THOUGHTS WITH IMPACT - PART 3

Critical Insights

From a Practitioner Mindset

Dr. Ali M. Al-Khouri

A Series of Published Articles in International Peer-Reviewed Journals

THOUGHTS WITH IMPACT - PART 3

Critical Insights

From a Practitioner Mindset

Dr. Ali M. Al-Khouri

A Series of Published Articles in International
Peer-Reviewed Journals

Preface

This book is the third in a series representing a collection of research articles published in several prominent peer-reviewed international journals. These articles are considered to contribute towards understanding management practices in the government sector. They symbolize the thoughts, experiences and learned lessons from large systems implementations in the United Arab Emirates and GCC countries and reflection on similar implementations in other countries in the world.

As we indicated in our previous series, existing publications on government practices are characteristically written from either an academic perspectives or touches the research areas superficially. We view these publications to have failed to capture critical management issues and considerations and make little or no use to practitioners. This is most often due to excessive concerns over data confidentiality and its use in the public domain.

Addressing the gaps in current literature is a key objective of our publications, not forgetting to adhere to scientific research structure, rigor requirements gathering, and coupled with the application of qualitative research methods primarily through the use of case studies.

The articles in this book have been grouped into four categories: (1) The New Digital Economy; (2) e-Government Practices; (3) Identity and Access Management; and (4) Identity Systems Implementation. These areas are considered to be crucial subsets that will shape up the upcoming future and influence successful governance models.

We aimed to be practical and attempted to put forward a readable content that exemplifies management practices in the government field and the efforts of the United Arab Emirates Government in particular. The articles in this book are considered to carry important knowledge pieces to both field practitioners and decision making authorities. They have been written from a philosophical "mind-set" that if we need to improve our organizations and thereafter our nations, we need to be transparent when we share knowledge and practices.

Our sincere and genuine goal behind this effort is the hope that these articles will help augment recent public sector development efforts in the United Arab Emirates, and the world over, and contribute to the advancement of research and serve as knowledge building tools for those interested in learning about public sector management practices in the United Arab Emirates.

Dr. Ali M. Al-Khouri
2012

Contents

The New Digital Economy

e-Government Practices

Identity and Access Management

Contemporary Identity Systems Implementation

The New Digital Economy

Emerging Markets and Digital Economy:

Building Trust in the Virtual World[1]

DR. ALI M. AL-KHOURI

ABSTRACT: This article provides an overview of the literature surrounding emerging markets and the global paradigm shift taking place towards the development of digital economies. It provides a review of recent practices in the government sector. The article promotes the concept of developing a government based identity management infrastructure to support the progress en route for building the digital economy. In light of the ever increasing information security threats in today's interconnected world, the article emphasizes that only through identification and authentication capabilities, emerging markets can maintain sustainability.

Key words: *emerging markets, digital economy, digital identity, identity management.*

[1] Al-Khouri, A.M. (2012) "**Emerging Markets and Digital Economy: Building Trust in the Virtual World**", International Journal of Innovation in the Digital Economy, Vol. 2, No. 3, pp. 57-69.

1. INTRODUCTION

THE world today is witnessing a huge shift in the economic power with the hitherto niche countries taking center stage, pushing the main players to the sidelines. The emerging markets have positioned themselves as knowledge based economies, working as the production houses and back office service providers for the current mature markets. We cannot but take cognizance of countries like China, India, Brazil, Korea, Malaysia and Resurgent Russia upstaging Euro Bloc countries and the US with their explosive growth figures. These emerging markets of today are fast set to become the main markets of tomorrow.

This defines the new order economy. The current mature markets are intricately integrated with the emerging markets in trade. The global integration is necessitated by a free flow information exchange and, in real time. Simply put, there are no alternatives but to become "more digital" with whatever assets are available (EIU, 2010). However, digital economy raises questions of security, privacy and trust. Computer and network security present great challenges to our evolving information society and economy (Cybenko et al., 2002), as global business will become ever more complex in the next three years, with more suppliers, more customers, and more digital payments (EIU, 2010).

Information networks aren't the same as they were just a few years ago. The channels of information dissemination are just simply too many now to list for a discussion. Information flows through broadcast channels, pod casts, databases, telephone networks and now the converged channels of the Internet. The moot point here is to determine “how do we ensure that the right information is provided to the right person at the right time in the right manner to ensure right outcomes”. There is a clear need for a sound identity management and authentication strategy to support global business growth. This article explores this critical area of practice. It provides an overview of the importance for such infrastructure development to maintain sustainability in emerging markets.

This article is structured as follows. The first section provides an overview of emerging markets, what they stand for, and the key drivers behind their development. The second section sheds light on the striking feature of the emerging markets that has characterized their growth and provides a conceptual overview of the term digital economy. The following two sections discuss the challenge of securing information networks and the need for a government based identity management system to address trust requirements. This is followed by a discussion and reflection on key areas around the subject matter and the article is concluded.

2. EMERGING MARKETS

Emerging markets is a term referred to the bloc of countries that are setting a new world order in economics. These countries have demonstrated a high rate of industrialization and growth rates in GDP[2] and prominent increase in their businesses; be it commercial

[2] Gross domestic product (GDP) refers to the market value of all officially recognized final goods and services produced within a country in a given period. GDP per capita is often considered an indicator of a country's standard of living; and is not a measure of

or social. In general, about 40 nations across the globe make the cut. These are the countries that have a very high economic activity; akin to the advanced "developed" nations like the USA, UK, France, Germany etc, but not quite there. Nonetheless, they are considered to wield big economic power. These countries spread across three major continents as depicted in Figure 1. The different shades of colour represent the strength in economic activity. The red colour represents countries with larger economic growth and business activity, which are also defining the world trade today and influence global investment decisions.

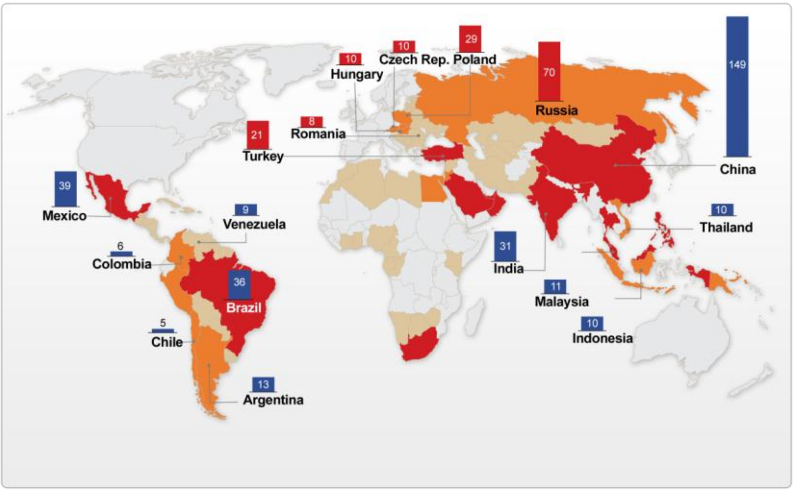


Figure 1: Emerging Markets Landscape

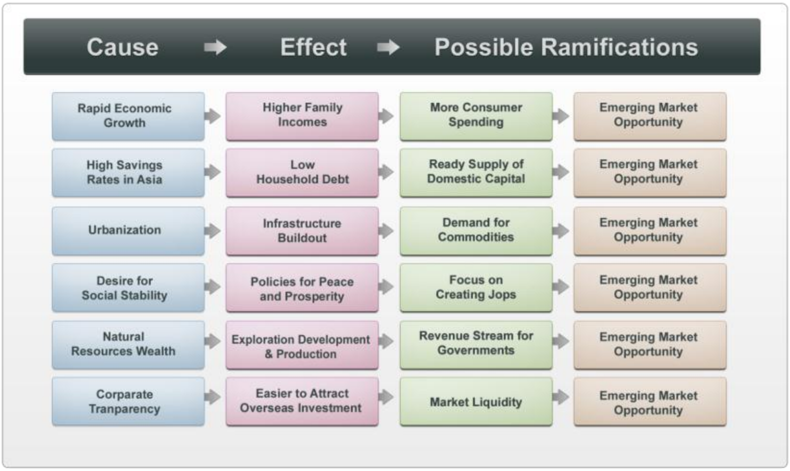
personal income. Gross domestic product is related to national accounts, a subject in macroeconomics.

GDP can be determined in three ways (1) the product (or output) approach; (2) the income approach: , and (3) the expenditure approach.

The most direct of the three is the product approach, which sums the outputs of every class of enterprise to arrive at the total. The expenditure approach works on the principle that all of the product must be bought by somebody, therefore the value of the total product must be equal to people's total expenditures in buying things. The income approach works on the principle that the incomes of the productive factors ("producers," colloquially) must be equal to the value of their product, and determines GDP by finding the sum of all producers' incomes

Among the emerging markets, some of the nations have higher sustained growth rates than the rest; and they construct what is referred to as the big emerging markets (BEM). Four nations are forming the foundation for emerging markets, namely; Brazil, Russia, India, and China also referred to as the BRIC of the emerging markets. These countries have demonstrated a substantial domestic consumption along with high exports, which altogether contributed to rapid core industrialization and the growth of the service industry. Countries of Colombia, Indonesia, Vietnam, Egypt, Turkey and South Africa are considered to form the second bloc of emerging markets; also referred to as CIVETS.

Emerging markets are changing the way the world works by developing into global powerhouses. Holmes (2010) identified six key drivers for emerging markets and the effect they have on the economic vitality in these markets. These are presented in Figure 2.



Cause ➡	Effect ➡	Possible Ramifications	
Rapid Economic Growth	Higher Family Incomes	More Consumer Spending	Emerging Market Opportunity
High Savings Rates in Asia	Low Household Debt	Ready Supply of Domestic Capital	Emerging Market Opportunity
Urbanization	Infrastructure Buildout	Demand for Commodities	Emerging Market Opportunity
Desire for Social Stability	Policies for Peace and Prosperity	Focus on Creating Jops	Emerging Market Opportunity
Natural Resources Wealth	Exploration Development & Production	Revenue Stream for Governments	Emerging Market Opportunity
Corparate Tranparency	Easier to Attract Overseas Investment	Market Liquidity	Emerging Market Opportunity

Figure 2: The 6 drivers of emerging markets. Source: Holmes (2010)

The literature indicates that BRIC countries together will yield more economic power than the G6 Nations by 2040 (Wilson & Purushothaman, 2003). With scorching double digit growth for the last few years, China will overtake the US shortly and according to analysts it is set to become the world's top economy in terms of world trade by 2015. India is expected to push the US further down to third place in a few more years to claim the second spot. Many Asian countries will follow suit flexing their surge in growth to become major economic powerhouses. Talking in numbers, world trade is expected to reach 371 Trillion USD in 2050 from the current 37 Trillion USD, with Asia expected to take as much as 46 percent of this according to a recent report by Citigroup (Buiter and Rahbari, 2011). See also Figure 3.

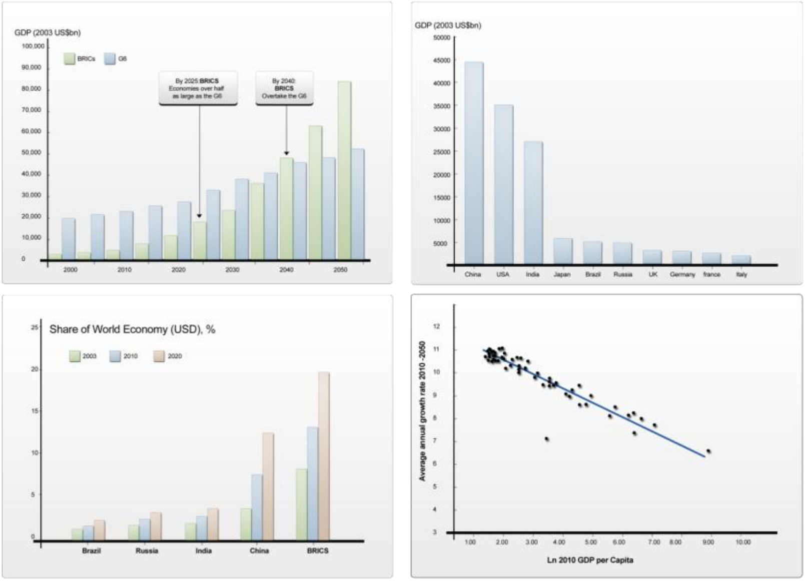


Figure 3: Emerging Markets Economic Activity

This is consistent with the population growth expected in these countries and the continent. With nearly two thirds of the world living in Asia, these countries are bound to become major economic powerhouses, emerging from their current fringe statuses. China, India, Malaysia are already on this growth radar as illustrated in Figure 3. A striking feature of the emerging markets is the digital leap that has characterized their growth. This is discussed next.

3. THE DIGITAL LEAP

Technological advances and market demands have made telecommunications and ICT products and systems increasingly complex and feature rich. This has enabled the development of the concept digital economy. Digital economy is an economy based on electronic goods and services and formed by an electronic business models. In other words, it is referred to the global network of economic and social activities that are enabled by information and communications technologies, such as the internet and web technologies (Shaw, 2006; Tapscott, 1997).

The ever-increasing efficiency of technology is changing the nature of work and therefore economic value (Kelly, 2011). This to say that the economics today are utterly different. The fundamental difference is that, while in the old economy, promoting efficiency and organizing work reigned supreme, in the emergent new economy inspiring the passions of employees to create and innovate is far more important (Chandra & Khanijo, 2009; Neef, 1997).

We need to comprehend that the 21st century is digitally driven economy. The concept of a digital economy emerged in the last decade of the 20th century (Tapscott, 1998). Negroponte (1996) argues that the fundamental distinction in the new economy is between "atoms" and "bits". See also Table 1.

Table 1: Atoms economy vs. Bits economy

	Atoms Economy	Bits (Digital) Economy
Distribution	Slow Extensive Labour intensive	Instant Free Brain Intensive
Based on	Scarcity	Abundance
Pricing	Inflationary	Deflationary
Inventory	Limited	Unlimited
Created	Mass Media Advertising	Relevancy/Targeted Adverting
Progress	Incremental	Exponential
Currency(s)	Money	Money Reputational Currency Attention Currency
Consumption	Once	Unlimited (increasing returns on consumption)
Free	Ad supported Gimmick/Sample	Ad supported Valid business model

He stated that the world had been based on an economy of "atoms" (physical stuff that we dream up, manufacture, and distribute, through a slow moving, "human handling" economy), whereas the future is about the "bits" economy or digital economy which is "...instantaneous and inexpensive transfer of bits at the speed of light." In other words, in this new economy, digital networking and communication infrastructures provide a global platform over which people and organizations devise strategies, interact, communicate, collaborate and search for information. Changes in today's business and consumer marketplace strongly supports Negroponte's proposition that digital bits are starting to become more valued than physical products made from atoms.

In line with Negroponte's proposition, and developing on the earlier work of (Kondratiev, 1925) and (Schumpeter, 1942), Perez (2002) defines the concept of “Techno-Economic Paradigm Shift” and explains how a new technology lies at the base of every revolution:

> "When the economy is shaken by a powerful set of new opportunities with the emergence of the next technological revolution, society is still strongly wedded to the old paradigm and its institutional framework. The world of computers, flexible production and the internet has a different logic and different requirements from those that facilitated the spread of the automobile, synthetic materials, mass production and the highway network. Suddenly in relation to the new technologies, the old habits and regulations become obstacles, the old services and infrastructures are found wanting, the old organisations and institutions inadequate. A new context must be created; a new ‘common sense’ must emerge and propagate."

Perez (2002) draws a line between the various technologies which have caused a great impact on the economy. According to Perez

(2002) we are now experiencing the fifth wave of Kondratiev. ICT is the technology that started this wave and it is causing a new paradigm shift.

As depicted in Figure 4, there is a very big difference with the earlier economic cycles we have experienced. The other cycles (water, steam, steel and oil) were all focused on producing tangible resources. The outcome of the ICT cycle is completely different. We are now producing intangible resources. This exemplifies the shift from atoms to bits. The information superhighway is about the global movement of weightless bits at the speed of light.

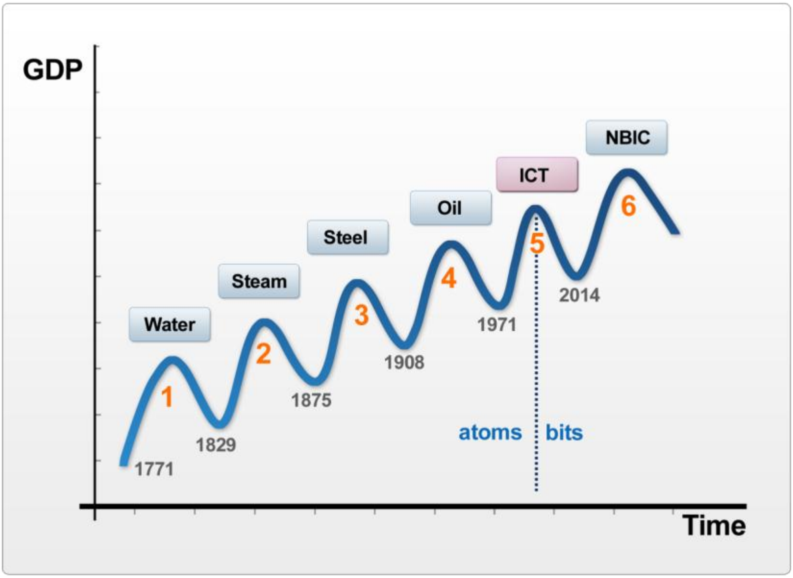


Figure 4: Kondratieff Waves

Indeed, repaid technology evolution has made digital economy a more viable alternative to both individuals and corporations. Technology has advanced in sync with industrial output. Higher industrial output meant higher productivity and profitability needs. In manufacturing terms, this has necessitated process optimization and therefore process automation. This was the turning point for technology development in emerging markets. Driven by a strong domestic consumption, the emerging markets have turned to technology for improving their productivity rates. Backed with a strong pool of skilled human resources, technology investments thus became the order of the day for these nations. In fact, the emerging market nations skipped a whole generation of technology adoption to adapt and adopt the latest in the industrial, communication and information technologies to lead and drive their knowledge based economies.

We are living in an information era, where societies around the world are becoming more and more information intensive. The reality is that we are living in a connected and united world were borders have disappeared on the information and communication highways. Needs of both advanced and emerging economies to cut costs and responding to rapidly growing industries and technology adoption, resulted in an explosive growth in connectivity. See also Figures 5 and 6.

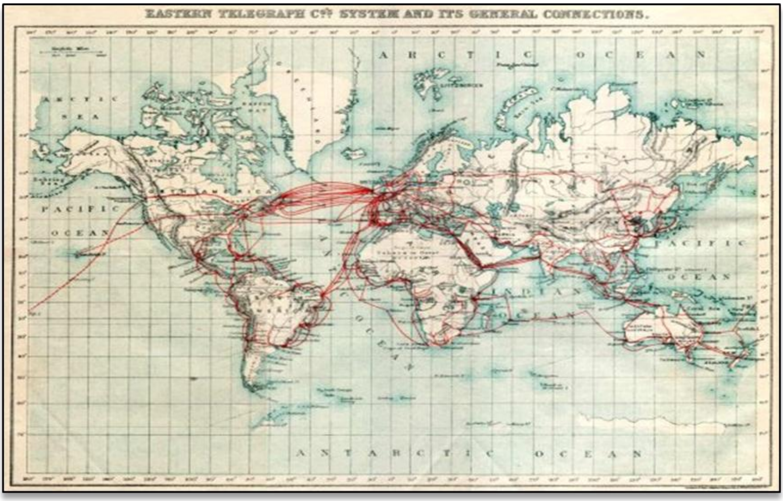


Figure 5: 1901-eastern-telegraph-world-cable-map - This is what the world's submarine cable system looked like in 1901 according to the Eastern Telegraph Company.

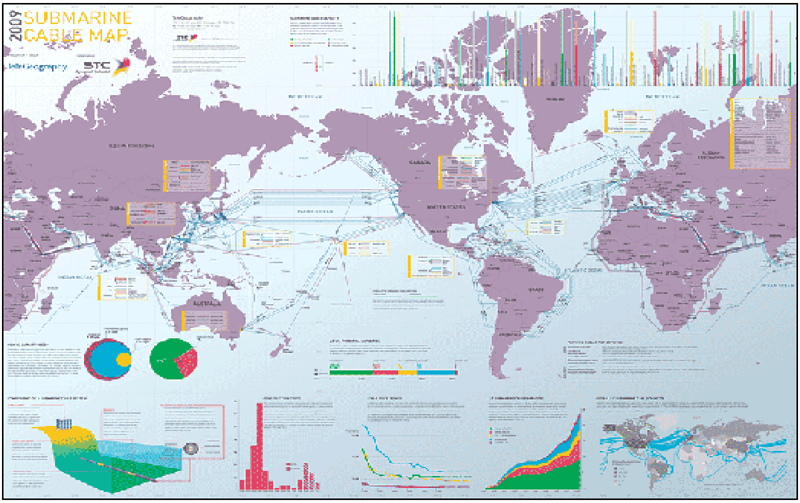


Figure 6: Submarine Cable Map [Image via Telegeography]

Looking at the submarine cable map in Figure 6, it shows how dependent we are, as a planet, on each other. Never has technology and commerce united the nations as it is now. However, in the digital world we live in, information security is the most serious risk that needs to be addressed by both governments and private sectors. Such digital exchanges can generate huge benefits for counterparties, but they also create a new breed of challenges and risks related to authenticating and certifying business partners and transactions (EIU, 2007).

The explosive growth of internet and e-commerce has taken Internet fraud to new levels (Meulen, 2011; McNally, 2011). More and more consumers are exposed to the risk of identity theft (Stickley, 2008). The potential for fraud is a major hurdle in the evolution and growth of online commerce (Cruz-Cunha and VarajÃ£o, 2010; Xu, J. and Quaddus, 2010). The next two sections discuss the issue of security and identity management in more detail.

4. INFORMATION SECURITY: THE CHALLENGE

Undeniably, information is a highly valued commodity to be protected and saved. Nations need to protect their Intellectual Property Rights (IPRs) in the digital world we live in (Gates, 2000). As such, networks need to be secured. In this age, information networks face severe potential threats. Technologies such as firewalls provide protection at the network periphery to secure internal systems from potential hacking attempts. Intrusion detection and prevention systems are increasingly being used to proactively monitor and thwart attacks from the outside world. There is literally war out there! Stakes are at very high risk.

For all the security we accord and try to provide, we can only do so much in protecting our information. We can thwart the outsiders and protect the insiders. What happens when the threat is from internal trusted sources? It has been proven beyond doubt that the biggest threat to information security is from internal "trusted" sources (Brancik, 2007; Contos, 2006; Probst et al., 2010).

It is so very easy to secure information by simply locking it away and denying access to it for everyone. But this does not serve the purpose of business. Information is needed to transact and for decision making. But once again, information in the hands of unauthorized people is treacherous. We need to secure information and yet make it available as needed.
The concept is rather simple; only provide information to authorized people or systems. People who are determined as non-authorized should not have the ability to access specified information. But in practical terms, how can this be achieved? The answer is "identification". Identification is the key to information security. We need to identify the authorized individuals who can receive authorized information. This should be understood in the context of identity management, as the next section elaborates on.

