services. Thus, the ID card provides verifiable credentials for a person wherever he/she goes.

6.2. Enterprise Mobility

Since verifiable credentials are available on demand, enterprises can now deliver services at the citizens' convenience without the citizens having to physically visit the service providers' premises—the service providers' premises have moved into the citizens' living rooms. For instance, service delivery agents carrying mobile PDAs could verify the service recipient's identity by reading the identity card data stored in the chip (See **Figure 4**).

Further authentication requirements could be met using PIN verification and/or biometric verification—both in contact as well as contactless mode. The current handheld terminals have add-on options for smart card readers that enable card reading through contact capabilities for example. The contactless capabilities of the identity card on the other hand enable the NFC mode to communicate with the HHTs/PDAs.

Figure 4. Mobile card reader terminal.

Cryptographic enhancements for biometric authentication on the HHTs/PDAs are possible by means of security access modules (SAMs), in the form of SIMs. Alternatively, the authentication infrastructure provided allows the HHTs to communicate securely on 3G/4G networks and to establish the necessary crypto-environment for biometric authentication.

The match-on-card feature for biometric authentication is used in both contact and contactless modes. This feature opens numerous possibilities for enabling e-commerce, in which identity is presented in a virtual world and goods are delivered to real entities that are identified authentically. A leading bank in the UAE is currently in the process of setting up a pilot system with the national identity cards for biometric authentication that uses handheld terminals to deliver bank debit/credit cards to their rightful owners.

Another initiative being developed is a pilot for opening customer accounts using customer services officers of banks to provide customer data by reading identity cards and signing to open the account by using the digital certificates in the identity card. This will follow the use of the identity card to conduct secure online financial transactions, which will use digital signatures and time-stamp capabilities. This, too, takes the banking business to the living rooms of their customers. The UAE's telecom service providers are also coordinating to use the national identity cards with NFC smart phones and enable mobile contactless transactions.

7. UAE National ID Card and the Future of Mobility

The UAE identity management infrastructure has laid a strong foundation and framework for identity verification and identity authentication. It has contributed to the development of an enhanced technological environment that facilitates secure transactions with true mobility. Developments in telecommunication networks and smart phones are revolutionizing people's lives. **Figure 5** provides an overview of mobile subscribers worldwide. UAE has nearly 150% mobile penetration, and smart phones are at nearly 100% utilization. The government is planning to integrate mobile phones with its national identity management infrastructure, in order to improve the accessibility of its services.

Public Key Infrastructure is an integral part of the UAE identity management system, with its population certification authority (CA) providing digital certificates for identity verification and digital signing. This capability can be extended to provide derived credentials for mobile users. This is a very interesting capability, since this infrastructure can be used to provide a wireless PKI. In other words, the UAE's government is working to issue certificates, in conjunction with the national identity, to mobile subscribers. The telecom networks would facilitate the transport and installation of the certificates onto their subscribers' phones. The private keys would be secured in an encrypted location on the SIM card itself, and not in the operating system of the mobile phones. This would tie in the mobile ID credentials to authentic national ID cardholders and valid phone subscribers.

This will serve two major objectives for the UAE. First, it would provide the ability for all national identity cardholders to conduct secure transactions with different service providers using their mobile phones, in a manner similar to the presence of the identity card. Digital signatures with time stamping would greatly enhance productivity and e-government transactions, and it would enable secure government communications.

Second, it would bring all non-identity cardholders under the realm of the national identity program. Thus, all visitors subscribing to mobile services would have digital certificates issued by the UAE national identity management infrastructure, which would enable them to conduct secure mobile transactions. This would also explicitly contribute to national security.

A typical example of using the mobile ID credentials derived from the UAE's national ID card is depicted in **Figure 6**.

The UAE has other exciting developments in the making that will use the post-issuance scenarios of the identity card to provide additional mobile services. One of the key initiatives in this direction is the ability of the national identity infrastructure to provide OTP (one-time-password) functions using Open AuTHentication (OATH) standards. As a post-issuance service, national identity cards could be loaded with an OTP applet that could then work in conjunction with NFC-enabled phones for an OTP for secure banking and financial transactions.