5. IDENTITY MANAGEMENT

Consumers are drivers of the digital economy. Identity in the physical world is expressed in a variety of forms: driver's licenses, passports, and more. For online applications, however, identity typically boils down to a set of bits that are transmitted across the wire, and then used by systems (Chappell, 2007). Being provided with the fast spreading and timely information on the Internet and mobile devices, the digital economy raises questions of security, privacy and trust (Laudon and Laudon, 2008; Turban et al., 2007). In simple terms, network security is complemented by information security and information security is achieved by identity management. Identity, therefore, forms the basis of any transaction.

Absorbing the needs of the future, governments in emerging markets have realized the need to put in place an infrastructure that can run synonymously with their hi-tech development requirements. Many countries in the emerging markets have begun to launching digital identification programs to provide digital credentials to their population. South Korea, Malaysia and India are shining examples of the emerging nations on the digital fast lane. Belgium, France, USA, Singapore have their share of success to share on the digital identity to their residents. In general, the emerging market nations are catching up fast on issuing digital identities to their population.

The digital identity provided by governments is becoming a reference point for personal identification providing the ability to electronically identify individuals over virtual networks such the internet (Al-Khouri, 2011; Westland and Al-Khouri, 2010). Technological advances in the field of biometrics have provided the ability to verify identities, validate credentials and allow authorized transactions in real time.

Biometrics, coupled with public key infrastructure (PKI) technology, form a unique personal identification profile. Issued by the government, such identity profiles become legally binding. The use of smart cards is seen as an enabler for electronic identification and provides the basis for identity validation for real time verifiability (Al-Khouri, 2011). See also Figure 7. With such technologies, trust is established remotely between the information seeker and the information provider; making the information exchange very secure.

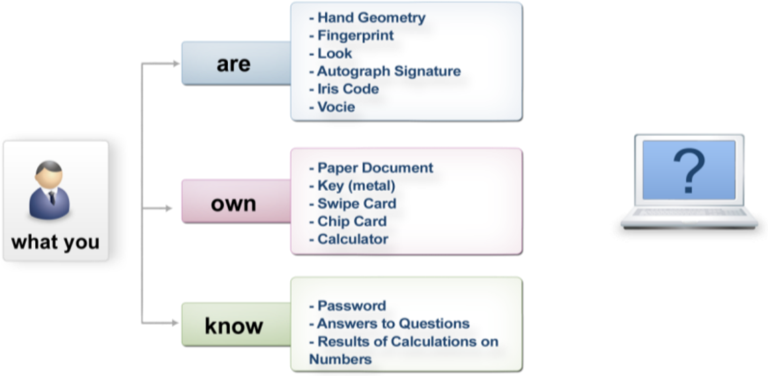


Figure 7: Multiple factor authentication

Figure 8 depicts a generic framework for applications of digital identities. Governments as a trusted source, issue national identity to their population. Such national identity establishes a legally accepted and binding identity of an individual that can be verified physically on site, or remotely over the internet.

Authentication mechanisms accorded by multiple factors such biometric, PIN and digital signatures allows secure transactions to take place. The framework basically encompasses a generic identity management model, where an identity profile is established, and can be used for audit trails and tracking purposes.

The multi factor authentication capabilities ultimately provide authorization to either physical or logical access.

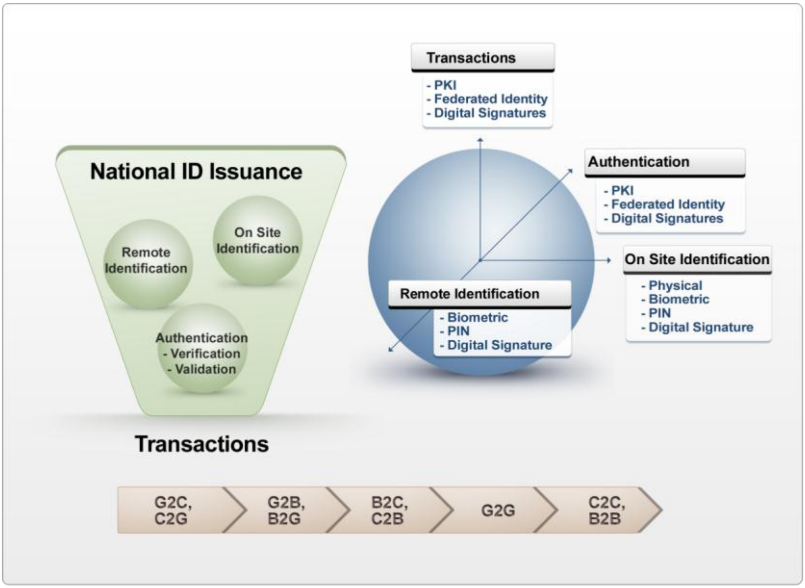


Figure 8: The digital identity paradigm

6. DISCUSSION

It is useful to think of the digital economy as having three primary components; supporting infrastructure, electronic business processes (how business is conducted), and electronic commerce transactions (selling of goods and services online) (Mesenbourg, 2000). The focus in practice has been on the process and much on the transactional sphere, but little attention was given to infrastructure development.

We very much emphasise on the role of governments to support the development of their own economies. The private sector alone cannot address the challenges related to identity management. The contemporary economic systems are pushing governments to share economy development responsibilities with the private sector rather evenly. See also Figure 9. The role of the government here, besides other responsibilities, is to lay down an identity management infrastructure through which trust can be established between the different entities.

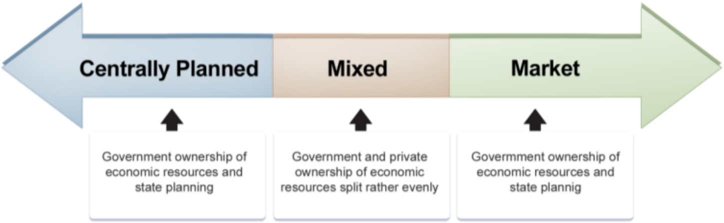

Centrally Planned
Mixed
Market
Government ownership of economic resources and state planning
Government and private ownership of economic resources split rather evenly
Government ownership of economic resources and state plannig

Figure 9: Economic System Models

In addition, it is important to note that a common feature of both electronic business processes and electronic commerce transactions is reliance on the use of computer-mediated networks. The reliance on the use of computer networks, and the benefits they can provide, is the "bottom line" difference between electronic and other kinds of business.

We should talk about entity identification in the same breath as network security and information security. Never has been identification so intricately associated with information security as it is in the present context of information dissemination.

Conventional wisdom has dictated the design and implementation of well proven technologies for protecting the networks from external threats like viruses, malware, hacking etc. Network Peripheral Protection has now evolved from conventional firewalls to intrusion detection to the current intrusion prevention systems. The trend is increasingly moving to deploying unified threat detection and prevention systems that combine network access policies, signature detection, and packet inspection with proactive monitoring of traffic from the external sources on the network.

While these technologies and measures provide a good degree of protection from external threats, and as we stated earlier that the biggest threat to information security comes from internal sources. This has led to development in technologies providing logical protection for information. Information sources need protection from unauthorized accesses apart from secure storage.

The critical parameter in sharing and shoring of information is trust or rather lack of it. The risk associated with this threat gets accentuated by the perception of the breach of trust. Many breaches have occurred by unwitting highly trust worthy entities dropping their access codes or passwords. This brings us to the all-important topic on management of identity.

Face to face, people have always shared information based on their personal mutual trust. This has always been the case with the digital leap economies. Now with the current network technologies enabling anywhere and anytime connectivity, information sharing is more remote than in person. The challenges have compounded thus in establishing trust between entities who are more often than not in asynchronous mode of sharing.

The challenges in identity management are by no means small. It needs commitment, political will, investments in technological infrastructure and seamless network connectivity (Bertino and Takahashi, 2010; Annunzio, 2007; Williamson et al., 2009). The examples of governments, who initiated digital identity programs, are likely to yield impressive results in the days to come. But this is subject to multiple other factors related to the clarity of the vision and the solidity of the path and the plans.

It is worth clarifying that providing a digital identity goes much beyond an identification number and a record in the national population register. The identity issuer stands for identity issuance, identity validation, identity verification and identity validation. An identity profile typically consists of a person's personal unique data including biometric data.

The digital identity consists of a digital certificate issued from a public key infrastructure (PKI) and a set of electronic biometric data. Together these characteristics provide irrefutable and more importantly verifiable data for personal identification, and, on demand. With the help of such digital identity framework, trust is established remotely between the information seeker and the information provider, thus making the information exchange very secure.

In short, identification and authentication are seen as the drivers for business growth. Global business is expected to become ever more complex, and a robust identity trust infrastructure that enables the authentication of counterparties identities is imperative. This should be extended to support global interoperability. Proper digital authentication will allow companies to trawl safely throughout the entirety of cyberspace to optimise their dealings, whether they are issuing requests for proposals, buying raw materials or selling into a new region (EIU, 2007).

CONCLUSION

We are living in an integrated world economy. Emerging markets play a major role in information dissemination and interactions with people who may geographically be resident outside their countries' borders. Security in the information dissemination goes beyond securing the networks from external threats. Information security is achieved mainly by managing trust between the different stakeholders.

Governments have begun to realize that in modern days, our digital identity is perhaps becoming just as important as our physical one. This article attempted to outline that in order to enhance the benefits of digital economy, countries will require maintaining a secure environment for transactions, in which consumers have trust. The article argued that trust management is achieved by the development of a government based digital identity management infrastructure, and that two major technologies; PKI technology and biometric technology are likely to play a vital role in such developments.

Such national government infrastructure should support the growth of country's digital economy into the future in terms of jobs and employment, health, education, the environment, social inclusion and recreation. We cannot much emphasise that pursing digital economy has the potential to boost country's productivity, global competitiveness and social well-being. It provides opportunities to improve access to services and once again form better economic, education, health, social and environmental outcomes.

REFERENCES:

[1] ACMA (2010) Tecnology developments in the digital economy, 2010, Australian Government, Australian Communications and Media Authority.

[2] Al-Khouri, A.M. (2011) "An Innovative Approach for e-Government Transformation", International Journal of Managing Value and Supply Chains, Vol. 2, No. 1, pp. 22-43.

[3] Al-Khouri, A.M. (2011) "PKI in Government Identity Management Systems", International Journal of Network Security & Its Applications, Vol.3, No.3, pp. 69-96.

[4] Annunzio, S. (2007) eLeadership: Proven Techniques For Creating An Environment Of Speed And Flexibility In The Digital Economy. Free Press.

[5] Bertino, E. and Takahashi, K. (2010) Identity Management: Concepts, Technologies, and Systems. Artech House Publishers.

[6] Brancik, K. (2007) Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks. Auerbach Publications.

[7] Buiter, W, Rahbari, E (2011), Global Growth Generators: Moving Beyond 'Emerging Markets' and BRICS, Citi, Global Economics View, 21 February, NYC.

[8] Chandra, A. & Khanijo, M. K. (Eds). (2009) The Knowledge Economy. SAGE Publications.

[9] Chappell, D. (2007) Digital Identity for .NET Applications: A Technology Overview, Chappell & Associates [Online]. Available from: http://msdn.microsoft.com/en-us/library/bb882216.aspx

[10] Contos, B. (2006) Enemy at the Water Cooler: True Stories of Insider Threats and Enterprise Security Management Countermeasures. Syngress.

[11] Cruz-Cunha, M.M. and VarajÃ£o, J. (Eds) (2010) E-Business Issues, Challenges and Opportunities for SMEs: Driving Competitiveness. IGI Global.

[12] EIU (2007) Digital identity authentication in e-commerce. The Economist Intelligence Unit. [Online]. Available from:

[13] EIU (2010) Digital economy rankings 2010: Beyond e-readiness. Economist Intelligence Unit.

[14] G. Cybenko, A. Giani, and P. Thompson, "Cognitive Hacking and the Value of Information" Workshop on Economics and Information Security, May 16-17, 2002, Berkeley, California.

[15] Gates, B. (2000) Shaping the Internet Age.

[16] http://www.microsoft.com/presspass/exec/billg/writing/shapingtheinternet.mspx

[17] Holmes, F. (2010)The Six Key Drivers of Emerging Markets [Online]. Available from: http://dailyreckoning.com/the-six-key-drivers-of-emerging-markets/

[18] Kelly, K. (2011) What Technology Wants. Penguin.

[19] Kondratiev, N. D. 1925. The Major Economic Cycles (in Russian). Moscow. Translated and published as The Long Wave Cycle by Richardson & Snyder, New York, 1984.

[20] Laudon, K.C. and Laudon, J.P. (2008) Management Information Systems Managing the Digital Firm (10th Economy Edition). Prentice-Hall.

[21] McNally, M. (2011) Identity Theft in Today's World. Praeger.

[22] Mesenbourg, T.L. (2000) Measuring the Digital Economy, U.S. Bureau of Census, mimeo <http://www.census.gov/eos/www/papers/umdigital.pdf>.

[23] Meulen, N.S. (2011) Financial Identity Theft: Context, Challenges and Countermeasures. T.M.C. Asser Press.

[24] Neef, D. (1997) The Knowledge Economy. Butterworth-Heinemann.

[25] Negroponte, N. (1996) Being Digital. New York: Vintage Books.

[26] Perez, C. (2002) Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages. Edward Elgar Pub.

[27] Probst, C.W., Hunker, J., Gollmann, D. and Bishop, M. (2010) Insider Threats in Cyber Security in Probst, C. W., Hunker, J., Gollmann, D. and Bishop, M. (Eds.), Insider Threats in Cybersecurity. Springer.

[28] Schumpeter JA (1942) Capitalism, Socialism, and Democracy, Harper & Brothers, New York, London.

[29] Shaw, M.J. (2006) E-Commerce and the Digital Economy (Advances in Management Information Systems). M E Sharpe Inc.

[30] Stickley, J. (2008) The Truth About Identity Theft. FT Press.

[31] Tapscott, D. (1997) The Digital Economy: Promise and Peril In The Age of Networked Intelligence. McGraw-Hill.

[32] Tapscott, D. (1998) Blueprint to the Digital Economy: Creating Wealth in the Era of E-Business. McGraw-Hill Companies.

[33] Thompson, P. (2003) "Cognitive Hacking and Digital Government: Digital Identity", presented at the International Conference on Polictics and Information Systems: Technologies and Applications in Orlando, Florida, on 2 August 2003.

[34] Turban, E., Leidner, D., McLean, E., Wetherbe, J. (2007) Information Technology for Management: Transforming Organizations in the Digital Economy. Wiley.

[35] Westland, D. & Al-Khouri, A.M. (2010) "Supporting e-Government Progress in the United Arab Emirates", Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

[36] Williamson, G., Yip, D., Sharoni, I. and Spaulding, K. (2009)Identity Management: A Primer. Mc Press.

[37] Wilson, D. and Purushothaman, R. (2003). Dreaming with BRICs: The path to 2050. Goldman Sachs Global Economics Paper No. 99.

[38] Xu, J. and Quaddus, M. (2010) E-business in the 21st Century: Realities, Challenges and Outlook (Intelligent Information Systems). World Scientific Publishing Company.

Biometrics Technology and the New Economy:

A Review of the Field and the Case of the United Arab Emirates [3]

DR. ALI M. AL-KHOURI

ABSTRACT: Over the past decade, biometrics technology has evolved from a technology used primarily in forensics and a narrow scientific and technological field to an indispensable technology in public and private sectors expanding its roots in areas calling for advanced security. Biometric technologies provide high levels of security and reliability to address requirements related to identification and verification of personal identities. In light of the ever increasing requirements for robust identity management, biometrics industry is evolving to play a central role in shaping the future economy.

This article provides a comprehensive overview of biometrics technologies, its functions, and areas of application, related international standards, and recent advances in the field. The second part of the article looks at the application of biometrics in the government sector

[3] Al-Khouri, A.M. (2012) " Biometrics Technology and the New Economy: A Review of the Field and the Case of the United Arab Emirates", International Journal of Innovation in the Digital Economy, Vol. 2, No. 4.

worldwide, and the emerging pivotal role of biometrics in consolidating the foundations of the digital economies.
It also sheds light on the experiences of the United Arab Emirates in deploying different advanced biometrics technologies in a wide range of applications. It also outlines the government plans to develop an identity management infrastructure to address multiple strategic objectives, some of which are related to revolutionising public services and supporting the development of the digital economy.

Key words: *Biometrics, identity management, digital economy, digital society.*

1. INTRODUCTION: BIOMETRICS HISTORY AND CURRENT STATE

HUMAN race has always been beset with the need for highly secure identification and personal verification methods, arising from various reasons spanning social, economic, commercial and legal considerations. Identification is a process through which one ascertains the identity of another person or entity. It has always been recognized that every human being has unique traits that can define his or her identity.

Recognition started from the faces that are as unique as they may appear. However, larger populations, advances in surgical alterations and modern citizen centric service models have necessitated varying methods of recognition and unique identification.

Derived from the Greek words: Bios (Life) and Metron (Measurement), biometrics represents the science of identity recognition. Biometrics as a science and an automated means of identification may only be a few decades old, but as a concept, it has been in existence for thousands of years (See Figure 1, and Table 1). Today, biometrics identification is recognized worldwide as a definitive personal identification method with specific metrics that gives both the service provider and the end user the assurance of a rapid, secure, and convenient transaction.

Clearly, personal identification has become a key requirement for today's increasingly digitised global economy. Indeed, trust in electronic transactions is essential to the vigorous growth of the global economy. Although markets shrink and expand in cyclical fashion, emerging nations continue to present emerging new markets with endless opportunities. However, globalisation is generally raising the level and intensity of competition to deliver better, faster, cheaper services and products in a secure and trusted environment. Businesses find themselves in need for modern identification solutions ever than before to establish such trust basis, i.e., for denial and accordance, and for acceptance and refusal.

Businesses and governments alike in the past decade have therefore paid high attention to protecting their infrastructures from impersonating and/or infiltrating activities; a crime that was reported to cost 35 billion dollars in the United States alone in 2011 (Vamosi et al., 2011). With such justified attention to identification requirements, methods of identification assumed greater prominence.

In addition, as e-government and e-commerce initiatives proliferate, offering more online electronic services, robust identification and authentication methods are needed to address control and security requirements. The existing literature referred widely to the fact that one of the main challenging issues facing e-government and electronic society's development is identity management and the issue of trust in online transactions and digital identities. Ultimately the digital identity needs to become the same as real-world human identity. Using biometric identifiers for identity management provide strong credentials and higher levels of identity assurance.

According to a recent research report by RNCOS E-Services, the global biometric market is anticipated to grow at a CAGR of around 22% between 2011 and 2013 (RNCOS, 2011). At a regional level, North America was reported to dominate the global biometric market share of over 30% in 2010. The Asian, Middle East and Africa region were expected to emerge as growing markets for biometrics by 2013.

The report has also indicated that the government sector accounts for the major share of the biometrics market whereas the healthcare and financial sectors emerging as the potential adopters of biometrics systems. Many banks in developing countries (specifically Asian nations, including India, China, Malaysia, etc.) have adopted biometrics to address identity fraud issues and to offer customers an easy and more convenient authentication alternative to cards and PINs for transactions like ATM withdrawals.
Once again, biometrics is seen to be a critical enabler for the new digital economy. Only by understanding its potentials, how it works, and building on the experiences gained from international implementations, we can expect to make significant progress in creating successful future for our societies. As such, this article is written in this scope of dialogue.

This article is structured as follows. The first section provides a general overview of biometrics, including its characteristics, applications fields, related international standards, and recent advances that are shaping the biometrics industry. The second section looks at how biometrics technologies are adopted in the government sector, and its emerging role in addressing identity management requirements and forming the basis for the new digital economy.

The third section then looks at some biometrics initiatives implemented in the United Arab Emirates over the past decade to address needs related to critical infrastructure systems development. Finally, the fourth section presents an overview of one of the recent multi-billion dollar programs implemented to develop an identity management infrastructure to act as a single source for personal identity provision in the country.

1.1 Biometric Characteristics

Biometric characteristics are divided into two broad categories; physiological and behavioural. Physiological characteristics are the ones that are closely linked to the human body. Iris, retina, facial features, fingerprint, palm print and DNA are physiological characteristics of the human body; offering positive identification that is difficult to counterfeit. Voice, speech, signatures, handwriting, key stroke sequences are characteristics used for behavioural pattern studies.

In order to recognize a person by his or her biometric characteristics and derived biometric features, an enrolment process must take place. The process entails the construction of a data record of the enrolled person and to store it in a biometric enrolment database. The enrolment data record may comprise one or multiple biometric references and arbitrary non-biometric data e.g., name, and personal information, etc. See also Figure 2.

The recognition process is initiated when the person to be recognised presents his or her biometric characteristic to the biometric capture device. The device generates a recognition biometric sample with biometric features which are compared with one or multiple biometric templates from the biometric enrolment database. This should result in acceptance or rejection of the recognition request.

The most common capturing process in biometrics today is optical. In most cases miniaturised CCD cameras are used, which capture either visible or infrared light (Brüderlin, 2001). Recent methods, particularly in fingerprint capturing, try to get away from the optical capture to use temperature, pressure and/or capacitance (ibid). The primary performance evaluation measures in biometric systems are depicted in Table 2.

However, the accuracy of these measurements varies, which has a direct relevance on the levels of security they offer (Shoniregun and Crosier, 2008). The error rates of biometrics systems are tuneable, which allows it to be configured according to the business objectives.

The error rates in biometrics cannot be entirely tuned down, however reducing one error rate will increase the other. A balance between risk (i.e. false accept) and operability (i.e. false reject) must be found which matches the business objectives best. As depicted in Figure 3, for most biometrics, a template comparison results in a score represented by the "Hamming Distance", which is the percentage of bits of two compared biometric templates that are different. If this percentage is lower than a set threshold, a match decision is made and vice versa.

In this example above the threshold is set to 0.41 which means, that the system recognises a presented biometric as an authentic when no more than 41% of the previous captured bits during the enrolment process are different from the captured bits at verification time. An authentic with more than 41% different bits is called a false non match, an impostor with less than 41% different bits is called a false match.

The diagram (Figure 3) shows how the configurable threshold determines the balance between false match and false non-match rates. The probability for a false match or a false non-match equals the area under the curve on either side of the threshold. By changing the threshold, one area reduces while the other increases, hence determining the balance.

Current technologies have evolved over the past five decades to higher mature levels due to the developments in the semi-conductor technology coupled with computing power. However, the foremost impediments of biometrics rotate around the complexity and privacy issues surrounding information abuse.

Biometric information abuse has caused some civil libertarians to be incensed by the risks posed by the personal nature of biometric information and how this information can be manipulated or misused. Conversely, the evolution of the biometrics to the current state in the world is best understood in the context of the applications of the biometrics. The next section looks at some different uses of biometrics which also explain the concept of identification and authentication.

1.2 Purpose of Biometrics

Personal identification numbers; often referred to as PIN numbers, were one of the earliest identifiers to offer automated recognition. PIN is a secret numeric password shared between a user and a system that can be used to authenticate the user. Despite its wide application, PIN-based authentication methods do not provide recognition of the person performing the transaction. Biometrics however represent unique identifiers and unlike PINs, it cannot be easily transferred between individuals. Most of current biometric applications are related to security and are used extensively in government sector.

The wide applications of biometrics in public domain are being motivated because of its advanced capabilities of (1) identification, (2) verification, (3) authentication and (4) recognition. In practice, it is noted that many in the field often do not understand the difference between the functions of these capabilities. Table 3 provides definition of each.

In the context of the above capabilities, biometrics has come a long way. From the 1858 hand print cataloguing of the Indian employees for pay day by Sir William Herschel; to the 1903 fingerprinting of criminals in New York State Prison; to the Visit

Program of the United States; to the World's largest biometric database in India for social benefit delivery, biometric are coming of age.

In the past decade, the industry has seen remarkable developments in the field of storage methods and enrolment and verification procedures. Physical fingerprints taken by fingers dipped in indelible ink have given way to electronic sensors that capture the fingerprint image. Photographs that provide facial recognition have given way to face analysis system capturing internal skull geometry and skin texture sensing.

Eye colour/ retina recognition has evolved into iris recognition that cannot be tampered with. Electronic Sensors have been developed to accurately capture the different biometric characteristics so that they can be stored as electronically recognizable templates. Table 4 provides a list of evolving biometrics technologies that are gaining varying acceptance levels in various industry segments.

In the light of rapid speed of technological advancements of biometrics, the industry has witnessed accelerated standardization efforts to support inter-changeability and interoperability of different systems. The next section provides a short overview of existing biometric standards that were developed to facilitate biometric systems interoperability, and enhance the effectiveness of biometrics products and processes.

1.3 Biometric Standards Evolution

Technically speaking, standards have been developed so that the electronic templates are generated, stored and retrieved in a uniformed way. The main impetus of biometrics standards is to define requirements, formats and software specification enabling interoperability between biometric systems, especially authentication systems. Biometric standards enable different streams of interoperability. One stream of standards enables interoperability of data collections and storage processes. The other steam enables interoperability of signal processing and matching technologies.

Evolution of standards signifies maturity of the technology, and standardization is envisaged to enable wide governmental adoption of biometrics. It provides a level playing field for device vendors and exchanging information at the national and international levels. This is to say that standards reduces risk to the integrator and the end user alike, primarily because it simplifies integration, and allows for substitution and upgrade of technologies, and reduces "vendor lock-in" effects (Tilton, 2006). This is likely to lead to a broader range and availability of products and movement towards commoditization (ibid).

There is still a long way to go for the standards that are developed to be uniformly adopted across the world. Biometrics standards have been developed by informal and formal standards organizations. In general, the following organizations are actively involved in the development of the standards and their adoption:

- International Committee for Information Technology Standards (INCITS) M1
- National Institute of Standards and Technology (NIST)
- Joint Technical Committee 1 (JTC 1)/Subcommittee 37 (SC 37)
- Organization for the Advancement of Structured Information Standards (OASIS)
- International Standards Organization (ISO)

The standards developed by these organizations provide a good indication to the current state of the biometric technologies. Currently, there exists a great maturity and consensus and definitive standards documents that have been released. They include, but are not limited to: Technical Interfaces, Data Interchange Formats, Application Profile Standards and Performance Testing.[4] These are briefly discussed next.

1.3.1 Technical Interfaces

These standards are related to the data capture of biometrics interfaces and interactions between biometric components and subsystems along with security mechanisms to protect stored data and data transferred between systems. They also include specifications of architecture and operation of biometric systems for supporting multi-vendor systems and their applications. ANSI INCITS 358-2002 BioAPI Specification v1.1, ANSI INCITS 398-2005

[4] Refer to pg 138 Biometrics "Foundation Documents" & the document "Biometric Standards" published by NSTC Sub Committee on Biometrics for Bio-Standards.

[NISTIR 6529-A] Common Biometric Exchange File Format (CBEFF) are examples of Technical Interface Standards.

1.3.2 Data Interchange Formats

These standards specify the content, meaning, and representation of formats for the interchange of biometric data, e.g., Finger Pattern Based Interchange Format, Finger Minutiae Format for Data Interchange, Face Recognition Format for Data Interchange, Iris Interchange Format, Finger Image Based Interchange Format, Signature/Sign Image Based Interchange Format, and Hand Geometry Interchange Format; and specify notation and transfer formats that provide platform independence and separation of transfer syntax from content definition. Examples include ANSI INCITS 377-2004 Finger Pattern Based Interchange Format, ANSI INCITS 378-2004 Finger Minutiae Format for Data Interchange, and ANSI INCITS 379-2004 Iris Image Interchange Format.

1.3.3 Application Profile Standards

These standards specify one or more base standards and standardized profiles, and where applicable, the identification of chosen classes, conforming subsets, options, and parameters of those base standards or standardized profiles necessary to accomplish a particular function. Some of these standards are: ANSI INCITS 383-2003 Biometrics-Based Verification and Identification of Transportation workers and ANSI INCITS 394-2004 Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management.

1.3.4 Performance Testing and Reporting

These set of standards specify biometric performance metric definitions and calculations, approaches to test performance, and requirements for reporting the results of these tests. Examples include ANSI INCITS 409.1-2005 Biometric Performance Testing and Reporting Part 1 - Principles Framework; ANSI INCITS 409.2-2005 Biometric Performance Testing a Reporting Part 2 - Technology Testing Methodology; and ANSI INCITS 409.3-2005 Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies.

These standards among others establish the maturity of biometrics as a technology for personal identification. However, it is to be noted here that there is no one biometric characteristic that can be considered as a bullet proof solution. Usage of the biometrics characteristics depends entirely on the application.

Applications of biometrics are dictated by the circumstances, available data, security and risk assessment, number of people to be covered and so on. For example, in the US with a huge database of fingerprints of criminals, crime detection is relatively easier for Crime Scene Investigators to pick the fingerprints from the crime scene and match them with known prints.

With the new visitor biometric data (fingerprint, facial features) being collected, the USA, UK and other European countries are seeking to secure their borders from unauthorized entrants. The Indian project which is billed as the world's largest biometric exercise seeks to collect the fingerprints of its 1.3 billion populations with the aim of ensuring transparent social benefit delivery to authorized individuals.

Fingerprint technology has wider acceptability worldwide due to its relatively lower implementation costs in comparison with other biometrics, and the availability of wider range of commercial applications in the industry. Nevertheless, the fingerprint as a biometric characteristic is not fraught without issues. For instance, any damage to the fingers renders the existing fingerprints useless. Further, it is very difficult to scan fingerprints and build templates for rough fingers or with cuts and damages.

These kinds of issues necessitate newer biometric technologies, newer sensors for detection and better computing algorithms for improvement of quality in enrolment and detection. The next section attempts to provide a highly level overview of developments in the biometric industry.

1.4 Advances in Biometrics

Recent advances in technologies and computing have enabled biometrics to evolve into a definitive and legally accepted means of personal identification. From the days of cataloguing fingerprints and establishing a match manually, computing techniques today have transformed biometrics.

Driven by the need to have more authentic characteristics for determining the identity, some biometric technologies are noticeably enhanced in the past decade. Multi-modal facial biometric with 3D face recognition is one of the techniques that have moved from laboratories to the commercial domain for mass production.

On the other hand, in the last half a decade, iris as a definitive biometric has advanced immensely. Iris is now a common biometric used to control borders in many countries in the world. Complemented by 3D facial recognition, the issue of live sensing of iris has been overcome to a large extent.

However, it is still not completely reliable in unsupervised applications. In supervised environments, iris recognition proffers excellent results. One of the well-known deployments of iris is UAE where iris detection is in place for monitoring all the visitors. This deployment is one the biggest and early success stories of iris technology in the world (Al-Raisi and Al-Khouri, 2006). See also Section 3 in this article.

Fingerprinting technologies now uses all ten fingers including the palm. As fingerprint databases growing bigger, it is no longer considered definitive with one or two fingers. The latest in hand geometry is Palm Vein recognition. Currently Fujitsu holds the patent for Palm vein recognition and scanners, detectors, and readers are commercially available using this technology.

The palm vein scanner works by capturing the images of vein patterns that are inside the body in a contactless manner, which makes it more sterile and hygienic to use. See also Figure 4. This makes palm vein patterns difficult to forge, and thus more secure. Palm vein recognition technology also has one of the lowest false acceptance rates (FAR) and false rejection rates (FRR) i.e. false rejection rate of 0.01% and a false acceptance rate of less than 0.00008% (Sarkar et al., 2010).

Palm Vein Recognition is expected to be the major determinant in biometrics and to overcome many drawbacks that current fingerprints carry. This is the technology that promises a good touch of excitement in the days to come.

Besides technology, the major advancements have been in the domain of computing. The ability to deploy large relational databases with fast search engines has resulted in faster detection and identification times. Identification of a person has become easier and faster with the ability of 1:n matches in huge databases.
This has helped the law enforcement agencies big time. Computing and network technology has helped data exchange and information sharing easier and faster. This has resulted in better intelligence sharing among nations. There are numerous initiatives worldwide in ensuring standards in communication and protocols for data exchange. These standards have made interoperability of diverse systems easier and more efficient.

Last, but not the least is the progress made in the quality domain. Quality standards have been put in place for the capture of biometric templates. NIST (National Institute of Standards & Technology) launched the NFIQ (NIST Fingerprint Image Quality) in 2004 and sought to standardize the algorithm for fingerprint minutiae matching. ISO has been active through its Sub Committee SC 37 in defining various standards for biometrics including data exchange, BioAPIs, fingerprint data formats and storage.

Currently many more standards are under development under the SC 37- for example: Conformance testing methodologies (eg ISO/IEC 19794-9/PDAM 1); Procedures for the operation of the Biometric Registration Authority- ISO/IEC DIS 19785-2, to cite a few.[5] Two other organizations actively involved in the standards development for biometrics are the INCITS (International Committee on Information Technology Standards) M1, and OASIS (Organization for the Advancement of Structure Information Standards).

These standards and the evolution of quality in biometrics promise major advances in biometric sensing technology. Better sensors provide higher sensitivity, better resolution and higher repeatability. This contributes to lower False Rejection Rate (FRR) figures, lower False Acceptance Rate (FAR) and better Cross-over Error Rates (CER).

Over the past few years, advancements in sensing technologies have enabled higher speed and throughput rates. Higher throughput rates meant larger number of enrolment capacity and processing. Such advancements have paved the way for many

[5] Refer to ISO Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770

governments to initiate mass enrolment programs at a national level to capture the biometrics of their population.

2. GOVERNMENT BIOMETRIC PROGRAMMES: Enabling initiatives of the new economy

Identity management has always been a key challenge for governments across the globe. Governments have striven to provide its citizens security and protection, ease of access across its national borders, and ensure that social benefits reach the rightful and deserving citizens. Governments in this day and age seek proven methods to establish the identities of their population in order to provide secure access to government applications and services. Table 5 summarizes a generic model used for identity requirements for benefit delivery and privilege accordance.

In the past, services or benefits delivered across different channels had to be severely limited owing to lack of credible verification of identity of the beneficiaries. Citizens had to necessarily walk into government offices that demanded different identification checks to verify the identity of a benefit claimant. Needless to say governments relied heavily on biographical information to manage the identity of their citizens. Passports, although considered as travel documents, were considered as a primary identity document in many countries around the world.

Many countries have made attempts to provide simpler identification methods in terms of paper based identity cards carrying the photograph of the person. These identity documents served a limited purpose since the identity largely depended on the photograph and it was easy to reproduce or fake such documents. Paper ID cards were then replaced by plastic cards. Plastic cards with embossing, watermarks, holograms were adopted to reduce the risk of fake cards. All of these approaches met with limited success due to the limitations of usage and applications of different business needs.

Governments around the world implemented copious identity management programs in the last 10 years that addressed discrete strategic needs. One of the early and major applications was in border security domain. Border security systems differ between countries, however, in general, all visitors and residents are normally needed to apply for a visa or a visa equivalent, with conditions appropriate to their stay. This visa is verified at the border and passes through a number of checking layers, many unknown to the traveller, and if found genuine and authentic, the person carrying the visa is allowed into the country.

Visas are produced in the form of a paper and attached to passports. Paper visas are fraught with issues. This is a major concern for the border security. The need for more effective management of national borders and identity fraud has brought about an increased demand for secure end-to-end identity systems.

Biometric technologies have emerged as critical components of identity and security programs. With the kind of reliability and acceptance that fingerprints, facial recognition and iris recognition have gained in the last decade, complemented by the advances in computing techniques, biometrics is being increasingly used internationally as a high-technology identity management tool to strengthen identification processes. See also Figure 5.

Evidently, there have been and continue to be numerous attempts by countries to enumerate their citizens, enlist them, register them and more importantly identify them. Table 6 provides a global overview of biometrics applications by governments worldwide.
The USA, India, UAE, Malaysia, South Korea, UK, France have been mentioned before that have taken a lead in biometric implementation. USA, UAE and UK are early adopters and leading examples of biometric implementations for Border Security. Entry of visitors to these countries is mandated by fingerprints to be collected at the time of granting of approval to visit the country (Visa Issuance). Fingerprints are verified at the time of actual entry and if found matching, entry is granted.

2.1 Emerging roles of governments

The globalisation and the rapid pace of development in information and communication technologies are redefining the nature of governments and their relationship with citizens (Guthrie, 2003). With such developments, public services are challenged to re-invent the government in the digital economy.

This necessitates re-thinking the way governments have been dealing with citizens and business, re-engineering their work processes and as well as enabling greater cross-agency collaboration to deliver services in a way which the public appreciates (ibid). As such, identity management is a critical success factor to enable such transformation. Robust identity management infrastructure is envisaged to enable digital economy, with identification and authentication systems that people can live with, trust and use (Stevens et al., 2010).

There is accumulating evidence that governments are sources of powerful forces influencing the development of new industries (Ke and Wang, 2008). Yet, governments, as a valid and powerful context have the potential to influence the digital economy creation (ibid). Existing literature argue that there is enough indication that due to network externality effects, governments need to take an active role in stimulating an e-environment to jump-start the move toward a higher level of e-readiness.

De Meyer and Loh (2004) allege that governments can play an important role in at least four areas: (1) stimulating the enhancement of the infrastructure that enable e-society; (2) investing in improved services (e-government); (3) stimulating an e-friendly business environment; and (4) creating an all-inclusive information society. He further elaborates that for an e-environment to exist, a basic ICT infrastructure need to be put in place in order to reach out to citizens and to provide a robust network over which business can operate.

The literature in general, widely disagrees with the concept of dependence on the private sector to build such infrastructure all alone, and believe that if it did, it will produce inept and hurdled efforts that will be insufficient to gain social acceptance and trust (Al-Khouri & Bal, 2007; Al-Khouri, 2010; De Meyer and Loh, 2004).

Apparently, biometrics offer tremendous opportunities to create new value, and to provide instant knowledge and processing capability to make quantum leaps in identity management and service delivery (Guthrie, 2003). Governments are therefore assuming new roles to build trust in online identities in order to improve electronic delivery of government and business services. This confidence is seen to encourage innovation in the online marketplace and foster the growth of the new digital economy.

Networks are a key component of this new society, as illustrated by the rise of mobile phones, email, and social networking websites, yet the networks in the digital world are constantly changing (IMA, 2011). Governments have for long been responsible to develop methods for physical identification of identities. In today's world, governments[6] are recognizing that their boundaries of responsibilities need to expand and include virtual and digital networks revolutionise and/or create new business and social paradigms.

- 6 President Obama's technology-based American presidential campaign changed the face of US elections and he has made it clear that he sees both technology and a strong communications infrastructure as vital to economic recovery and growth. This includes a radical approach to the deployment of a modern communications infrastructure, including redefining universal service to extend its scope to broadband and unleashing the power of the wireless radio spectrum.
- The French Government has recently launched its France Numerique 2012 plan, an ambitious communications sector strategy designed to strengthen France's digital position and enhance its broader competitiveness at a time of global economic slowdown and crisis. The message laid out in the plan is clear: the digital economy is the most dynamic sector in the world and as the global recession bites, it is essential to nurture those parts of the economy that can generate growth potential and jobs.

> "Modeling the digital world is not like modeling the physical world, where established equations govern the movement of atoms or the flow of electrons. Interactions between people and information are more complicated, and we need to develop new concepts and models to understand and predict their behaviour in the new digital society."
>
> **The insitute of mathamtics and its application, UK.**

Biometrics provides a stupendous opportunity to create a new understanding of digital interactions. Many governments in the world have invested intensely in the last decade to develop identity management solutions for identification and authentication of physical and virtual identities. These solutions are based on the traditionally accepted means of identification and authentication of one or more of three general principles: (1) what the person knows (some form of shared secret like passwords), what he possesses (some kind of unique token or key e.g., smart card), or what he is (some aspect of his physical being i.e., biometrics).

The application of Public Key Infrastructure technology with its digital signature capability coupled with biometric identifiers have the potential to provide a strong authentication and non-repudiation assurances in digital networks. Digital signatures identify and authenticate the originator of the information. They allow the receiver to ascertain the identity of the sender and to determine whether the message changed during transit (Uhlfelder, 2000). In addition, they permit verification that the information has remained unchanged after the sender signed the message and allow a user to securely identify himself or herself on the network (ibid).

The use of digital signatures and biometric identifiers when implemented together may complement each other, with the strengths of each technology offsetting potential weaknesses in the other (Jueneman and Robertson, 1998). Having said this, the next section provides an overview of recent deployments of biometrics technologies in the United Arab Emirates to address different national strategic needs.

3. UAE INITIATIVES IN BIOMETRIC IDENTIFICATION

UAE is a pioneer in its biometric implementation. It has integrated multiple biometric technologies in critical infrastructure systems in the last decade. Following are few examples of recent projects in the field of biometrics implementation.

3.1 Iris recognition

At the country’s entry points, all visitors are required to undergo an iris scan. Via secure national network infrastructure, each of the daily estimated 20,000 travellers entering the country goes through iris screening; where each presented passenger's iris is compared exhaustively against all templates in the 2.3 million watch-list database.

The UAE began the implementation of iris recognition technology at its borders in 2001 to inhibit illegal entry of persons in the country.

The UAE was the first in the world to introduce such a large scale deployment of this technology. Today, all of the UAE's land, air and sea ports of entry are equipped with iris systems.

UAE iris watch-list database is currently the largest in the world, both in terms of number of iris records enrolled (more than 2.3 million people) and number of iris comparisons performed daily i.e., more than 15 billion cross comparisons in an exhaustive (1:n) comparison. More than 320,000 deported people had been caught at airports trying to re-enter the country after being deported using new passports with sometimes different biographical information.

3.2 Facial Recognition

Facial recognition (facial on the move) has been implemented recently at UAE airports in 2008 to enhance security procedures and detect persons who might pose a threat to the country. The system allows critical identification checks to be performed from a distance without a person's active participation. The system helps inspectors at control points inside the airports to implement continuous and proactive checks designed to immediately detect persons who should be denied entry or detained.

The system can identify persons live or from photographs. It can identify persons while they are moving with a high degree of accuracy. The system which is still at a trial phase is expected to be rolled at all points of entry in the country in the coming 2 to 3 years.

3.3 Fingerprint based - Electronic Gates

UAE has another biometric application working at its airports; namely biometric based electronic gates (e-gate). The e-gate facility which was first introduced in 2002 in Dubai International Airport, is the first airport in the region and the third in the world offering this service to travellers. The service is basically available for quick passage through passport control.

The electronic gate uses fingerprint biometrics to automatically process all registered passengers arriving and leaving from any of the UAE airports. This is an advanced passenger clearance system that considerably accelerates the movement of traffic through electronic screening of passengers' data with the help of a smart card. It was estimated that more than 4 million travellers used electronic gates in 2010. The government is working on a plan to encourage the usage of electronic gates and to make it almost compulsory for travelling adults without children companions.

3.4 Electronic Passport

The UAE government is in the process of launching its new electronic passport in the coming six months (also referred to as a biometric passport). The new passport contains biometric information mainly fingerprints and ICAO standard photograph, that will be used to authenticate the identity of travellers. The information on the chips can be scanned and verified at airports, other ports and border posts.

PKI technology is used to sign the electronic data stored in the passport microprocessor chip. This is expected to enhance the current security features of passports and provide greater protection against tampering and reduce the risk of identity fraud. The issuance process is linked with the expiry of the existing passports as it will be replaced with the electronic ones. The biographical and fingerprint data are pulled electronically from the national identity register, detailed below.

3.5 National Identity Register

Another ambitious and large scale biometric program was launched in 2003. The program aims to set up a national identity register and to enrol an estimated 9 million population in the country. This program, which is also referred to by the UAE government as the national identity management infrastructure, aims to serve multiple strategic objectives. The primary objective was to set up a government entity that has an imperative role as the single source for personal identity provision in the Country.

Through a comprehensive data bank, the government seeks to help conserve billions of government investments in the duplication of data by different government agencies. The advanced identification mechanisms offered by this program are envisaged to provide a highly credible identity base to revolutionise public services and support digital economy creation. Section four further elaborates on this project and discussed its key components and objectives.

3.6 Federal DNA Project

The government has begun a DNA identification database development in 2010. The project which is still in its pilot phase, targets to collect DNA samples of 10 million people both national citizens and foreign residents in the next few years. The federal DNA database is primarily seen to contribute to areas related to crime detection and identification of criminals.

The field of biometrics overall in the United Arab Emirates is gaining prominence and the government seems to be convinced of the potentials of these technologies to provide a stronger authentication and reduce the risk of identity fraud. It has invested substantially in biometrics solutions in the past few years as we have illustrated in the few examples above.

The market in the UAE has seen some trails of biometrics in public and private sectors however they were primarily limited to the field of physical access control. The application of the new UAE biometric identity card capabilities, to provide secure identification and personal verification solutions, is envisaged to improve public acceptance of the technology and vitalise electronic transactions, as the next section outlines.

4. THE NATIONAL IDENTITY REGISTER PROGRAM OF UAE

The UAE has a very interesting population demographics. Out of an estimated 8.2 million, only as little as 10% of its population are national citizens. The remaining 90% represents foreign resident population working on a maximum of 3 year work permits or as expats family companions. Nearly citizens of 180 countries across the globe are legal residents in the UAE. The strong economic growth in the country attracted such diverse workers from all over the world, and is continuing to grow at a rapid rate. Figure 6 shows the changing patterns of population demographics in the UAE.

The UAE realised the need for a more sophisticated identity management system in light of the unique composition of its population. The UAE launched its national identity register program in 2003. The actual population enrolment started in mid 2005.

The program was lunched with the objective to build an identity management infrastructure that has a derivative role as the single point of authority for the provision of identity information in the country. This was envisaged to allow the government to better plan its development priorities. Clearly, the growth rate was a determining factor to address the changing needs of its people for infrastructure (e.g., schools, hospitals, housing, roads), resources (e.g., food, water, electricity), and jobs.

Another important objective was related to improving government service delivery, and to develop the infrastructure for the new digital economy. The program with its advanced technological components, intend to develop and provide digital identities to each citizen and resident in the country and in an attempt to revolutionise its e-government and e-commerce initiatives. The digital identity of a person is established through a combination of three critical components:

- National Identification Number
- A set of biometrics (photograph, fingerprints, - iris is being piloted)
- A Digital certificate consisting of Private and Public keys issued by a National PKI (Public Key Infrastructure).

All the attributes of the personal identity are packaged together and issued in a single instrument of identity; the UAE National Identity Card. Out of an estimated 8.2 million population, more than half have been enrolled in the scheme to date. The remaining population is expected to be enrolled by 2013.