8. Conclusions

Most of the initiatives outlined here are likely to be instigated by other governments elsewhere in the world. Although some countries have initiated similar pilot projects, these are mainly being driven by the private sector, with little involvement from government bodies. Certainly, the development of mobile networks and commu--

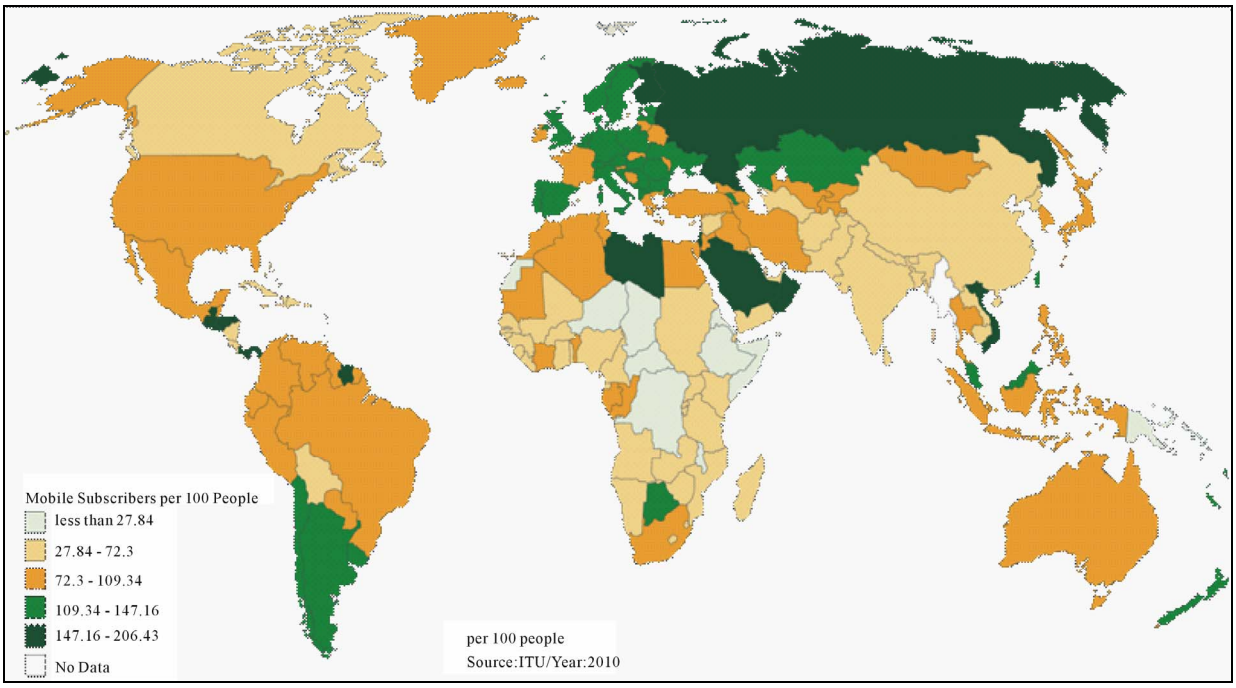

Figure 5. Number of mobile subscribers by country, per 100 people. Source: http://chartsbin.com/view/1881.