The government follows a stringent enrolment processes compliant with international standards in acquiring the biometric data of the citizens. Registration centres are established all across the country serving the citizens and residents to enrol in the National Identity Register.

Mainly, fingerprints (rolled prints, palm prints, writer's palm prints) and facial recognition are captured biometrics. Following NFIQ compliant standards, the biometric data is processed and stored in the card along with the digital certificate. See also Figure 7. Iris recognition is expected to complement the current biometrics during renewals. The main reason for not including a third biometric was due to reasons related to not causing interruption to the enrolment process.

4.1 The UAE National ID Card Features

Adopting a slew of security features, and internationally recognized biometric standards and the latest computing techniques, UAE issues the most advanced smart cards to all its citizens and residents. Figure 8 depicts some of the physical security features in the card.

The microprocessor card which is Java based serves a dual purpose of micro computing as well as secure storage. Micro computing allows complex encryption algorithms to run efficiently and effectively on the card. This enables secure storage of data ensuring tamper proof identity data including biometric data.

The UAE was one of the early adopters of match-on-card feature. This feature enables fingerprint Match-on-Card user authentication as an alternative and to complement smart card PIN verification. This in turn gives access to the digital certificates on the card that can then be used for logon, digital signature, file encryption, secure VPN access among other services.

This solution provides a secure two or three factor authentication capability that is convenient for users, easy to deploy and manage, and fully compatible with the smart card security components available in Windows operating systems. It is also compatible, with the majority of fingerprint sensors available in the market.

The card is a hybrid smartcard that also contains PIN protected personal data including digital certificates, and the holder's biographical data and two best fingerprints. The card is envisaged to be the only acceptable identity document to access any government and some critical private sector services like the financial sector. The 144KB-combi card is a multi-application card and designed to be fully compliant with the two major industry standards:

- The Global Platform Card Specification Version 2.0.1', that defines the card management; and
- Visa Card Implementation Requirements Configuration 1-Compact" by virtue of the enhancement in the card by the additional security features described in the "Open Platform 2.0.1".

Both the Java Card Runtime Environment (JCRE) and the Global Platform (GP) standards contribute to the security features of the UAE National ID card. Java provides cryptographic mechanisms and enforces firewalls to protect applications and maintain data and operation security within the multi-application shared card space. The GP 2.0.1' specifications extend the Java Card cryptographic authentication mechanisms to ensure dynamic and secure loading/ updating of individual applications in the dynamic and multi-applet Java Card.

Three unique features are provided in the card that makes the UAE national identity card distinct in its application in the world. There are five applets in the UAE identity card: (1) ID and ePurse applet, (2) PKI applet, (3) Match on Card (MoC) applet, (4) eTravel Applet, and (5) MIFARE Applet. See also Figure 9. These applets do not share data inside the card and are completely secure.

Communication with the card can only be established using the SDK/Tool Kit distributed by the government.

The applets are self-contained in the card and run as applications on the card, without the stored data ever leaving the card. These features enable instant identification/recognition, validation of credentials, verification and most importantly provide assurance of the established identity. This is envisaged to greatly enhance the acceptability and reliability of the card in the country.

4.2 Functions of the UAE National ID Card

The main function that the UAE card serves is that of establishing irrefutable identification of the cardholder. Match on Card function provides instant verification of the biometric data of the cardholder. One of the key infrastructure technologies in the program is Public Key Infrastructure (PKI). The PKI provides the functionality of digital signature enabling transactions between individuals and organizations on the virtual space of internet.

The primary need stems from requirements related to develop secure (authentication) communication mechanism. The government seeks to support e-government and e-commerce initiatives through this card to act as an enabler of electronic transactions.

In addition to the core functions, the card is poised to be the singular identity system in the country by providing integration support for inter-agency identity requirements. The card has multiple data containers that would enable and facilitate e-government. Labour and Employment data, Road Authorities, Law Enforcement agencies, e-Gate/ e-Passport, e-Purse are some of the important data containers available in the card.

Different government departments can enable their specific identity metadata for the card holder in these containers. Table 7 provides an overview of the capabilities and functions of the UAE identity card.

4.3 UAE e-Government Initiative

A recent report by the business school INSEAD and the World Economic Forum showed that the UAE ranked first in the Middle East and North Africa (Mena), and 24th worldwide, in terms of information and communication technology (ICT) readiness (Dutta and Mia, 2011). The UAE government realised the need to adopt more effective approaches to promote in principle, the authentication of online identities, and to address the overall requirements of trust, identity management and privacy and in the context of electronic governance.

The UAE ID card, coupled with the Public Key Infrastructure technology, provides strong authentication capabilities to support online services. PKI technology provides key building blocks of digital identities, i.e., generation, management and validation of digital certificates, digital signatures, and electronic time-stamping.
The UAE government recently introduced its federated identity management solution (also referred to as the National Validation

Gateway) which is based on its new smart identity card and advanced PKI capabilities. The solution provides identity authentication services to service providers (e.g., e-government, banks, hospitals, commercial entities). It is implemented as a service over the cloud to provide different services as depicted in Table 8.

The solution is currently available to e-government authorities. There are eight e-government authorities in the country; one federal e-government authority and seven local authorities, one in each emirate. Currently there are 48 government services[7] that are integrated with this infrastructure.

The user basically needs to download an applet on his computer machine. Using the card reader, he needs to use his card to logon to the e-government portal. The method of authentication may vary depending on the service provides requirements. The portal may perform the authentication function in offline mode, or it may redirect the user to the national validation gateway. The feedback from the latter will determine the go or no-go authorisation (access control decision) to desired resources.

The UAE federal government is working on drafting a legal framework to legalise digital identities and digital signatures. The government is planning to make all G2C e-government electronic transactions take place only through its new smart ID card in the coming 3 to 5 years. The government is planning to drive digital

[7] http://www.abudhabi.ae One can register to access the portal and its services using the Emirates ID Card

economy growth throughout the country using its new biometrics-based identity infrastructure.

4.4 Role of Biometrics in ID Card in G2G, G2B, G2C

As the levels of worldwide information system security breaches and transaction fraud increase, the UAE government is moving aggressively towards e-government transformation, particularly to develop combined, seamless services, which are electronically delivered to its population or other public or private sector entities (Westland and Al-Khouri, 2010). This comes in line with its objective to improve the efficiency, quality and transparency of government services.

The government plans include the development of multiple self-service channels e.g., over regular internet, kiosks, IVR and wireless channels. Biometric authentication of personal identities is seen more convenient and considerably more accurate than current methods such as the utilization of passwords or PINs.

As mentioned earlier, the UAE card is enabled with a Match-on-Card application. This allows service providers like government agencies to verify the identity of the cardholder and deliver services with complete confidence on the identity of the person receiving the services. With so many secure and transactional features enabled in the card, the UAE national identity card is set to become the country's most valued card both in physical and electronic transactions.

Biometrics in general is envisaged by the UAE government to provide high levels of identity assurance for homeland security including applications for improving airport security, and strengthening the national borders, and in preventing identity theft. There is seen to be a growing awareness and interest in biometrics in the country and in the region overall, of its potential in more accurately identifying and verifying the identity of individuals and protecting national assets.

The government has recently released an enhanced version of the Software Development Tool Kit (SDK) to enable licensed organisations to integrate the new smart identity card and biometric applications into their systems and develop legally compliant electronic signature and biometric authentication systems.

The SDK tool kit provides a high level API (Application Programming Interface) which help application software development easily and quickly made and UI (User Interface) of wizard type so that it saves time and efforts to develop an application. It is operated on various platforms, supporting diverse operating systems and development languages (Al-Khouri, 2011).

With such efforts, the use and reach of biometrics in the UAE is expected to increase considerably in the few years to come. As more identification and verification systems will be implemented to address various industries requirements who will likely find it in their best interest both in terms of cost and necessity to safeguard their data and assets.

The government is planning to push its biometric-based ID card solutions in multiple domains of applications. It has launched recently several initiatives in cooperation with private sector organisations to encourage the development of an extensive array of highly secure identification and personal verification solutions by integrating its new identity card functions in public sector applications, e.g., (1) network access to control unauthorized access to computers and networks in government organizations, (2) financial industry to promote e-commerce and online transactions, and (3) healthcare industry to provide security at hospital premises and recognition of patients identities, (4) law enforcement and (5) immigration and airports.

4.5 Interoperability Framework

To further enhance transactions using the new smart identity card, the UAE government is actively working with different stakeholders in the country and in the region to define interoperability standards. A framework has been defined that determines the role of the new smart identity card and the biometric verification that would be needed for authenticating a stakeholder in any transaction.

Standards are being defined for data interchange and exchange that will allow government departments and different agencies to communicate securely. The ID card with its PKI features is central to such a communication. Federated Identity Management is being provided and is currently in its pilot stage, integrating access of different web services using the identity management system set up by the government.

Taking the interoperability to a new level, initiatives are being taken to setup a Gulf Interoperability Framework that will enable the UAE smart identity cards and other national ID cards in the GCC[8] countries to be used across the borders. There have been serious moves in the recent years to ensure that identity cards across GCC countries are technically compatible and interoperable. There are some recent developments of APIs relating to biometrics, digital qualified signatures and digital authentication, to enable e-business transaction across borders (Al-Khouri and Bechlaghem, 2011).

CONCLUSION

Biometric technologies that have long history of use in law enforcement applications are now transitioning with wider social acceptance towards both public sector and commercial applications. Utilized with other advanced technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives.

Only by learning more about these technologies and exploring its potentials, and drawing on the experiences of successful and failed programs, governments can develop robust and vibrant biometrics community. Such efforts are needed to build identification and

[8] GCC is the acronym for Gulf Cooperation Council, also referred to as the Cooperation Council for the Arab States of the Gulf (CCASG). It includes six countries namely, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. The number of GCC population is estimated to be around 40 million people (GCC Portal, 2011). GCC citizens can usually travel freely between member states without the need for visas, and can use either their passports or national identity cards for border crossings.

authentication systems that people can live with, trust and use, which should also enable the forming of the new digital economy. Successful pursuit of biometrics challenges will generate significant advances in capabilities designed to improve safety and security in future mission within national and homeland security, law enforcement, and personal information and business transactions. Interoperability will still be a major hurdle.

From one angle, interoperability across geographical borders and business sectors, across processes, devices and systems is beneficial to biometrics diffusion. However, and looking at it from another angle, national interests in maintaining control and vendor resistance (aspiring to future market dominance due to lock-in effects) are expected to challenge interoperability efforts, despite the significant standardisation work being done at national and international levels.

Although technical interoperability is receiving increasing attention to some extent, the interoperability of processes may be more challenging. These challenges will come to surface as attempts of innovate service delivery models start taking place to push biometrics applications away from the existing narrowed objectives and promote wider diffusion in our societies. As such, when systems become more interoperable, the need for building more robust identity management grows as well as to meet national and international needs.

Government and industries are likely to become more dependent than ever on more robust identity management tools and identity governance principles. Biometrics will play a key role in addressing the new challenges of the years to come.

BIBLIOGRAPHY

[1] Al-Khouri & Bal, J. (2007), "Electronic Government in GCC countries." in International Journal Of Social Sciences, 1(2), pp.83-98.

[2] Al-Khouri, A.M. (2011), "PKI in Governemt Identity management Systems." in International Journal of Network Security & Its Applications, 3(3), pp. 69-96.

[3] Al-Khouri, A.M. and Bechlaghem, M. (2011), "Towards federated e-Identity Management across GCC: A solution's Framework." in Global Journal of Strategies and Governance 4(I). pp. 1-20.

[4] Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002), "Biometric perils and patches." Pattern Recognition 35(12), pp. 2727-2738.

[5] Brüderlin, R. (2001),"What is Biometrics?" [Online]. Available from: http://www.teleconseil.ch/english/introduction.html. Accessed: August 12, 2011.

[6] Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005), "PalmHashing: a novel approach for cancelable biometrics." in Information Processing Letters, 93(1), pp. 1-5.

[7] De Meyer, A. and Loh, C. (2004), "Impact of ICT on government innovation policy: an international comparison", in International Journal of Internet and Enterprise Management 2(1).

[8] "Dermatoglyphics," Hand Analysis, International Institute of Hand Analysis, 24 January 2005.

[9] Dutta, S. and Mia, I. (ed.) (2011), "The Global Information Technology Report 2010-2011". [Online] Available from: http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf Accessed: August 15, 2011.

[10] GCC Portal: http://www.gcc-sg.org/eng/index.html. Accessed: August 12 2011.

[11] Guthrie, I. (2003), "Electronic Government in the Digital Society." Lomonosov Moscow State University, Russia. [Online] available from: egov_digital_society. Accessed: August 12, 2011.

[12] IMA (2011), "Building the Digital Society," The insitute of mathamtics and its application, UK. [Online]. Available from: building_the_digital_society_20101213122904. Accessed: August 12, 2011.

[13] Jueneman, R.R. and Robertson Jr., R.J. (1998), "Biometrics and Digital Signatures in Electronic Commerce", in 38 Jurimetrics J. [Online] Available from: http://nma.com/mcg-mirror/mirrors/digsig.pdf. Accessed: August 1, 2011.

[14] Ke, W. and Wang, X. (2008), "How do governments matter to the creation of digital economy?" in Fensel, Dieter and Werthner, Hannes (editors) Proceedings of the 10th international conference on Electronic commerce (ICEC), Innsbruck, Austria, August 19-22, 2008.

[15] McMahon, Z. (2005), "Biometrics: History," Indiana University, Indiana University Computer Science Department [Online]. Available from: http://www.cs.indiana.edu/~zmcmahon/biometrics-history.htm. Accessed: August 12 2011.

[16] Renaghan, J. (2005), "Etched in Stone," Zoogoer, August 1997, (Smithsonian National Zoological Park, 26 January 2005).

[17] Richardson, A. (2009), "Why Identification Cards are Important in Today's Economy", Articles Factory [Online]. Available from: http://www.articlesfactory.com/articles/business/why-identification-cards-are-important-in-todays-economy.html. Accessed August 21, 2011.

[18] RNCOS (2011), "Global Biometric Forecast to 2012" [Online]. Available from: http://pdf.marketpublishers.com/463/global_biometric_forecast_to_2012.pdf. Accessed August 30, 2011.

[19] Ross, A. & Jain, A. (2003), "Information fusion in biometrics." in Pattern Recognition Letter 24(13), pp. 2115-2125.

[20] Rukhin, A. L. & Malioutov, I. (2005). Fusion of biometric algorithms in the recognition problem. Pattern Recognition Letters, 26(5), 679-684.

[21] Sarkar, I., Alisherov, F., Kim, T., and Bhattacharyya, D. (2010), "Palm Vein Authentication System: A Review". International Journal of Control and Automation, Vol. 3, No. 1, pp. 27-34.

[22] Shoniregun, C.A., and Crosier, S. (2008), Securing Biometrics Applications. Springer-Verlag.

[23] Tilton, C. (2006), "Biometric Standards – An Overview." Daon. [Online]. Available from: http://www.securitydocumentworld.com/client_files/biometric_standards_white_paper_jan_06.pdf. Accessed: August 12, 2011.

[24] Uhlfelder, D. (2000), "Electronic Signatures and The New Economy" [Online]. Available from: http://ubiquity.acm.org/article.cfm?id=354571. Accessed: August 1, 2011.

[25] Vamosi, R., Monahan, M., Kim, R., Miceli, D., Van Dyke, A. and Kenderski, J. (2011) 2011 Identity Fraud Survey Report. Javelin Strategy and Research.

[26] Westland, D. and Al-Khouri, A.M. (2010), "Supproting e-government progress in the United Arab Emirates," in Journal of E-Government Studies and Best Practices, pp.1-9.

[27] Woodward, J.D. (1997), "Biometrics: Privacy's foe or privacy's friend?," in Proceedings of the IEEE (Special Issue on Automated Biometrics), 85, pp. 1480-1492.

Charts, tables and graphs

List of Tables

Table 1: recognition means in the history of civilisation

Research Reference	Evidence
Renaghan (2005)	Details of a cave dating 31,000 years back revealed hand prints of pre-historic humans with pre-historical pictures apparently signed by fingerprint stamps of authors.
McMahon (2005)	Chinese and Indian historians have references of fingerprints used as signatures in transactions going back five thousand years.
"Dermatoglyphics", (2005)	The Babylonian clay tables of 500 BC show evidence that human kind used to record business transactions and sign it using fingerprint stamps.

Table 2: Biometric performance measures

Performance Measure	Description
False (non-match) rejection rate (FRR) or type I error	The measure of the percentage of times a valid subject has been falsely rejected by the system. FRR (%) = number of false rejections * 100/total number of unique attempts.
False (match) acceptance rate (FAR) or type II error	The measure of the percentage of times an invalid subject has been falsely accepted by the system. FAR (%) = number of false acceptance * 100/total number of unique attempts.
Cross-over error rate (CER)	A measure representing the percent at which FRR equals FAR. This is the point on the graph where the FAR and FRR intersect. The cross-over rate indicates a system with good balance over sensitivity and performance.

Enrolment time	The time taken to initially enrol a new subject with a system by providing samples for creation of reference templates.
Failure to enrol rate (FTER)	Used to determine the rate of failed enrolment attempts. FTER = number of unsuccessful enrolments/total number of users attempting to enrol.
Throughput rate	The time taken by the system to validate transaction data with the data in repository to process the identification or authentication function. This is the rate at which enrolled subjects are processed for acceptance or rejection by the system.

Table 3: Biometric functions

Biometric Capability	Explanation
Identification	is the process whereby one tries to match a submitted sample of biometric information with an existing database of known identities. If a match is established, the identity of the person is established.
Verification	is the process by whereby a confirmation to an identity claim is established. It provides an answer to "Am I really who I claim I am?"
Authentication	is the process by which the truthfulness of the submitted biometric sample is established. The authenticity of the biometric sample submitted establishes the credentials of the person.
Recognition	is the process which is not necessarily for identification or verification. It is meant for recognizing an individual – especially when no features are available for detection. DNA is an excellent example of Recognition application.

Table 4: Evolving biometrical technologies

Biometrics Technology	How it operates ?
Fingerprints	A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.
Iris Scan	One of the most accurate biometric processes in which the veins structure in the iris is used as biometric sample to identify a person. Being an internal organ of the eye whose random texture is stable throughout life, the iris is immune (unlike fingerprints) to environmental influences, except for its papillary response to light. Working on completely different principles from retinal scanning, iris recognition is far more user friendly and offers very high accuracy.
Facial recognition	Facial recognition is an automated method to record the spatial geometry of distinguishing features of the face. Non-cooperative behaviour by the user and environmental factors, such as lighting conditions, can degrade performance for facial recognition technologies.
Voice Recognition	Focuses on differences resulting from the shape of vocal tracts and learned speaking habits. The technology is not well-developed as background noise may affect its performance and reliability.
Palm print/hand geometry	The capture of measurements encompassing the width, height and length of the fingers, distances between joints and shapes of the knuckles. While reasonably diverse, the geometry of an individual's hands is not necessarily unique.
Retinal Scan	Measures the blood vessel patterns in the back of the eye. Because the retina can change with certain medical conditions, such as pregnancy, high blood pressure, and AIDS, this biometric has the potential to reveal more data about individuals than only their identity, and is perceived an intrusive technology, and has lost popularity with end-users.

Vein pattern image	The vein (vascular) pattern image of an individual's hand can be captured by radiation of near-infrared rays. It can be done by using the reflection method to photograph the veins in the hand by illuminating the palm and photographing the reflected light from the back of the palm.
DNA	Except for identical twins, each person's DNA is unique. It can thus be considered a 'perfect' modality for identity verification. DNA identification techniques look at specific areas within the long human DNA sequence, which are known to vary widely between people. The accuracy of this technique is thus very high, and allows both identification and verification.
Gait recognition	Captures a sequence of images for analysis of how an individual walks. Still in an early stage of research & development.
Keystroke recognition	Assesses the user's typing style, including how long each key is depressed (dwell time), time between key strokes (flight time) and typical typing errors. This is more suited as an internal security technology, such as providing computer access within an organisation.
Signature recognition	Analyses a series of movements that contain unique biometric data such as personal rhythm, acceleration and pressure flow. Since these movements can vary with each signing, differentiating between the consistent and the behavioural parts of a signature is difficult.

Table 5: Identity requirements for government service delivery

Application	Remarks
Simple Identification	Security Check and Physical Identification
ID Required to be entered as data	ID required as entry in Service Application Forms
Service Requested OTC (Over the Counter)	ID required to ensure that it is the correct person submitting the request

Service to be delivered OTC (Over the Counter)	ID required to ensure that it is being delivered to the correct person and require confirmation of service delivery (signature of service beneficiary)
Service Requested Remotely	Manual Entry of ID in Application Forms
Service to be delivered remotely	ID required to ensure it is being delivered to the correct person and require confirmation of service delivery

Table 6: International practices of biometrics applications

Country	Biometrics Applications
Canada	• 2005: Iris recognition at airports to expedite pre-approved travellers through customs and immigration • 2011: Fingerprints-based immigration and border entry system launched
USA	• 1999: FBI's IAFIS (Integrated Automated Fingerprint Identification System) becomes operational with the world's largest biometric database with about 55Million records. • 2004: US-VISIT (US-Visitor and Immigrant Status Indicator Technology) launched for border control with full integration to IAFIS as the goal • 2007: e-Passports issued with Basic Access Control and PKI • 2008: FBI expands this databasewith NGI (Next Generation Identification to include multimodal biometrics (faces, iris, fingerprints and palm patterns)
Mexico	• 2009: The Mexican government announces new biometric identity card which will carry fingerprints, a retina scan and a photograph on a magnetic strip to fight corruption in social programs under Mexican Interior Ministry (Instituto Mexicano del Seguro Social).
Salvador	• 1999: Fingerprints based drivers license initiative launched

	• 2007: Multimodal Biometric passport deployment started and later expanded to include criminal justice system apart from Border control.
Costa Rica	• 1998: National ID Card initiative with fingerprints and photographs launched to replace paper based ID cards • 2003: Central Bank launches biometric identification system for secure access to central bank databases for member banks • 2010: Smart Cards initiative launched for secure biometric information on the cards
Colombia	• 1995: Digital Identification reform brought in for introducing biometric information in digital format for National Civil registration and issue of new ID cards for the purpose of Elections and Civil transactions. • 2005: Automated Banking Machines introduced for ATM transactions using biometrics • 2009: The Colombian government makes significant changes to the Cedula and it requires all citizens to change to the new national ID for the presidential elections in 2010.
Grenada	• 2009: Initiates the Civil Identification Registration Program as a part of the Caribbean initiative for Electoral and Civil Identification purposes
Venezuela	• 2007: launches National ID Card with facial and fingerprint data modernizing the Civil Registry for the purpose of electoral system and civil transactions.
Ecuador	• 2007: Part of the CLARCIEV initiative in preparing digital civil registry with biometric identification of photograph and fingerprints. • 2009: Launched the Biometric Screening System for Foreigners at various points of entry to prevent illegals from neighboring countries to enter
Bolivia	• 2009: Biometric Registration of all eligible citizens conducted and a biometric database of Electoral Voter List is created. Successfully conducts Presidential Elections using the biometric database.

Brazil	• 2007: National ID Cards with Biometric Data provided to replace paper cards • 2010: Uses Biometric database for conducting elections using biometrics as a primary identification for voters • 2011: New Generation Smart Cards- called the Civil Identity Registry (Registro de Identidade Civil – RIC) with enhanced security features for biometric data of fingerprints and facial data launched and expected to replace all existing cards by 2019
Argentina	• 2010: Re launches National ID in the form of the Passport booklet including biometric information of fingerprints and facial data • 2011: launches Biometric enrollment for travel and ID documents for expats living outside of Argentina and also for foreign visitors intending to travel to Argentina
Chile	• 1997: Wide spread use of Biometrics in Criminal records • 2007: Part of CLARCIEV- initiative in Civil Registry • 2007/2008: Implementation of Biometric Research Laboratory to validate facial/Iris identification database, benchmarking of search algorithms for 1:N in a 16Million records database
Togo	• 2009: Keeping in line with their commitment to the Economic Community of African States (ECOWAS), Togo adopts the Biometric Passports containing non-repudiated fingerprint information to enhance border access. Non-machine readable passports phased out in 2010, along with other African Nations of ECOWAS (namely Nigeria, Niger, Guinea, Senegal, Cote D'ivoire, Liberia, Benin and Ghana) –Togo, has issued Biometric passports to its citizens
EQ. Guinea	• 2010: The Economic and Monetary Community of Central African States (CEMAC) is set to put biometric passports into circulation within its member states. Members of CEMAC are Cameroon, Congo, Central African Republic, Gabon, Equatorial Guinea and Chad.
Congo	• 2004: Congo launches a unique Iris based identification system for rehabilitation of the ex-combatants of wars to civil life. This program- The Programme National de

	Désarmement, Démobilisation, et Reinsertion (PNDDR) has proved immensely successful. • 2010: Launches Biometric Passports under the CEMAC program.
Tanzania	• 2011: National Identification Authority launches system for issuing of 25 Million Smart ID Cards with biometric for national identification and civil use. • 2011: Biometric authentication based Kiosks deployed as part of e-Government initiatives for enabling eligible citizens to access the Social Security funds and conduct transactions electronically through the kiosks.
Namibia	• 2007: Biometric Driver's license deployed and in action
South Africa	• 1993: HANIS (Home Affairs National Identification System) launched with biometric data collection as part of Identification booklet issued with a 2D Barcode • 2002: Automatic Fingerprint Identification System introduced for aiding criminal justice, digitizing about 4.5Million criminal records and fingerprints collected from 1920 • 2010: Smart ID Card with Biometric data initiated
Germany	• 2003: AFIS introduced for visitors to Germany as part of Schengen Visa for biometric identification. Iris recorded at Airports on entry for monitoring visitors • 2005: e-Passport System with integrated biometric data goes live with facial image as primary biometric identifier • 2007: Second Gen e-Passport released with fingerprint as the primary identifier complying with EU regulations on eMRTD • 2010: RFID based Smart cards with digital data including biometric information initiated to replace normal plastic ID Cards • 2010: Biometric data enabled RFID Smart Cards started to be issued as National ID Cards
UK	• 2001: A formal entity- The BWG (Biometrics Working Group) established under the CESG (Communications-Electronics Security Group). The UK Biometrics Working Group (BWG) is a cross government group focused on

	the use of biometric technology across government and Critical National Infrastructure (CNI) • 2005: Iris and Fingerprint recognition for visa holders and frequent travellers for Border Control • 2006: e-Passports with Biometric data – fingerprint, iris and facial data started to be issued to British citizens compliant with US Visa Waiver Program • 2010: Second Generation e-Passports with enhanced security features introduced.
Portugal	• 2006: e-Passports compliant with EU standards issued. • 2007: National ID Cards with fingerprint data, photograph and digital signature issued to citizens. • 2007: Portugal's Faro Airport becomes the first airport to begin using e-Passport biometric reading for fast track entry into the country followed by Lisbon.
Turkey	• 2007: Smart cards with personal information and fingerprint data launched for Healthcare services. • 2010: e-Passports with fingerprint and facial recognition launched in Turkey
Saudi Arabia	• 2003: Starts issuing Smart Card based National ID Cards with fingerprint data • 2006: Starts issuing Biometric data enabled smart cards as National ID Card for all citizens and residents for primary ID for civil transactions. • 2010: Saudi announces requirement of fingerprints for all visitors as part of identification for border security.
UAE	• 2003: UAE is the first country to Start Iris recognition for all visitors at Dubai airport and subsequently extends it to all International airports in the country. • 2004: Biometric enabled e-Gate card launched and issued to residents and citizens enabling fast track entry and exit from the Country's airports based on fingerprint identification • 2005: Starts issuing chip based Smart Cards as National ID Cards with biometric data (fingerprint), photograph and digital signature for signing. • 2009: Biometric e-Passports program launched with RFID

	and fingerprint data that can be read by machines. • 2010: Starts issuing second generation ID Cards with RFID capabilities as a combi-card • 2011: National Elections being held with the help of National ID Cards with Biometric verification for voters.
Bahrain	• 2005: Introduces the Smart Card based ID Card with fingerprint data for identification and authentication to replace the CPR card in a phased manner. • 2009: Installs biometric scanners and high security immigration gates at its airport, becoming the third country after UK and Japan to do so
Qatar	• 2006: Introduces Smart Card based ID Card with fingerprint, facial features and iris data along with personal data to replace their existing plastic ID Card.
Oman	• 2004: Launches National Registry System for issuance of smart cards as Electronic ID Card with biometric information securely embedded in the ID cards for all civil transactions. • 2006: Issues Smart ID Cards to all citizens
Kuwait	• 2009: Launches new smart card ID Cards for Civil ID Cards that include fingerprint and DNA information as biometric data for identification of citizens and residents in the country. Biometric Data is part of the Civil Register. Enhanced capabilities include PKI for digital signatures.
India	• 2009: India launches the most ambitious Bio-enrollment program for identification of its 1.2Billion population. The program aims at providing a Unique Identity to all the citizens with the fingerprints as primary identifiers and iris scan as well. The primary goal of the Biometric ID is to ensure social benefits distribution to rightful and deserving citizens and prevent theft of social funds.
China	• 2005: One of the early adopters of Biometric technology for automated border crossing- installs biometric access gates between Shenzen and Hongkong, catering to nearly 400,000 crossings every day. This is followed by Zhuau-Macau border in 2006.

Thailand	• 2005: Smart ID Cards with fingerprint biometric data with Match-On-Card capabilities launched for personal Identification.
Malaysia	• 2005: MyKad- the National ID Card with smart card capabilities launched with biometric data for identification of card holders extending from their 2011 initiative. • 2005: Cyber Security Malaysia becomes the sole certification agency for smart card based applications and readers for Common Criteria certification in Malaysia. • 2011: Biometric fingerprint system introduced for all foreign visitors entering Malaysia at the Airports and other entry points (Singapore-Malaysia) • 2011: Election Commission adopts biometric technology for voter identification
Japan	• 2006: Biometric Passports meeting US Visa Waiver program start being issued to Japanese Citizens • 2007: Biometric Identification systems deployed in airports across the country and extended to all borders in 2008 • 2010: Widespread use of Biometrics in Kiosks, ATMs
Taiwan	• 2009: Biometric e-Passports launched for issuing e-Passports to Taiwanese citizens • 2011: Biometric Border Control systems deployed on trial
Philippines	• 1998: Social Security Cards with Biometric data issued to Philippines citizens and residents to prevent fraud • 2009: e-Passports with Biometric data introduced to replace all existing passports. All renewals issued with new Biometric passports • 2010: The Government announces Biometric registration for Elections for Voter registration
Indonesia	• 2009: Biometric Passports start being issued as e-Passports • 2010: Launches biometric verification and identification at the airports border control

Australia	• 2006: Biometric e-Passport system launched • 2008: Smart gate- Biometric border control systems launched • 2011: Australia seeks to establish Biometrics Working Group to guide biometric implementation across the nation
New Zealand	• 2006: Biometric Immigration systems for border control at airports launched • 2009: Biometric Registry for Immigration and Biometric Passports for citizens deployed

Table 7: Overview of UAE ID card capabilities and functions

Applet	Interface	Functionality
ID & E-Purse Applet	Contact and Contactless except for E-Purse the interface is only Contact	There are 10 personal identification data folders in the EEPROM of the UAE Card. Those 10 personal identification data folders provide various identification data about the ID Card holder including E-Purse data. The function of the "ID Applet" is to manage access to those folders. Another function of the "ID Applet" is to provide cryptographic services namely mutual authentication and verification of digital certificate of personalized data. The 10 identification folders (referred to as ID Application Data Folders) are as follows: 1. Public ID Data 2. E-Purse Data 3. Labor Data 4. Health Data 5. Defense Data 6. Driving License Data 7. Family Book Data 8. Social Services Data 9. Address Data 10. Qualification Data

PKI Applet	Contact	The function of the PKI applet is to facilitate the electronic authentication of the ID Card holder and to facilitate the generation of electronic signatures by the ID Card holder (within a PKI infrastructure). The PKI Application Data Folder in the EEPROM contains provision for 5 RSA Key Pairs and provision for the corresponding 5 RSA Certificates. During personalization, only 2 Key Pairs are personalized and their corresponding 2 digital certificates are constructed. Those 2 Key Paris are used for the Authentication and Digital Signature functionalities. The files for the remaining 3 Key Pairs and their corresponding 3 digital certificates are left empty (RFU). 3 PINs are personalized (User, Admin, & RFU)
MOC Applet	Contact	The MOC is a third party applet. Hence, the applet byte code is personalized in the EEPROM. The MOC applet stores two fingerprint templates of the ID Card holder. The applet facilitates the biometric authentication of the ID Card holder by comparing the ID Card holder fingerprint captured by a biometric terminal at a service counter against the fingerprint template stored inside the ID Card.
eTravel Applet	Contact and Contactless	This is an ICAO compliant applet. It contains 5 data groups and a separate elementary file as follows: DG1: MRZ containing basic personal details DG2: Portrait DG11: Additional personal details DG13: Full name (Arabic) and date of expiry DG15: Active Authentication Public Key EF.SOD (Post Perso): Data signature Phase 2 will contain the following additional data groups and an elementary file: DG3: 2 fingerprints (ISO 19794-4) DG14: RSA or ECDSH Parameters (EAC Authentication) EF.CVCA: Certification Authority Reference

MIFARE Applet	Contactless	This is an applet that emulates the functionality of the 1K MIFARE contactless card.

Table 8: National Validation Gateway Services

PKI Validation Services	Identity Data Provider Service	Card Validation Services
- Used in a business scenario where a Service Provider handles the authentication process and needs only PKI validation. - A secure 'valid/not valid' engine providing Real Time validation of ID certificates through OCSP.	- For Service Providers that hand off the complete authentication process to Emirates Identity Authority[9]. - Offers Authentication as a Service (e.g. On-demand Authentication) - Implements the SAML IdP (Identity Provider) protocols - Provides 2-factor ID Card authentication	- Added-values services such as PIN Change, Verify Card Genuine and Biometric Verification.

[9] Emirates Identity Authority is an independent federal government organisation established in 2004 to manage the implementation of the national identity register.

List of Figures

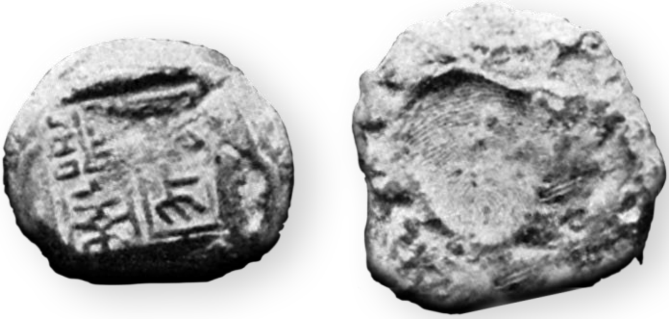


Figure 1: Late B.C. - Picture writing of a hand with ridge patterns was discovered in Nova Scotia.

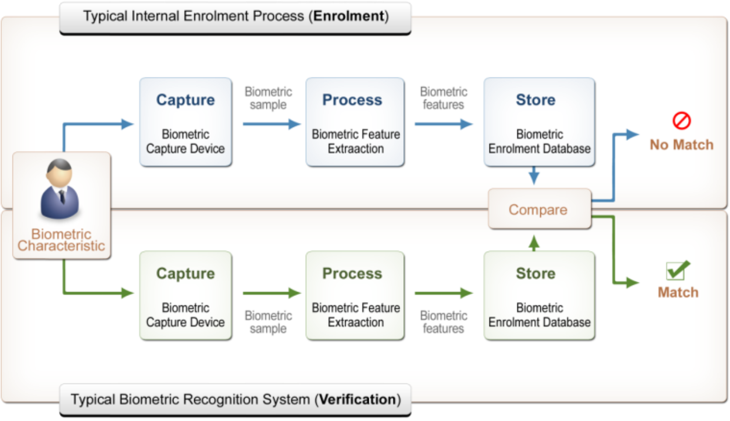

Typical Internal Enrolment Process (**Enrolment**)
Capture
Biometric Capture Device
Biometric sample
Process
Biometric Feature Extraaction
Biometric features
Store
Biometric Enrolment Database
No Match
Compare
Biometric Characteristic
Capture
Biometric Capture Device
Biometric sample
Process
Biometric Feature Extraaction
Biometric features
Store
Biometric Enrolment Database
Match
Typical Biometric Recognition System (**Verification**)

Figure 2: Enrolment and verification processes

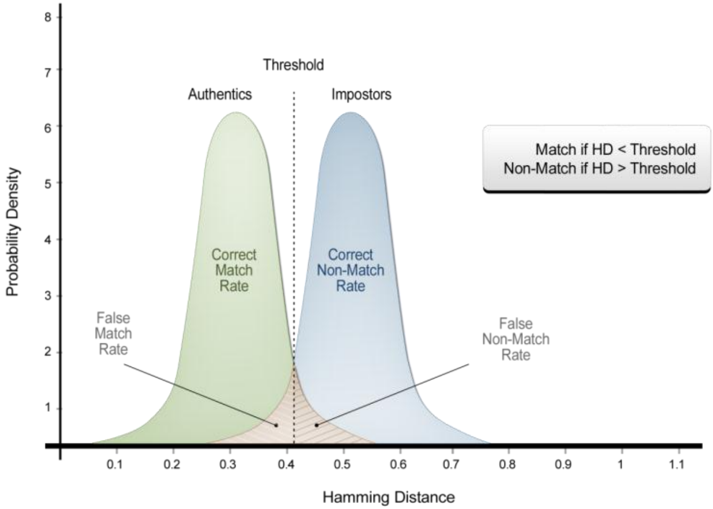
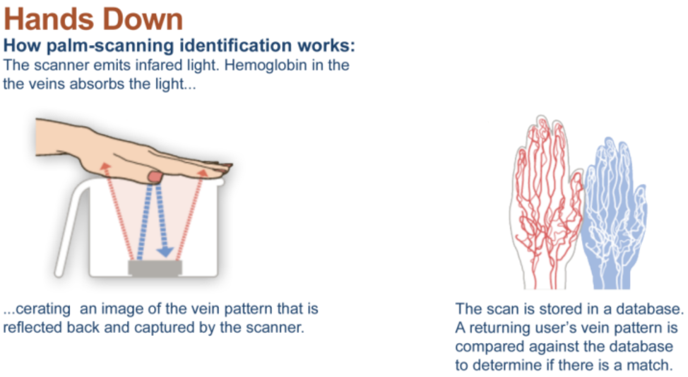


Figure 3: Tuning biometric systems


Hands Down

How palm-scanning identification works:

The scanner emits infared light. Hemoglobin in the the veins absorbs the light...

...cerating an image of the vein pattern that is reflected back and captured by the scanner.

The scan is stored in a database. A returning user's vein pattern is compared against the database to determine if there is a match.

Figure 4: Palm Vein Recognition

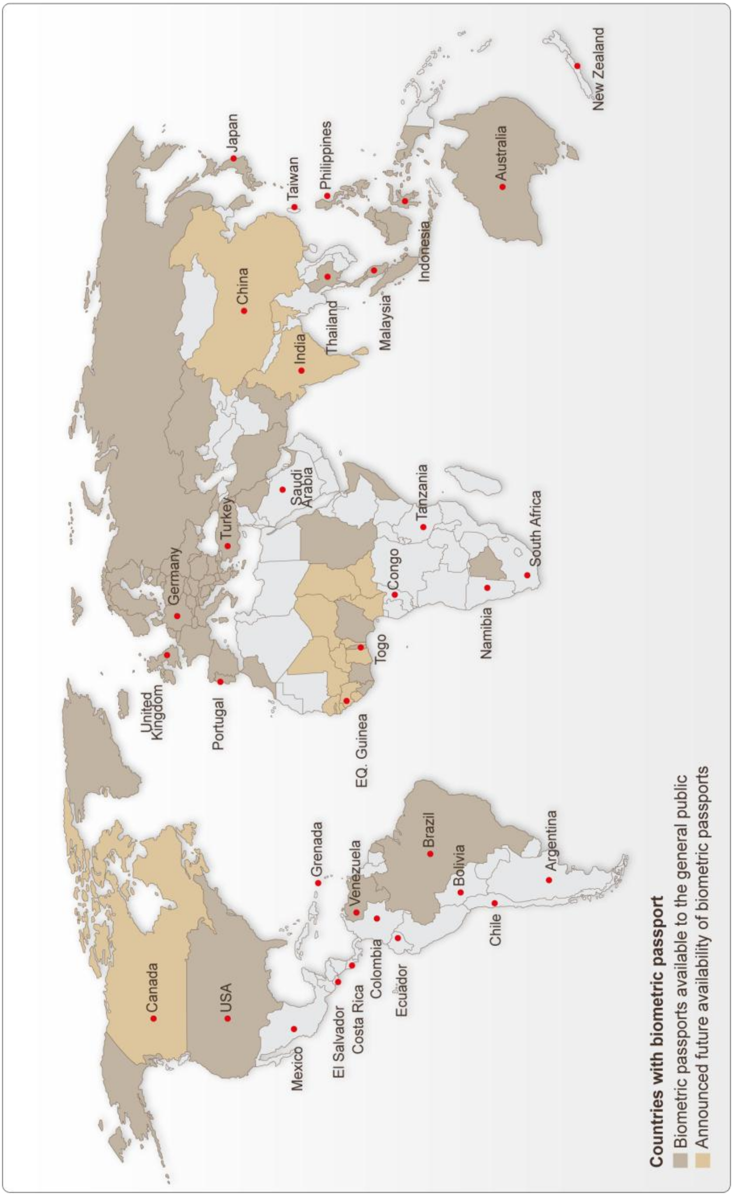
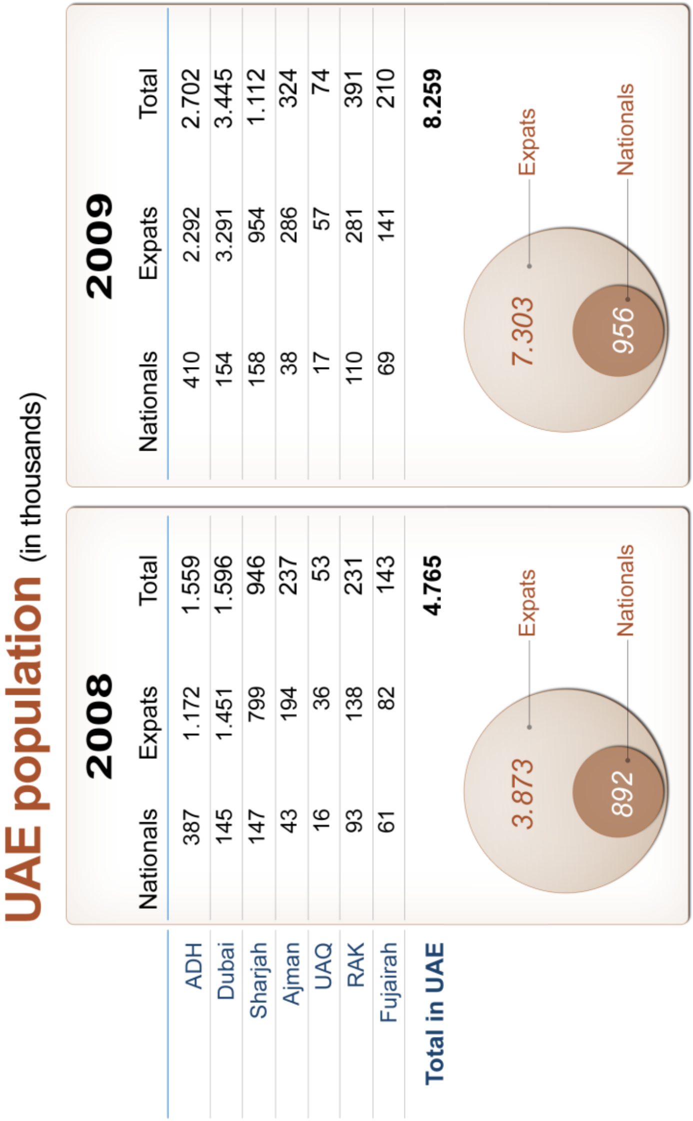


Figure 5: Global biometric adoption



UAE population (in thousands)

	2008			2009		
	Nationals	Expats	Total	Nationals	Expats	Total
ADH	387	1.172	1.559	410	2.292	2.702
Dubai	145	1.451	1.596	154	3.291	3.445
Sharjah	147	799	946	158	954	1.112
Ajman	43	194	237	38	286	324
UAQ	16	36	53	17	57	74
RAK	93	138	231	110	281	391
Fujairah	61	82	143	69	141	210
Total in UAE			**4.765**			**8.259**

Figure 6: UAE population demographics

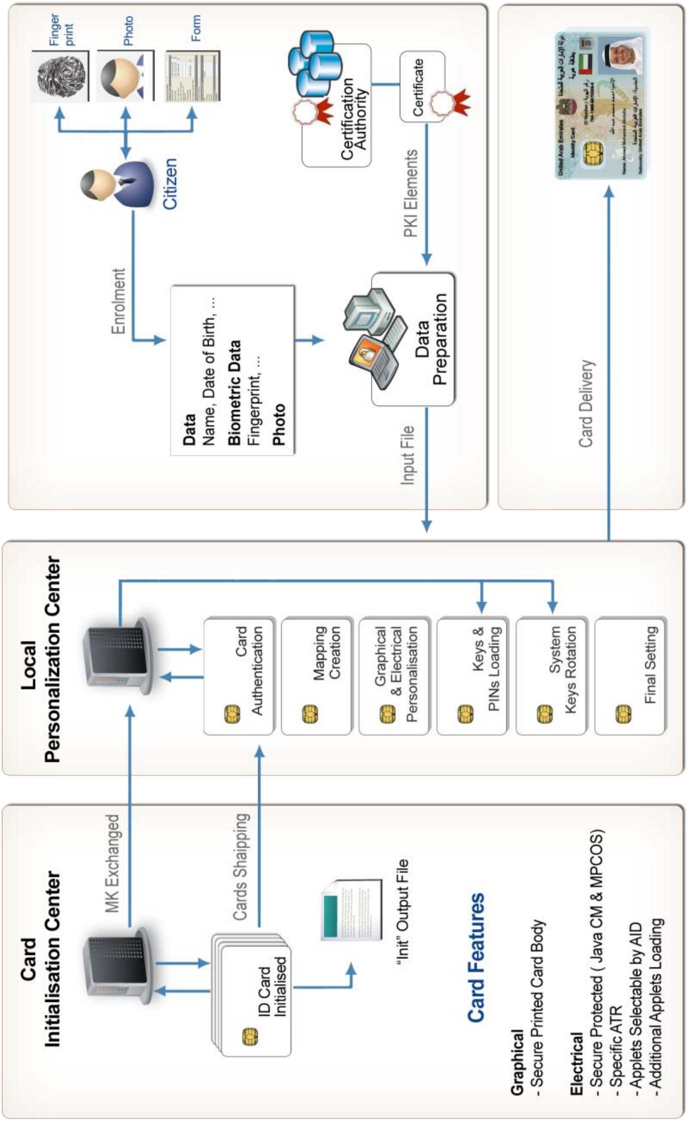


Figure 7: UAE ID card issuance process.