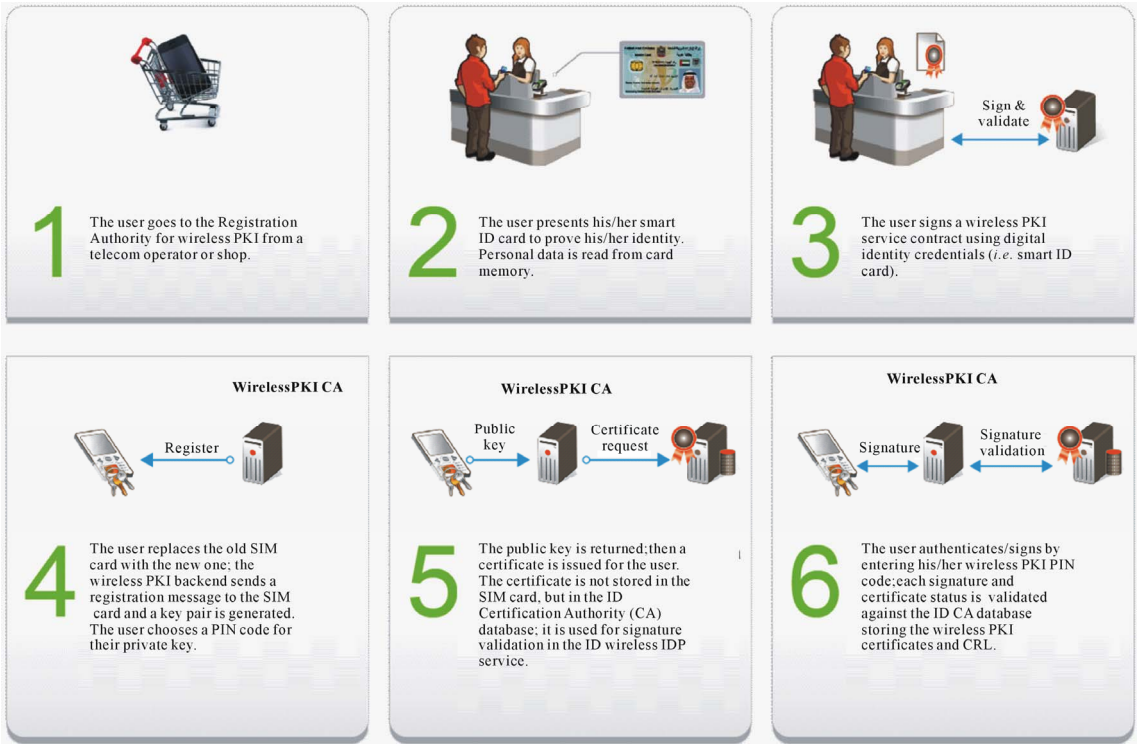

Figure 6. Wireless PKI registration and usage.

nication technologies will push governments to rethink their "role" and definition of "identity" in the digital world.

Governments are facing increasing pressure to improve the quality of life and address the changing and ever-complex needs of their populations. There will be no choice but to accept the concept of mobile identification. The future of "mobile identification" in the information era will determine the competiveness of countries and their readiness to survive the challenges of tomorrow.

Let us wait and see.

REFERENCES

[1] D. Royer, "Economic Aspects of Mobility and Identity," Future of Identity in the Information Society, 2012. doi:10.5121/ijmvsc.2011.2102 http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp11-del11.3.economic_aspects.pdf

[2] A. Deuker and D. Royer, "Next Generation Networks," Future of Identity in the Information Society, 2009. http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables2/fidis-wp11-del11_11_Next_Generation_Networks.final.pdf.

[3] S. Srirama, M. Jarke and W. Prinz, "Mobile Host: A Feasibility Analysis of Mobile Web Service Provisioning," *Proceedings of 4th International Workshop* (*CAiSE*' 06) *on Ubiquitous Mobile Information and Collaboration Systems* (*UMICS* 2006), Luxembourg, 5-6 June 2006, pp. 942-953.

[4] A. M. Al-Khouri, "An Innovative Approach for e-Government Transformation," *International Journal of Managing Value and Supply Chains*, Vol. 2, No. 1, 2012, pp. 22-43.

[5] A. M. Al-Khouri, "e-Government Strategies the Case of the United Arab Emirates (UAE)," *European Journal of ePractice*, No. 17, 2012, pp. 126-150.

[6] A. M. Al-Khouri, "Emerging Markets and Digital Economy: Building Trust in the Virtual World," *International Journal of Innovation in the Digital Economy*, Vol. 3, No. 2, 2012, pp. 57-69. doi:10.4018/jide.2012040105

[7] A. M. Al-Khouri, "Electronic Government in the GCC Countries," *International Journal of Social Sciences*, Vol. 1, No. 2, 2007, pp. 83-98.

[8] A. M. Al-Khouri, "PKI in Government Digital Identity Management Systems," *European Journal of ePractice*, No. 14, 2012, pp. 4-21.

[9] L. Haddon, "Domestication and Mobile Telephony," In: J. E. Katz, Ed., *Machines that Become Us*: *The Social Context of Personal Communication Technology*, Transaction Publishers, New Brunswick, 2003, pp. 43-55.

[10] J. Keeney, D. Lewis, D. O'Sullivan, A. Roelens, V. Wade, A. Boranand and R. Richardson, "Runtime Semantic Interoperability for Gathering Ontology-Based Network Context," *Network Operations and Management Symposium*, Vancouver, April 2006, pp. 56-65.

[11] W. Kim, "On Digital Convergence and Challenges," *Journal of Object Technology*, Vol. 4, No. 4, 2005, pp. 67-71. doi:10.5381/jot.2005.4.4.c5 http://www.jot.fm/issues/issue_2005_05/column5.pdf

[12] R. Mantena and A. Sundararajan, "Competing in Markets with Digital Convergence," 2004. web-docs.stern.nyu.edu/old_web/emplibrary/04-12Sundararajan.pdf

[13] M. Mueller, "Digital Convergence and Its Consequences," *The Public*, Vol. 6, No. 3, 1999, pp. 11-28. http://javnost-thepublic.org/article/pdf/1999/3/2/

[14] S. Narendra, "Connecting Identity and Mobility: A Secure, Scalable and Sustainable Mobile Wallet Approach," *IQT Quarterly*, Vol. 4, No. 1, 2012, pp. 18-21. http://tyfone.com/IQT_Quarterly_Summer2012_Tyfone_article.pdf

[15] J. Strassner, M. O. Foghlu, W. Donnelly and N. Agoulmine, "Beyond the Knowledge Plane: An Inference Plane to Support the Next Generation Internet," *Global Information Infrastructure Symposium*, Marrakech, 2-5 July 2007, pp. 112-119.