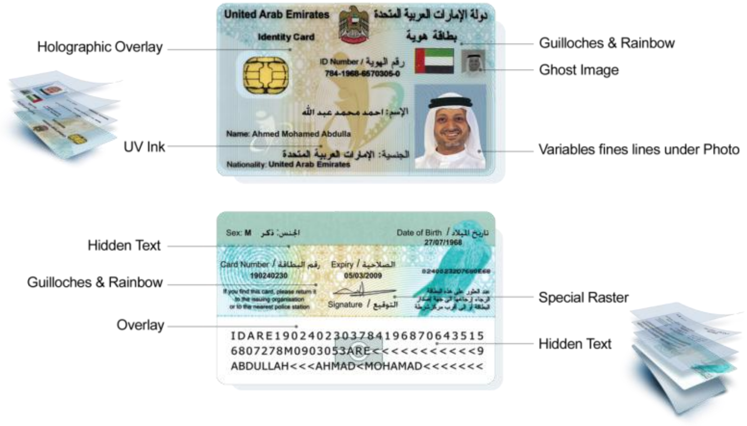

Holographic Overlay
UV Ink
Guilloches & Rainbow
Ghost Image
Variables fines lines under Photo
United Arab Emirates
دولة الإمارات العربية المتحدة
Identity Card
بطاقة هوية
ID Number / رقم الهوية
784-1968-6570305-0
الإسم: احمد محمد عبد الله
Name: Ahmed Mohamed Abdulla
الجنسية: الإمارات العربية المتحدة
Nationality: United Arab Emirates
Hidden Text
Guilloches & Rainbow
Overlay
Special Raster
Hidden Text
Sex: M الجنس: ذكر
Date of Birth / تاريخ الميلاد
27/07/1968
Card Number / رقم البطاقة
190240230
Expiry / الصلاحية
05/03/2009
If you find this card, please return it to the issuing organisation or to the nearest police station
Signature / التوقيع
IDARE1902402303784196870643515
6807278M0903053ARE<<<<<<<<<<<<9
ABDULLAH<<<AHMAD<MOHAMAD<<<<<<<

Figure 8: UAE Card security features

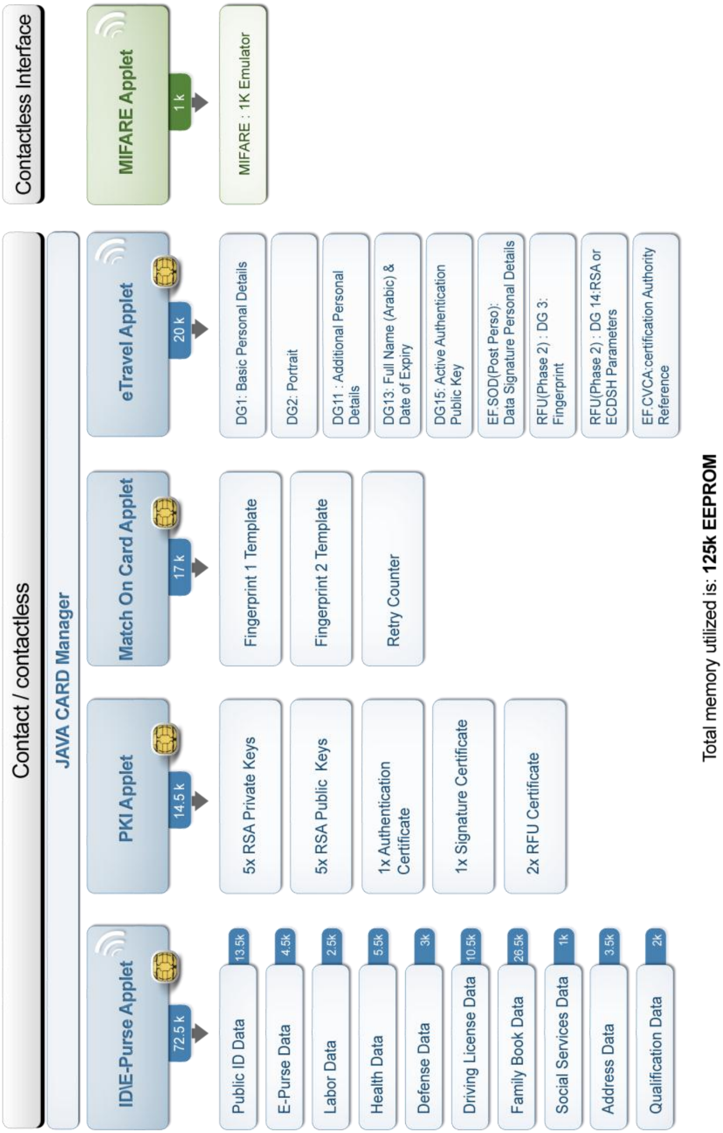


Figure 9: Identity applets in UAE card

E-Government Practices

PKI in Government

Digital Identity Management Systems[10]

DR. ALI M. AL-KHOURI

ABSTRACT: Despite the significant investments in e-Government, reported experiences show limited and struggling success cases. In the last 15 years, governments efforts have been scattered, as agencies were mainly concerned with the development of informational portals and some basic online services resulting from the automation of a few traditional transactions.

In fact, Governments have been cautious in terms of their preferred eGovernment approaches and strategies. A large number of governments services are still provided over the counter and requires the physical presence of citizens. This is in principle due to the fact, that existing eGovernment environments lack effective methods through which they can establish trust and avail services over digital networks.

This article discusses the need for trust establishment to advance e-government in light of the existing and

[10] Al-Khouri, A.M. (2012). "PKI in Government Digital Identity Management Systems". Surviving in the Digital eID World, **European Journal of ePractice**, No. 14, pp. 4-21.

emerging realities. It looks at the evolving forms of identities, namely; digital identities and the role of PKI technology in enabling such requirements.

The key contribution of this article is that is provides an overview of a large scale national PKI program which was deployed part of a government identity management infrastructure development scheme in the United Arab Emirates. It provides an insight into the architecture and features of the PKI deployment. It presents how the UAE government planned and set up a national identity validation gateway to support both online and traditional transactions. It also includes some reflections on key management considerations and attempts to make reference to some European initiatives to highlight similarities and differences with the UAE and GCC projects.

Key words: *e-Government, eService, PKI, identity management, ID card.*

1. INTRODUCTION

THE 24-hour authority is now a much sought after objective for many national Government development programs (Bicking et al., 2006). Delivery models of Government services over digital networks is seen to enhance access and overall governance (Ebbers et al., 2008). In fact, other governments see this as an opportunity to address three major challenges of the modern age, namely; economic productivity, social justice and the reform of public services (UK Cabinet Office, 2005).

The "24-hour authority" allows citizens and other stakeholders like commercial organizations, companies etc., to contact different authorities at anytime and anywhere and regardless of their geographical distances. Many governments worldwide have released regulatory bylaws to guide and inflict the development of user driven portals and services with 24x7-availability. This is a strong assertion of the 24-hour authority endorsement by different governments on different levels i.e., local, regional, national, international, etc.

Having said that, it is well noted in various publications that the majority of citizens still show a stronger preference for traditional access channels of OTC (Over the Counter) interactions with government and private organisations (Ebbers et al., 2008; Streib & Navarro, 2006). This shows that there exists a clear gap in the channels of services that Governments provide and what citizens and government agencies also prefer. Nonetheless, the 24-hour interaction with the Government for service delivery remains a desirable feature for both the citizens and the governments (Becker et al., 2011).

Generally, the interactions of citizens with their governments can be either informational or transactional in nature. The following figure depicts a model of citizens Interactions with their Government.

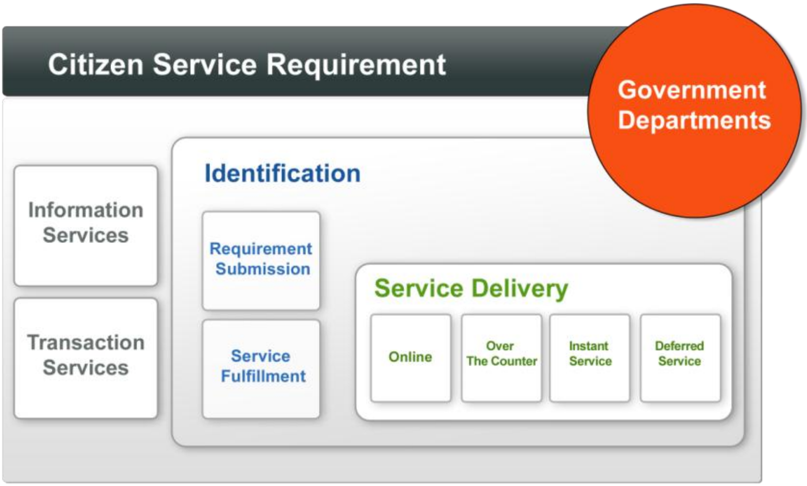


Figure 1: Citizens Interactions with Government Services

The key enabling factor between the requested service by the citizen and thereafter the fulfillment of the service itself is the Identity Establishment of the service applicant and the service recipient. Governments for long have spent great effort and struggled to some extent in providing and ensuring effective and secure identification systems to their citizens. Different government departments devised their own identity mechanisms in receiving service requests and service deliveries.

At a national level, a unified identification mechanism has always been a challenge. We would also argue that the deficit in establishing trust in government services is a more condescending challenge and might carry more unscrupulous consequences. In one of our earlier publications we pointed to the fact that e-Government initiatives around the world have not succeeded in going through the third and fourth phases of e-Government development (Al-Khouri & Bal, 2007a; Al-Khouri & Bal, 2007b). See also Figure 2.

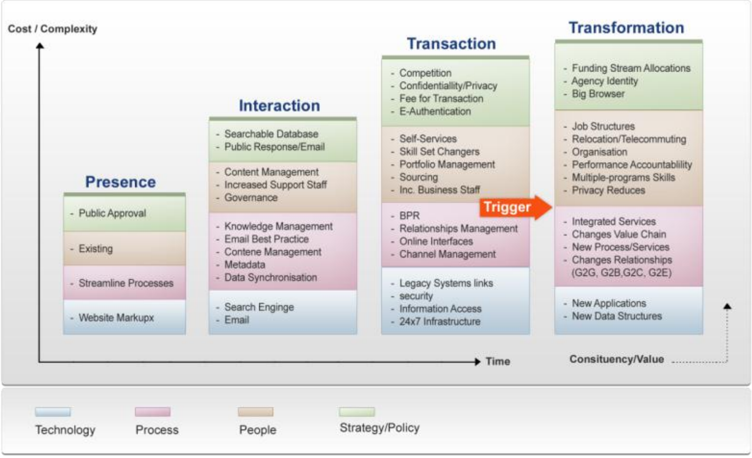


Figure 2: Four Phases of e-Government – (Baum & Maio, 2000)

In our studies, we highlighted the need for fundamental infrastructure development in order to expand outreach and accelerate e-Government diffusion. See also Basu, 2004; Baum and Maio, 2000; Schedler and Summermatter, 2003).

The purpose of this article is to provide an overview of the UAE government PKI program which was implemented part of a national identity management infrastructure development initiative. It explains the major components of the system and how the government intends to support e-government progress in the country. More pragmatically, we seek to make a contribution to the available research literature on the implementation of PKI in national identity management systems.

This article is structured as follows. The first section discusses the need for trust establishment in light of the existing and emerging validation methods. The next two sections looks at the evolving forms of identities, namely; digital identities and the role of PKI technology in enabling such requirements. Next, a brief highlight is provided around e-Government and identity management initiatives from around the world. Then in the following two sections, we introduce the UAE national identity management infrastructure and describe the UAE PKI program and bring to light its major components. Finally, some reflection is provided on key management considerations and an attempt to make reference to some European initiatives to highlight similarities and differences with the UAE project, before the paper is concluded.

2. TRUST ESTABLISHMENT BY IDENTITY

Trust establishment in a traditional or e-Government environment is necessitated by the fact that a citizen is largely anonymous among the mass multitude of population. Yet the government is expected to reach out to the citizen and provide its services on a personalized level (Heeks, 2006). The following table provides an overview of the types of trust establishment needed for different service types.

Table 1: Trust establishment and validation methodsThis article is structured as follows. The first section discusses the need for trust establishment in light of the existing and emerging validation

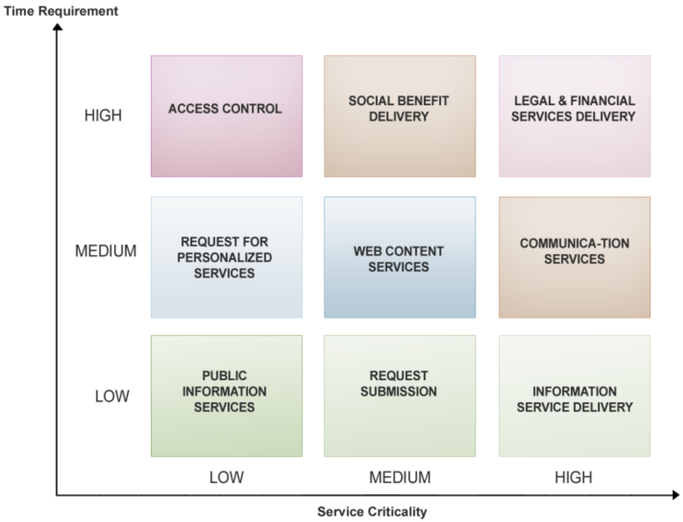
methods. The next two sections looks at the evolving forms of identities, namely; digital identities and the role of PKI technology in enabling such requirements. Next, a brief highlight is provided around e-Government and identity management initiatives from around the world. Then in the following two sections, we introduce the UAE national identity management infrastructure and describe the UAE PKI program and bring to light its major components. Finally, some reflection is provided on key management considerations and an attempt to make reference to some European initiatives to highlight similarities and differences with the UAE project, before the paper is concluded.

Table 1: Trust establishment and validation methods

Service Type	Application	Method
Informational	Public Information Simple Identification – no need of identity verification	Physical entry of name or ID
Informational	Private Information- ID Required to be entered as data for information retrieval	Manual Entry of ID Documents to prove ID of intended service recipient
Transactional	Service Request submission: ID Required to be entered as data- OTC (Over The Counter)	Manual Entry of ID Documents to prove ID of intended service recipient
Transactional	Service to be delivered OTC (Over the Counter)- Ensure that it is being delivered to the correct person	Documents to prove ID of intended service recipient
Transactional	Service to be delivered OTC (Over the Counter)- Ensure that it is being delivered to the correct person and require confirmation of service delivery (signature of service beneficiary)	Documents to prove ID of intended service recipient

Transactional	Service Being Requested Remotely	Manual Entry of ID + Documents to prove ID of intended service recipient
Transactional	Service to be delivered remotely- ensure it is being delivered to the correct person and require confirmation of service delivery	Auto ID/ Digital ID Verification

For each interaction, the trust establishment varies to the extent of the service being requested and delivered. This is depicted in the trust matrix illustrated below.



Time Requirement	LOW	MEDIUM	HIGH
HIGH	ACCESS CONTROL	SOCIAL BENEFIT DELIVERY	LEGAL & FINANCIAL SERVICES DELIVERY
MEDIUM	REQUEST FOR PERSONALIZED SERVICES	WEB CONTENT SERVICES	COMMUNICA-TION SERVICES
LOW	PUBLIC INFORMATION SERVICES	REQUEST SUBMISSION	INFORMATION SERVICE DELIVERY

Figure 3: Trust matrix

This is a simple trust matrix to illustrate the basic needs of the citizen interactions with their government. For each type of interaction, the trust requirements vary depending on the nature and criticality of the service being sought and being delivered. The Higher the criticality, the higher and more complex becomes the trust requirement.

Trust is established by a set of credentials that need to be presented by the service seeker. Whether the service is being sought or delivered over the counter or over remote service channels, trust establishment is constructed based on the presented credentials. These credentials thus are considered essential constituents of the Identity Profile that needs to be presented both to prove the identity of the service seeker as well as the service provider.

There are a number of conventional credentials that citizens are used to provide to establish their identity. For instance, birth certificates issued at hospitals which are later certified by the municipal authorities are considered legal documents of existence. Other affidavits and notarized documents serve as legal documents to establish an identity. These are the basis on which Governments seek to provide identification documents to their population.

In the current complex digital world where a person can do different identities, such documents fall woefully short of trust establishment needs. Many Governments around the world have recently stepped in to precisely address this critical requirement and provide digital identities to their citizens (Al-Khouri, 2011). The digital identity in government terms can be defined as a set of verifiable credentials provided by the Government to its population that can be used to identify and authenticate them by a trust chain setup by the government itself. One of the approaches in this path is the development and integration of a government identity management system with Public Key Infrastructure (PKI) technology. The following section will elaborate on this further.

3. DIGITAL IDENTITIES

For any Government transaction, citizens need a “recognized’ ID. This recognition is well accorded when it is issued by the Government itself. Government issued IDs are no new phenomenon. However, paper based IDs that were long issued (like passports, social security IDs, etc.) are no longer adequate.
Governments, in the last ten years have re-engineered their citizen identity systems to meet the challenges and needs of the e-world and its new economy (Broster, 2011; Stavrou, 2005). In fact, the last few years has witnessed the evolution of the digital identifies or so called e-Identities by various governments across the world (Griffin, et al., 2007; Seifert, 2003;).

Driving factors for issuing digital identities have been varying for different governments. However, the underlying need for digital identity has remained the same around the globe. Strengthening primary identification issuance process, enhancing border security, supporting social security, and improving social benefits delivery are some of the key drivers for digital identity evolution. The need of Government entities to become a 24-hour authorities has also been a major contributor in this regard. All this together has played a major role in the development and deployment of different national identity management initiatives and frameworks in different parts of the world to develop digital identities (Al-Khouri and Bechlaghem, 2011).

As mentioned earlier, digital identity is not just a number but a set of parameters that constitute a profile of the identity holder. The scenarios in an eGovernment environment can be much more complex as the identity holder may play different and simultaneous roles. The Government as the identity issuer needs to provide a generic identity and yet meet the demands of effective identity management including security and privacy. This is the paradox of identity management.

It is the role of the government to associate digital identities to specific persons who will be authorised to perform certain actions in physical or digital forms. This association is facilitated through creation of an identity profile consisting of name, ID number, biometric information, digital certificates and digital signatures that altogether construct a strong digital identity (Al-Khouri, 2011; Wilson, 2005).

Many governments have considered PKI technology to establish and implement this binding. In basic terms, PKI attaches identities to digital certificates for the purpose of assured, verifiable, and secure digital communications. The next section explains this further.

4. PUBLIC KEY INFRASTRUCTURE (PKI)

Public key infrastructure, commonly referred to as PKI, is an Information Communication Technology (ICT) infrastructure is a term used to describe the laws, policies, procedures, standards, and software that regulate and control secure operations of information exchange, based on public and private keys cryptography (Brands, 2000). Table 2 summarises the primary elements that make up the PKI components. The term PKI is used in this article to refer to the comprehensive set of measures needed to enable the verification and authentication of the validity of each party involved in an electronic transaction.

Table 2: Basic PKI Components (The Open Group- Architecture for PKI)

Component	**Description**
Digital Certificates	Electronic credentials, consisting of public keys which are used to sign and encrypt data. Digital certificates provide the foundation of a PKI.
Certification Authorities (CAs)	Trusted entities or services that issue digital certificates. When multiple CAs are used, they are typically arranged carefully prescribed order and perform specialized tasks, such as issuing certificates to subordinate CAs or issuing certificates to users.
Certificate Policy and Practice Statements	Documents that outline how the CA and its certificates are stored and published.
Certificate Repositories	A directory service or other location where certificates are stored and published.
Certificate Revocation Lists (CRL)/ OCSP	Lists of certificates that have been revoked before reaching the scheduled expiration date. OCSP – Online Certificate Status Protocol is an Internet Protocol for obtaining the revocation status of the certificate.

PKI offers high levels of authentication for online users. It also provides advanced functions such as encryption and digital signature, to provide higher levels of protection of elevated echelons of data privacy, and streamline workflow and enable secure access (Stavrou, 2005). The cornerstone of the PKI is the concept of private keys to encrypt or digitally sign information. One of the most significant contributions a PKI has to offer is non-repudiation. Non-repudiation guarantees that the parties involved in a transaction or communication cannot later on deny their participation. The importance of PKI is captured in the citizen service model shown below in Figure 4.

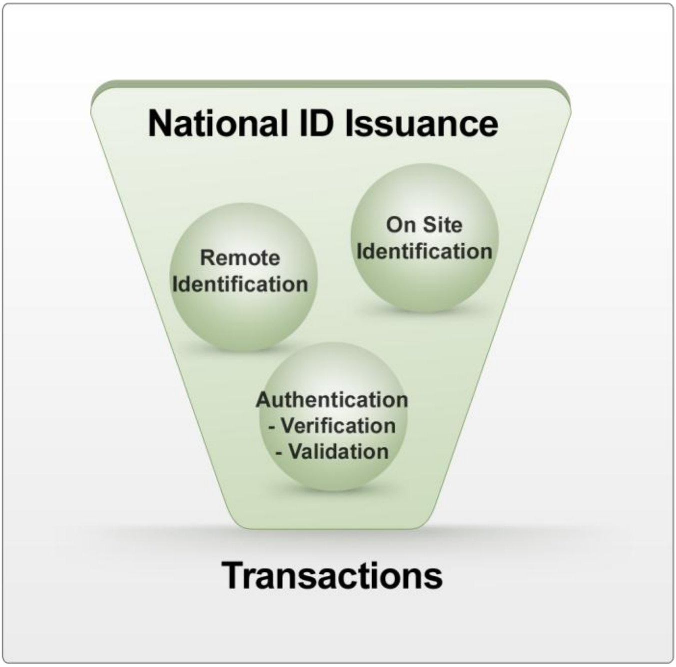


Figure 4: Citizen Service Model

As highlighted earlier, identification remains the cornerstone for trust establishment in any transactions. On site identification or remote identification over digital networks depends on the identity credentials presented to the identification seeker. The presented identity is validated and verified which should lead to availing or denying the requested service. This transaction of identity verification is achieved more securely with PKI. Figure 5 shows the different needs of identity verification and validation.

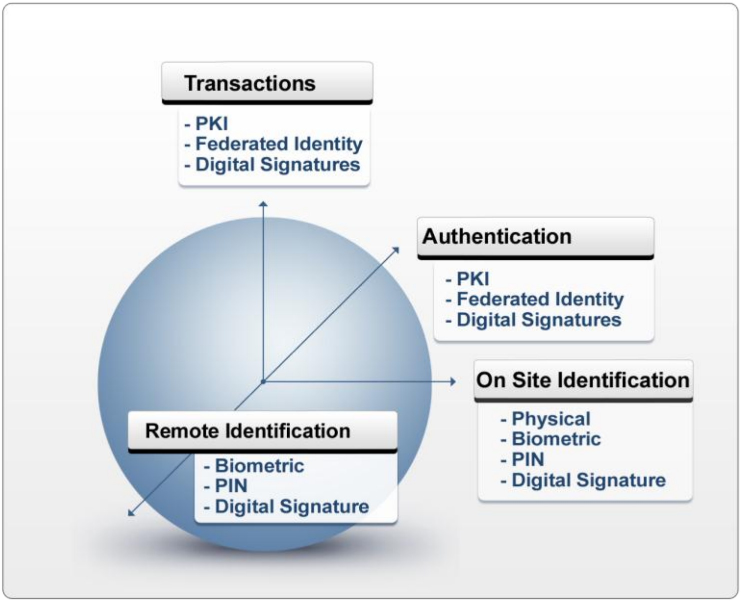


Figure 5: Identity Requirements

Complemented with other methods, PKI enables users to securely communicate on an insecure public network providing public keys and bindings to user identities. The following sections attempt to provide an overview of government identity management systems from around the world and the subsequent sections will present the UAE government efforts to integrate PKI technology to construct digital identity profiles of its population.

5. EGOVERNMENT AND IDENTITY MANAGEMENT INITIATIVES AROUND THE WORLD

According to the 2010 UN e-Government Survey, South Korea is ranked first in the world in e-Government, more specifically in digital IDs and national ID based commercial transactions, followed by the United States of America (UN, 2010). Western Europe follows closely behind.

Over the last decade, Belgium, Finland, Norway led the Digital revolution. These countries have transformed their Government transactions and enabled many secure G2C internet-based service modeled transactions. Digital certificates issued to the citizens are key characteristics of these systems. The USA, under the Office of the CIO, has developed a comprehensive Identity and Credential Management Framework and is spearheading the unified National ID card implementation.

The Middle East has taken a cautious approach and it seems to seek to learn from existing implementations to avoid the pitfalls of early adopters and adopt successfully tested technologies in field of identity management. The 2010 United Nations e-Government Survey (UN, 2010) and the 2010 Global Information Technology Report (Dutta, S. and Mia, 2011) validate this statement amply.
The United States, UK and most of European countries have implemented biometric identification systems to identify visitors and transform border control mechanisms. South Korea on the other hand, has issued smart card based national IDs to all its citizens and residents and enabled eID-based transactions, with the Identity

validated and verified by the Government. UAE, Oman, Bahrain, Qatar, and many other countries in the Middle East have also launched multiple large scale biometric-based identity programs providing secure and modern identity documents to their citizens and residents.

Overall, Governments in the last decade have spent tremendous efforts and substantial financial expenditure in modernising their identity systems with the aim to develop compelling Identity Profiles to strengthen security systems and protocols used across government agencies. The next section will provide an overview of one of the very successful government initiatives to develop a sophisticated and modern identity management system.

6. UAE IDENTITY MANAGEMENT INFRASTRUCTURE

UAE has been at the forefront of adopting advanced identification technologies in the Middle East region and among all Arab countries. It is ranked as one of the leading countries in the region in facilitating e-Government services, and the highest in terms of its network infrastructure coverage (Dutta, S. and Mia, 2011; UN, 2010). Backed by a state of art ICT infrastructure and the network connectivity, electronic collaboration and integration is facilitated between different Government departments to share data which in turn enabled many forms of e-government service models; i.e., G2C, G2G, G2B.

UAE embarked on an ambitious national identity program in 2003 and have successfully enrolled 99% of citizens and nearly 70% of the entire population. The program which is being implemented by a federal government entity named Emirates Identity Authority (also referred to as Emirates ID), envisages to enroll all the population (estimated around 9 million) by 2013. Each individual above the age of 15, is required to visit an identity registration center for his/her biometrics and photo to be captured. Those who are below this age will only be registered with biographical data, however, linked to their parents in the database.

Each individual in the population is issued with a smart ID card. The UAE ID card is one of the most technologically advanced and secure smart cards in the world. It contains unique identity number, basic biographical data, biometric information (for those above 15), and digital certificates of the card holder.

Cardholders can digitally sign transactions thus enabling e-commerce. The national PKI validation gateway enables real time verification and validation of digital transactions and strong user authentication capabilities. The government is working on a 5-year PKI-enabled services rollout implementation model to integrate the card with public sector services and social benefits delivery and enable PKI-based transactions.

It is worth to mention that the UAE have recently concluded (and successfully so) the national elections for the Federal National Council where the national ID card (including the use of digital certificates) served as the only identification method to cast votes electronically. This enabled country wide elections to be held and results declared within all in one day.

The UAE card has many capabilities. One is related to e-purse functionality which is planned for 2013 that will enable service providers to offer micro payments for all cardholders with their identities validated, verified and authenticated by the national Government validation gateway. Another capability is related to signing documents and notarization. Of specific interest would be the digital signature capability of the UAE national ID card. For example, electronic documents can be digitally signed using the certificates provided in the national ID card. These signatures can be represented on physical prints of the documents as QR codes that carry the digital signature. Thus digital signatures can be physically available on paper documents which can also be verified. A smart phone can read the QR[11] code on a digitally signed paper document and refer it to the OCSP[12] or the CRL[13] for verification. Verification of the signature can then be carried out in real time.

[11] QR code: an abbreviation for Quick Response code; is a type of 2D bar code that is used to provide fast readability and large storage capacity of information through a smart phone. It has wide use in the United Kingdom and the United States; and is growing fastest in Canada and Hong Kong.

[12] OCSP (Online Certificate Status Protocol) is one of two common schemes for maintaining the security of a server and other network resources.

[13] CRL (certificate revocation list) is a list of certificates that have been revoked before their scheduled expiration date.

7. THE UAE PKI PROGRAM

When the UAE ID card program was launched in 2003, the government deliberately decided to integrate PKI to create digital identity credentials for its population and as an essential component of its identity management infrastructure. At the time, it was a massive exercise to determine the PKI requirements and to specify the features and functions of the proposed infrastructure. Back in 2003, there were not too many references or precedents available that boasted of a successful PKI implementation. Our worldwide PKI implementation study revealed that barring Belgium and to a certain extent South Korea, no other country had a proven track record of the architecture required. It was then left to the project team to define the needs of the PKI (See also section 8).

Considering a long term support requirements and operational requirements, the team chose to go with a commercial product available and customize it to the government specific needs. Having decided on the solution platform, the next crucial decision was on the architecture of the PKI itself. The primary design element for the architecture development was the process to provide credentials to all population in the country and address e-government requirements.

The UAE PKI project aimed to develop a comprehensive and intergraded security infrastructure to enable a primary service of confirmed digital identities of UAE ID cardholders on digital networks; primarily on the internet. The program has two strategic objectives: (1) to enable verification of the cardholder's digital identity; (authentication services) by verifying PIN Code, biometric, and signature certificate and (2) to provide credibility (validation services) through the development of a Central Certification Authority. See also Figure 6 below.

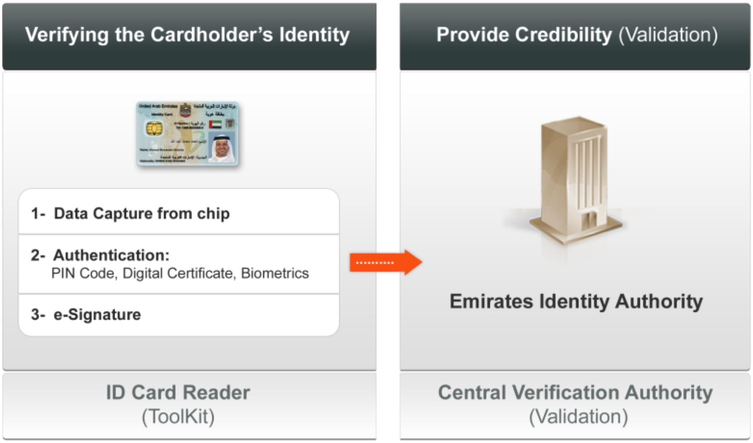

Verifying the Cardholder's Identity
Provide Credibility (Validation)
1- Data Capture from chip
2- Authentication: PIN Code, Digital Certificate, Biometrics
3- e-Signature
Emirates Identity Authority
ID Card Reader (ToolKit)
Central Verification Authority (Validation)

Figure 6: UAE PKI project primary objectives

7.1 Central Certification Authority

The Central Certification Authority, also referred to as the Government Root Certification Authority, is intended to be the highest Certification Authority in the hierarchical structure of the Government Public Key Infrastructure in the UAE. The high level UAE PKI architecture depicted in Figure 7 will encompass a root and multiple certified subordinate CAs' to support own PKI policy and function.

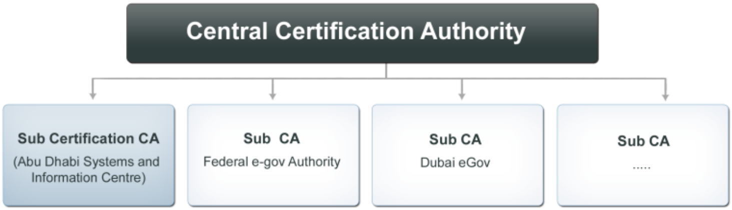


Figure 7: UAE PKI Architecture

The PKI architecture was designed to support two operational models for the implementation of a third party sub CA. In the first option, an eGovernment authority may implement its own CA including the required software and hardware infrastructure. It will rely on the same PKI infrastructure to certify its Public CA using own Root certificate.

This meant that we needed to have a Certificate Authority for the population and a Certificate Authority for the Government. From a technical and interoperability stand point, it made perfect sense that we may have two or more different CAs that function under one Root CA.

The second option assumes that a given eGovernment authority CA is setup as part of the same PKI infrastructure. A virtual partition is implemented on the Population CA. The eGovernment CA will be initialised and configured on this new virtual partition. A virtual key container is created on the HSMs so that the Sub CA key pair and corresponding certificates are separated completely from the Root keys. The solution of this second option is illustrated in the Figure 8 below.

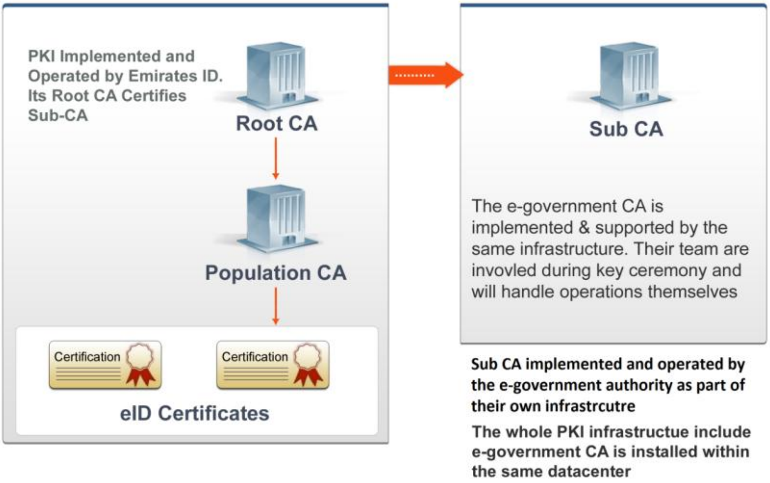

PKI Implemented and Operated by Emirates ID. Its Root CA Certifies Sub-CA
Root CA
Population CA
Certification
Certification
eID Certificates
Sub CA
The e-government CA is implemented & supported by the same infrastructure. Their team are invovled during key ceremony and will handle operations themselves
Sub CA implemented and operated by the e-government authority as part of their own infrastrcutre
The whole PKI infrastructue include e-government CA is installed within the same datacenter

Figure 8: UAE PKI Architecture

Thus a Root CA was setup, and a Population CA underneath it to issue digital certificates to the population. The government priority was to ensure that the population be empowered with the Government issued credentials and to package and store these credentials into a smart card. It was decided to have a modular design approach in place that would enable the roll out of other CAs under the Root CA on demand.

7.2 Online Users Authentication

The above architecture enabled us to meet our strategic objectives of providing digital identity and verifiable credentials to the population of citizens and residents in the country. Verification of the digital certificates was the next function that needed to be addressed. This was achieved in three complementing steps:

1. **Issuance of a smart card with the digital profile in a secure encrypted format:**
   The smart card itself is an advanced 144K combi card that combines the power of contact and contactless technology for card reading functions. The Java OS used in the card is encrypted with keys from the PKI that allow exchange of keys between the card the card reader using advanced secure access module (SAM) cards or hardware security module (HSM).

2. **Development and distribution of a toolkit that enabled service providers to integrate smart card readers with the ability to read the tamper proof encrypted data in the card:**
   The developed toolkit allows service providers to integrate the UAE ID card reading, verification and authentication capabilities with their own legacy applications. Distribution of these toolkits meant that many government departments could now securely establish the identity of the cardholder and deliver critical services to the citizens and residents in lesser time.

3. **Publish a CRL on website and setup an OCSP:**
   The CRL is published diligently on a secure portal on daily basis providing the revocation list. In addition to this, a Positive Certification List (PCL) is also provided, considering the huge number of cards in circulation. In addition to the CRL, the PKI is provided with an OCSP service to enable online real time transactions.

The following diagram provides an overview of the overall UAE PKI Architecture.

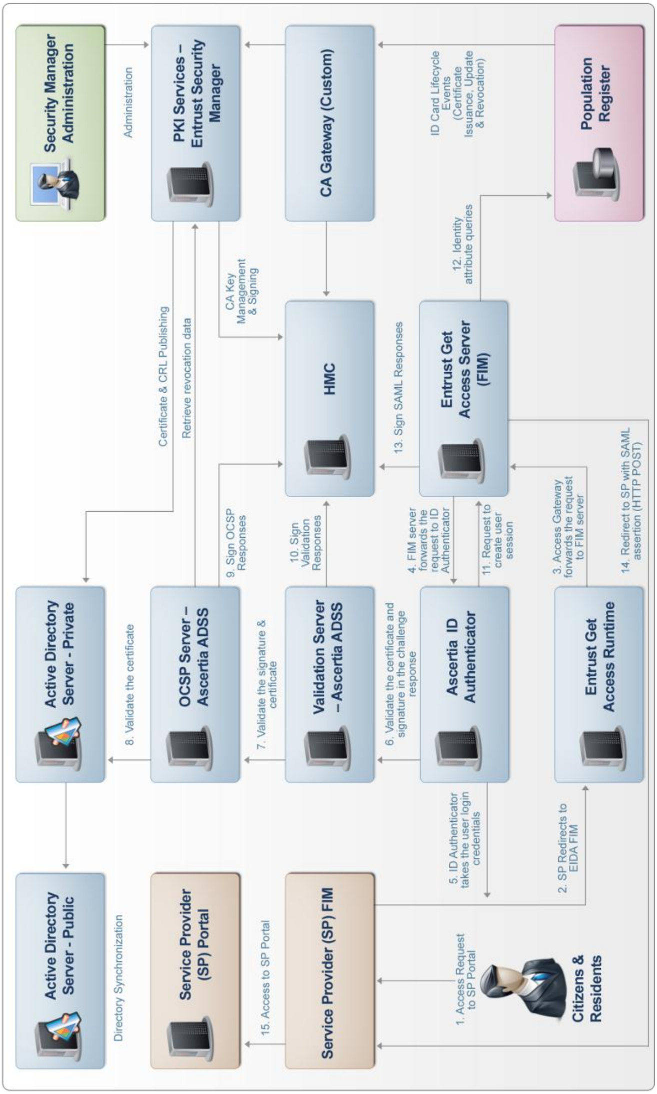

Security Manager Administration
Administration
PKI Services – Entrust Security Manager
CA Gateway (Custom)
ID Card Lifecycle Events (Certificate Issuance, Update & Revocation)
Population Register
Certificate & CRL Publishing
Retrieve revocation data
CA Key Management & Signing
HMC
13. Sign SAML Responses
Entrust Get Access Server (FIM)
12. Identity attribute queries
Active Directory Server - Private
9. Sign OCSP Responses
10. Sign Validation Responses
4. FIM server forwards the request to ID Authenticator
11. Request to create user session
3. Access Gateway forwards the request to FIM server
14. Redirect to SP with SAML assertion (HTTP POST)
8. Validate the certificate
OCSP Server – Ascertia ADSS
7. Validate the signature & certificate
Validation Server – Ascertia ADSS
6. Validate the certificate and signature in the challenge response
Ascertia ID Authenticator
Entrust Get Access Runtime
5. ID Authenticator takes the user login credentials
2. SP Redirects to EIDA FIM
Active Directory Server - Public
Directory Synchronization
Service Provider (SP) Portal
15. Access to SP Portal
Service Provider (SP) FIM
1. Access Request to SP Portal
Citizens & Residents

Figure 9: UAE PKI Deployment Overview

Abu Dhabi e-Government was the first government agency to connect to the national UAE PKI infrastructure. The portal ties in e-Services of nearly 45 local authorities. Most of the G2C services are tied with the UAE ID card some of which require strong user authentication like ID card, biometrics, and chip-based PIN. See also Figure 10.

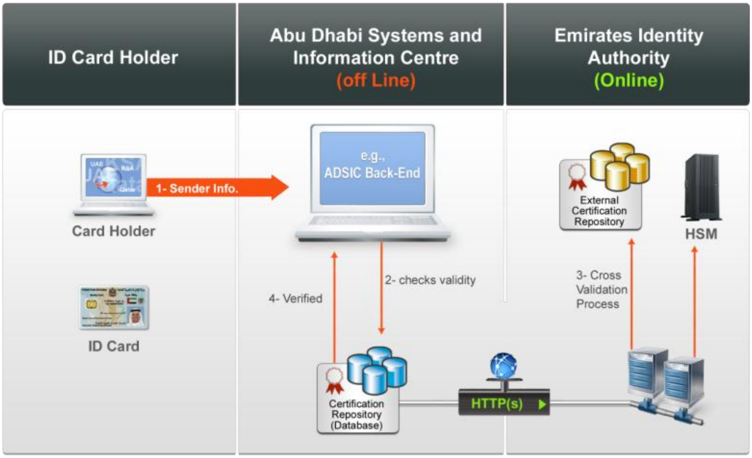

ID Card Holder
Abu Dhabi Systems and Information Centre
(off Line)
Emirates Identity Authority
(Online)
Card Holder
1- Sender Info.
e.g., ADSIC Back-End
ID Card
4- Verified
2- checks validity
Certification Repository (Database)
HTTP(s)
External Certification Repository
HSM
3- Cross Validation Process

Figure 10: PKI Authentication and Validation Workflow

There are six other local e-government authorities and one federal that are planned to get connected to this infrastructure by 2013. The UAE central bank is another entity that is envisaged to be connected as a sub-certification authority who will in turn provide its services to banks and financial institutions in the country to facilitate financial G2C transactions.

The UAE national PKI program is still in its evolution stages and will mature with time. It is expected that by end of 2013, many objectives of the PKI program will be met with G2G, G2C and G2B transactions carried out using the digital signatures and credential verification features of the UAE ID card.

Following the example set by UAE, more countries in the Middle East are moving towards implementing their own national PKI solutions. Moves are afoot in the region to ensure that there is interoperability among the various national ID cards and more specifically been GCC countries[14]. Similar to the European initiative GCC countries are working on developing a common e-identity infrastructure that will enable the authentication of GCC citizens by any service provider at a member state e.g., border control, public services, etc (Al-Khouri and Bechlaghem, 2011).

Having said this, the following section highlights some of the learned lessons and management considerations from the UAE program.

8. MANAGING THE IMPLEMENTATION

The UAE PKI deployment was fraught with issues and challenges. Dynamic scope change that kept changing the project objective was the most serious issue. Functional requirements changed with time as government service providers became more involved during the implementation phases.

More serious was the issue of the project team taking a technical implementation approach rather than a business driven requirement development approach. It took several executive steering meetings to ensure that the technical implementations

[14] GCC is the acronym for Gulf Cooperation Council, also referred to as the Cooperation Council for the Arab States of the Gulf (CCASG). It includes six countries namely, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. The number of GCC population is estimated to be around 40 million people.

morph into business deployments. This was a key learning from our PKI implementation.

Though PKI is a technical platform implementation, it is of no consequence if the technology implemented does not meet the business requirement. Project teams led by technical leaders complicated the implementation and a strong management resolve ensured that the business requirements are kept in sight.

One key business requirement was to ensure that a digital certificate is generated from a request coming from the population register. This meant that the population enrollment and registration process had to be integrated into the technical process of certificate generation.

Another example is related to the perspectives of the different government stakeholders. We had to involve potential government service providers to ensure that there is a smooth on boarding process that would enable these service providers to integrate the ID card into their processes for ID verification. We realised that those government departments did not fully understand integration mechanisms until the later phases of implementation, which impacted and delayed deployment plans. This involved more of a business process integration challenge than technical process integration. Change requests were largely led by technical considerations leading to complex deployment architectures.

9. GCC AND UAE PKI PROGRAM IN REFERENCE TO EUROPEAN LEADERS

The UAE PKI Program, though fundamentally served the same purpose as those implemented elsewhere in the world. Being part of the national identity management program, the UAE PKI program is serving more objectives than one. The PKI is an integral part of the personal profile which includes biometrics stored in the ID card. This proffers major advantages to the service providers to work with multi factor authentication making service delivery across multiple channels easily possible.

On a different note in UAE, the Government has taken the lead to develop and distribute the toolkit for the ID card integration. In Europe, Malaysia and South Korea that are major users of national ID cards and PKI, the toolkit and ID card integration is left to the service and solution providers. Having said this, the next section concludes this article.

In Europe the national ID cards do not generally contain the biometric data, as transactions rely solely on the digital certificates and reduce the service channels to the web. This also affects the authentication mechanism that can be used. PKI for all that it can be, is not an authentication mechanism. Authentication is accorded the use of biometric. This marks a major differentiator in the UAE ID program.

On a different level, the GCC identity interoperability project underway draws many parallels with the European Interoperability

Framework which looks at specifying how administrations, businesses and citizens communicate with each other within and across Member States borders. Several EU Member States have rolled out smartcard based electronic ID (eID) solutions to their citizens. There are good references of national ID card equipped with PKI digital certificates being deployed in Europe with Belgium, Estonia, and Germany, as leading examples.

In general, GCC countries have been evaluating interoperability architecture guidelines and standards issued by the EU, and they still seem to have no one single approach to a possible architecture. However, GCC countries have defined few waves of implementation to facilitate services and identity verification between member states (see also Al-Khouri and Bechlaghem, 2011).

CONCLUSION

Governments around the world have made substantial investments in eGovernment initiatives with the aim to provide better public services to both citizens and businesses. To us, eGovernment involves innovation and transformation of business operating models, to provide significant added value in terms of efficiency and effectiveness of operations.

Nonetheless, Governments efforts have been scattered and were mainly concerned with the development of informational portals and the automation of some of the traditional interactional and transactional services. All this did not support governments to move through the advanced transformational stages of e-Government due to multiple reasons ranging from technical, economical, and political factors. In fact, one of the key barriers to eGovernment progress is lack of effective methods through which trust can be established over digital networks.

We attempted in this article to highlight the role of PKI and advanced identity management systems in addressing this requirement. Public Key Infrastructure has proven itself invaluable in e-Government and e-Commerce environments despite the complexity and associated risks with its large scale deployments. However, the literature do not include sizeable and qualitative reported experiences of PKI implementations in the Government sector.

We attempted in this article to present the case of one of the large scale government PKI deployments in the United Arab Emirates which was implemented part of a national identity management infrastructure development scheme. The national PKI implementation was based on the need to establish binding digital profiles of all population in the country. Combined with the recently issued biometric-based smart ID cards to all population, PKI technology offers advanced capabilities to secure digital transactions and offer multi-factor authentication of online users. The application of PKI is envisioned by the Government of the UAE to strengthen security and public confidence and ultimately ensure the protection of digital identities.

The national identity validation gateway set up in the UAE, is envisaged to support the progress and evolution of e-government in the country. The gateway will provide identity verification services to all public sector organisations and government agencies as well as private sector. This is likely to enable the development of more complex forms of G2C eGovernment and e-commerce business models in the country.

In conclusion, it is our belief that the UAE PKI case presented in this article may constitute a significant lesson for European and other governments. However, further examples of ongoing projects elsewhere in the world are necessary to stimulate a comprehensive understanding and to identifying possible viable alternatives and adjustments to be made for the European context as well as at deepening the understanding of the full range of costs and benefits in financial, political and social terms.

REFERENCES

[1] Al-Khouri, A.M. & Bal, J. (2007a). Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics. Journal of Computer Science, 3(5), 361-367.

[2] Al-Khouri, A.M. & Bal, J.(2007b). Electronic Government in the GCC Countries. International Journal Of Social Sciences, 1(2), 83-98.

[3] Al-Khouri, A.M. (2011). An innovative approach for e-Government Transformation. International Journal of Managing Value and Supply Chains, 2(1), 22-43.

[4] Al-Khouri, A.M. and Bechlaghem, M. (2011). Towards Federated e-Identity Management across GCC – A Solution's framework. Global Journal of Strategies & Governance, 4(1), pp. 30-49.

[5] Basu, S. (2004). e-Government and developing countries: an overview. International Review of Law Computers, 18(1), 109-132.

[6] Baum, C., & Maio, A.D. (2000). Gartner's four phases of e-Government model. Gartner Group Inc., Stamford.

[7] Becker, J., Algermissen, L. and Falk, T. (2011.) Modernizing Processes in Public Administrations: Process Management in the Age of e-Government and New Public Management. Springer.

[8] Bicking, M., Janssen, M. and Wimmer, M.A.(2006). Looking into the future – scenarios for e-Government in 2020. In Soumi, R., Cabral, R., Hampe, J.F., Heikkilä, A., Järveläinen J. and Koskivaara, E.(Eds.) Project eSociety: Building Bricks, NY: Springer Science & Business Media.

[9] Brands, S.A. (2000). Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press.

[10] Broster, D. (2011). Digital Governance Tomorrow: Extrapolation or Discontinuity? Establishing a Dialogue on Identity & Behaviour in a Digital Society. Borderless eGovernment Services for Europeans, 6th European Ministerial eGovernment Conference, Poznan, 17-18 November 2011, retrieved December 12, 2011 from

http://www.egov2011.pl/egov2011/public/main/attachments.html?co=show&instance=12&parent=81&lang=en&id=121

[11] Dutta, S. and Mia, I. (eds.) (2011). The Global Information Technology Report 2010–2011, retrieved December 12, 2011 from http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf.

[12] Ebbers, W. E., Pieterson, W. J. & Noordman, H. N. (2008). Electronic government: Rethinking channel management strategies. Government Information Quarterly, 25, 181-201.

[13] Griffin, D., Trevorrow, P. & Halpin, E. (2007). Introduction e-Government: A welcome Guest or Uninvited Stranger?. In Griffin, D., Trevorrow, P., and Halpin, E., (Eds.) Developments in e-Government - A critical Analysis, Amsterdam: IOS Press.

[14] Heeks, R. (2006). Implementing and Managing e-Government: An International Text, London: Sage Publications Limited.

[15] Schedler, K. and Summermatter, L. (2003). e-Government: What Countries Do and Why: A European Perspective. In Curtin, G.C., Sommer, M.H. & Vis.-Sommer, V. (Eds.)The World of e-Government ,The Haworth Political Press.

[16] Seifert, J.W. (2003). A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance, retrieved December 4, 2011 from http://www.fas.org/sgp/crs/RL31057.pdf

[17] Stavrou, E. (2005). PKI: Looking at the Risks, retrieved July 12, 2011 from http://www.devshed.com/c/a/Security/PKI-Looking-at-the-Risks/

[18] Streib, G. & Navarro, I. (2006). Citizen demand for interactive e-Government: The case of Georgia consumer services. American Review of Public Administration, 36, 288-300.

[19] UK Cabinet Office. (2005). Transformational Government: Enabled by Technology, retrieved December 12, 2011 from http://www.cabinetoffice.gov.uk/media/141734/transgov-strategy.pdf.

[20] UN. (2010). UN E-government Survey – 2010: Leveraging e-government at a time of financial and economic crisis, UNDESA

retrieved December 6, 2011 from http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan038855.pdf.

[21] Wilson, S. (2005). The importance of PKI today. China Communications, Retrieved July 5, 2011 from www.china-cic.org.cn/english/digital%20library/200512/3.pdf.

An Innovative Approach For E-Government Transformation[15]

DR. ALI M. AL-KHOURI

ABSTRACT: Despite the immeasurable investment in e-government initiatives throughout the world, such initiatives have yet to succeed in fully meeting expectations and desired outcomes. A key objective of this research article is to support the government of the UAE in realizing its vision of e-government transformation. It presents an innovative framework to support e-government implementation, which was developed from a practitioner's perspective and based on learnings from numerous e-government practices around the globe. The framework presents an approach to guide governments worldwide, and UAE in particular, to develop a top down strategy and leverage technology in order realize its long term goal of e-government transformation. The study also outlines the potential role of modern national identity schemes in enabling the transformation of traditional identities into digital identities. The work presented in this study is envisaged to

[15] Al-Khouri, A.M. (2011) "An Innovative Approach for e-Government Transformation", **International Journal of Managing Value and Supply Chains**, Vol. 2, No. 1, pp. 22-43.

help bridge the gap between policy makers and implementers, by providing greater clarity and reducing misalignment on key elements of e-government transformation. In the hands of leaders that have a strong will to invest in e-government transformation, the work presented in this study is envisaged to become a powerful tool to communicate and coordinate initiatives, and provide a clear visualization of an integrated approach to e-government transformation.

Key words: *e-Government, Transformation, National ID Schemes.*

1. INTRODUCTION

AMONG the many promises of the Information Communication Technologies (ICT) revolution is its potential to modernise government organisations, strengthen their operations and make them more responsive to the needs of their citizens. Many countries have introduced so-called e-government programmes that incorporate ICT and use it to transform several dimensions of their operations, to create more accessible, transparent, effective, and accountable government [1-3].

In recent years, e-government development has gained significant momentum despite the financial crisis that crippled the world economy [5-6]. For most governments, the recent financial crisis was a wakeup call to become more transparent and efficient [7]. In addition, there is also growing demand for governments to transform from a traditional agency and department centric model to a "Citizen-Centric" model [8-10]. Such a transformation is expected to enhance the quality of life of citizens in terms of greater convenience in availing government services [1] and thereby result in increased customer satisfaction levels and trust in government [11-13].

Government agencies are increasingly embracing Information and Communications Technology (ICT) to boost efficiency and integrate employees, partners and citizens in a seamless manner [14,15]. On the other hand, it is becoming increasingly difficult to achieve these outcomes and meet the needs of the citizens with fragmented e-government initiatives (ibid). Such a situation is forcing many governments to take an integrated approach to improve the effectiveness of delivering services to their citizens [16]. Having closely studied many of the leading e-government programs around the world, some of which have formed dedicated e-government institutions to deliver the desired transformation, we see that very few have succeeded in achieving the outcomes they initially hoped to deliver. This does not mean that the world has not witnessed any e-government initiatives that have succeeded in delivering effective e-services to citizens. Rather we see that most e-government programs have automated and digitized some existing processes rather than transformed government services.

E-government is not just about enabling existing government services on the Internet, but rather is about a re-conceptualization of the services offered by governments, with citizens' expectations at the core of the re-conceptualization. As such, this can only be achieved through vertical and horizontal integration of government systems to enable communications crossing the boundaries of the different government agencies and departments, which should result in a "one stop service centre" concept. The existing body of knowledge is full of strategies, frameworks, and approaches, developed by consulting companies or by academic researchers, however, practitioners in the field of government have been hesitant to accept or fully believe in the practicality of these frameworks.

This research study was particularly developed to provide an analysis of the current e-government status-qua in the United Arab

Emirates and to support the government in pursuing its objective towards e-government transformation. Thus, it offers an innovative framework from a government practitioner's viewpoint and in light of the existing literature in the field.

The recommended framework is an amalgamation of learnings from various e-governments initiatives across the globe. It defines a comprehensive approach addressing technology, strategy and the broader approach to realizing e-government transformation. It proposes many innovative models to support the visualization of numerous dimensions of transformed e-government.

This research article is structured as follows. First, a short literature review on the concept of citizen centricity in e-government applications is provided. Next, some recent statistics on the progress of e-government with focus on the UAE is presented, covering some of the recent efforts of the government of the UAE in terms of its strategy, e-services and distribution, and recent developments. The research and development methodology is outlined thereafter, and subsequently the proposed framework is presented and discussed. The paper concludes with the presentation of some key thoughts and considerations around success factors and improvement opportunities

2. DEPARTMENT CENTRIC TO CITIZEN CENTRIC

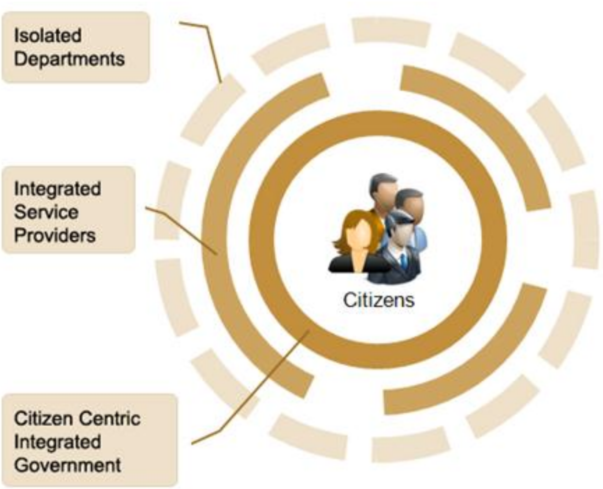

Isolated Departments
Integrated Service Providers
Citizen Centric Integrated Government
Citizens

Figure-1: Stages of e-government transformation

Modern governments are steadily transforming from the traditional department centric model to a citizen centric model for delivering services [8-10,17]. Such a model aims to change the perspective of government constituents, so that they view their government as an integrated entity rather than discrete agencies and departments. However such a transformation has multiple stages.

Figure-1 attempts to depict that a Government consists of various agencies and service providers each of which has many departments offering services to citizens. In a department centric approach, citizen needs to interact with each department separately causing inconvenience and inefficiency. Moreover, any services that requires approvals or intervention of more than one department, would take a long time to deliver. The next stage in the transformation process is the integration at the service provider level where multiple services and departments under a single agency or service provider are integrated to give a single agency feel to the citizens. However, citizens still need to interact with different agencies for different purposes, leading to less transparency and convenience for the citizen. Fully integrated government provides vertical[16] and horizontal[17] cross service providers and cut through various layers of delivery [12]. Government integration results in projecting a single government view to the citizen and allows them to avail services from One-Stop-Shop portals and Service Access Points.

2.1. Characteristics of Citizen Centric E-government

Citizen centric e-government should (or would) enjoy increased trust of citizens and should ensure accountability of government transactions [18]. It should also provide enhanced collaboration among departments and stakeholders, thereby enabling fast decision making and consensus [19]. Citizen centric e-government could also help avoid duplication and overhead through shared services and infrastructure, thereby helping achieve reduced service delivery cost while enhancing customer satisfaction.

Business intelligence gathered via integrated service provision would also enable the government to track the effectiveness of initiatives and schemes and enhance decision making. Citizen

[16] Vertical Integration: This stage initiates the transformation of government services rather than automating its existing processes. It focuses on integrating government functions at different levels, such as those of local governments and state governments.

[17] Horizontal Integration: This stage focuses on integrating different functions from separate systems so as to provide users a unified and seamless service.

centric e-government in its final form would provide improved transparency and consistent user interfaces and convenient channels for citizens to access e-government services [20]. Via the enforcement of strict Service Level Agreements (SLA) with all government entities, government can ensure that citizens get improved responsiveness for their service requests and increased security and privacy, thereby earning their trust when they avail e-services [21]. In addition, these services are also available anywhere, and anytime, breaking the traditional limitations of public sector working hours.

Effective e-government integration would provide opportunities for businesses to provide inputs and to air concerns, increase transparency and a serve to level playing field for service offerings [22]. Businesses should stand to gain from faster clearances of permits and licenses, reduced overhead, improved customer service and verification of customer identities in a fast and reliable manner. The next section will shed light on some recent statistics on e-government progress worldwide, with a specific focus on the progress made by the UAE.

3. E-GOVERNMENT WORLDWIDE AND IN THE REGION

UN agency known as UN Public Administration Network (UNPAN) benchmarks global governments against four key metrics – 'Online Service Index', 'Telecommunication Infrastructure Index', 'E-Participation Index' and 'Human Capital Index'. These indices collectively represent measurements of a nation's readiness in terms of (1) telecommunication infrastructure, (2) maturity of e-services,

(3) participation of citizens in decision making and (4) human resource availability to meet the requirements of offering e-government services. Below are highlights of the most recent UN survey conducted in 2010 [23].

3.1. Un E-Government Survey 2010 Findings

Table-1 above lists the top 10 countries in the UN survey 2010 [see also 24]. As per the UN report these countries have achieved maturity in the transactional stage of e-government. For example The Republic of Korea has consolidated its position in offering transactional e-services and is planning to achieve transformation towards citizen-centric e-government by the year 2012.

Table-2 provides the UN rankings of the top six Middle East countries in terms of their e-government readiness over a 5 year period. Of the six countries listed above, five are from the GCC, with only Jordan being a non GCC Arab country included. Bahrain and the UAE were ranked top two respectively, followed by Kuwait at 3rd, Saudi Arabia at 5th, Qatar at 6th and Oman at 8th. It is also observed that there has been steady progress by Bahrain in the field of e-government.

Between 2008 and 2010, Bahrain has made remarkable progress in terms of improving its UN e-government ranking, jumping 29 points up to rank 13 worldwide after being ranked at 42 in the UN eGovernment Readiness Survey in 2008. Saudi Arabia has also advanced from (70) to (58), and Kuwait from (57) to (50), and Oman from (84) to (82), which is attributed, in general, to these countries further investment in IT infrastructure. On the other hand, the UAE fell 17 points, slipping from 32nd to 49th while Qatar fell by nine ranks, moving from 53rd to 62nd.

Table 1: Top 10 Countries in the UN Survey 2010

Rank	Country	Index
1	Republic of Korea	0.8785
2	United States	0.8510
3	Canada	0.8448
4	United Kingdom	0.8147
5	Netherlands	0.8097
6	Norway	0.8020
7	Denmark	0.7872
8	Australia	0.7864
9	Spain	0.7516
10	France	0.7510

Table 2: UN Ranking of Middle East Countries e-Gov Readiness

Country	2010 Ranking	2008 Ranking	2005 Ranking
Bahrain	13	42	53
UAE	49	32	42
Kuwait	50	57	75
Jordan	51	50	68
Saudi Arabia	58	70	80
Qatar	62	53	62

Though one may view these findings as being a numbers game, the e-government index provides governments the opportunity to look little deeply into their long-term strategy and the short-term policy for quick performance. Overall, the survey pointed out that e-government initiatives in GCC countries have helped underpin regulatory reform, while promoting greater transparency in government. The survey results are hoped to play a key role in enhancing the delivery of public services, enabling governments to respond to a wider range of challenges despite the difficulties in the global economy.

3.2. E-Government Progress In UAE

The UAE has been at the forefront of adopting advanced technologies to improve the efficiency of governance. The visionary leadership of UAE has initiated numerous e-government programs aimed at enabling the government in effective policy making, governance and service delivery. A key focus of the 2011-2013 UAE Government strategy is to improve government services and bring them in line with the international standards, with special emphasis on education, healthcare, judicial and government services. The principles of the UAE e-government strategy are summarized as follows:

- Maintain continuous cooperation between federal and local authorities;
- Revitalize the regulatory and policy making role of the ministries, and improve decision making mechanisms;
- Increase the efficiency of governmental bodies, and upgrade the level of services by focusing on customer needs;
- Develop civil service regulations and human resources, by focusing on competence, effective Emiratization and leadership training;
- Empower Ministries to manage their activities in line with public and joint policies;

- Review and upgrade legislations and regulations

The UAE has been going through various stages of e-government developments. In order to provide a clearer perspective of where the UAE stands against international benchmarks, collectively as a nation and as individual emirates, the below data has been used to provide a common understanding of the status quo. The data samples considered for this exercise are indicative but not exhaustive, and have been compiled based on publicly available information.

3.2.1. E-Services Profile Of UAE

Layne and Lee [25] developed a four-stage process to depict the e-government applications evolvement. These are Information, Interaction, Transaction and Transformation. The first stage embraces the publication of information on websites for citizens seeking knowledge about procedures governing the delivery of different services. The second stage involves interactivity where citizens can download applications for receiving services.

The third stage involves electronic delivery of documents. The fourth stage involves electronic delivery of services where more than one department may be involved in processing a service request or service.

The following chart (Figure-2) depicts a summary of the status of various services in the UAE as benchmarked against the commonly used stages of e-government i.e., Information, Interaction, Transaction and Transformation. From the above data, it is evident that collectively as a nation, the UAE government e-services are at the 'Information' stage and there is an equal distribution of e-Services between 'Interaction' and 'Transaction' stages. The important observation to be noted is that there is bigger challenge of inter-agency integration (Ready, 2004), which is the key to achieving 'Citizen-Centric' e-government.

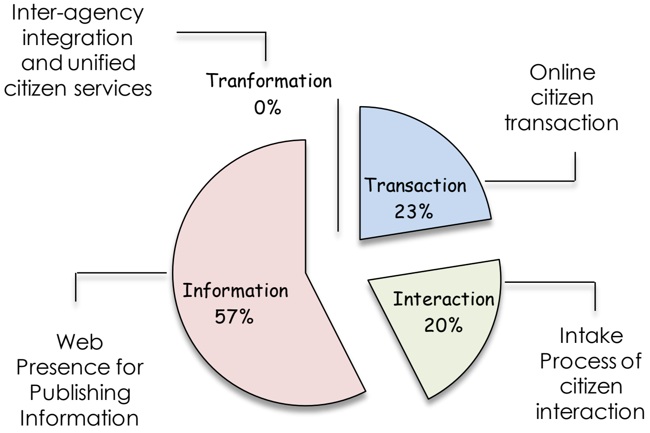


Figure-2: UAE e-government profile summary

Note: Figures are based on limited sample of publicly available information and is only indicative

3.2.2. E-Services Distribution Across Emirates

Having seen the overall e-government status across UAE, the following Figure-3 shows the distribution of government e-services across each emirate. From the graph it is evident that the e-government initiatives in Abu Dhabi and Dubai are more advanced than the other emirates and have the foundation for providing citizen-centric services. Based on this foundation there is growing momentum at the federal level to move towards shared services and increased integration.

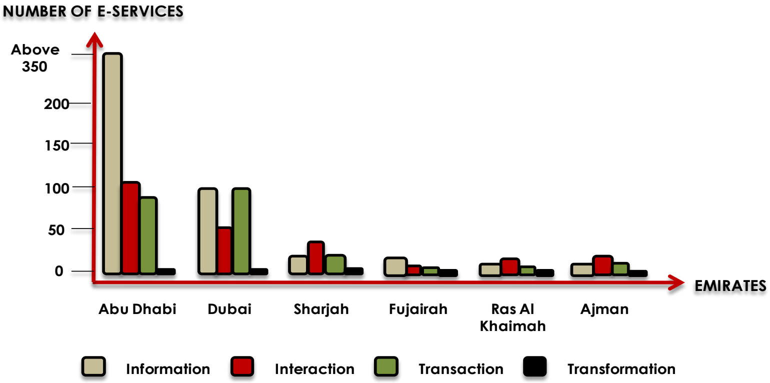
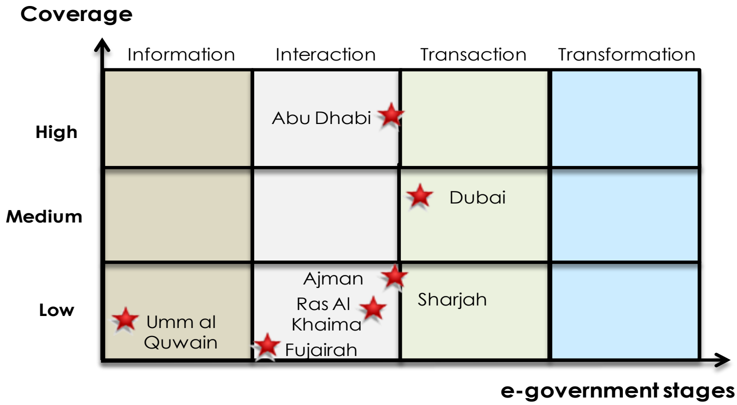


Figure-3: E-services distribution across Emirates

Note: Figures are based on limited sample of publically available information and is only indicative. The figure are high in Abu Dhabi is because most of the federal ministries are based in Abu Dhabi.

3.2.2. Current Stage Of UAE In E-Government Evolution



	Information	Interaction	Transaction	Transformation
High		Abu Dhabi		
Medium			Dubai	
Low	Umm al Quwain	Ajman Ras Al Khaima Fujairah	Sharjah	

Note: e-government stage across the UAE is observed to be transitioning from interaction to transaction.

Figure-4: e-Government stages across UAE

Figure-4 illustrates the stage of each emirate in the UAE and the evolution of e-government in each. Combining the observations made so far, we can infer that the UAE as a nation is in the transition stage from Interaction to Transaction. While service coverage (i.e., number of services) is higher in Abu Dhabi, Dubai has made more progress towards implementation of transactional services. The UAE government has been making resolute and strong progress towards laying the fundamental infrastructure needed to enable the e-government environment. The UAE has one of the highest quality broadband connections in the world, according to findings by the University of Oxford [26].

According to a recent research published by the Economist Intelligence Unit, the UAE was found to be leading the Middle East region in terms of its continued and steady improvement in broadband, mobile and Internet connectivity levels [27]. See also Figure-5. On the other hand, the UAE is now considered to have the highest rates of fibre optic[18] penetration in the world, according to research carried out by IDATE on behalf of the FTTH Council Europe Middle East Working Group [28]. The UAE is ranked fourth in the world, with 30.8 per cent of the country's households and businesses connected to fibre optic systems, behind Japan, South Korea and Hong Kong. The UAE is described as representing 96% of the Middle East region's FTTH/H subscribers and 76% of all homes passed by fibre.

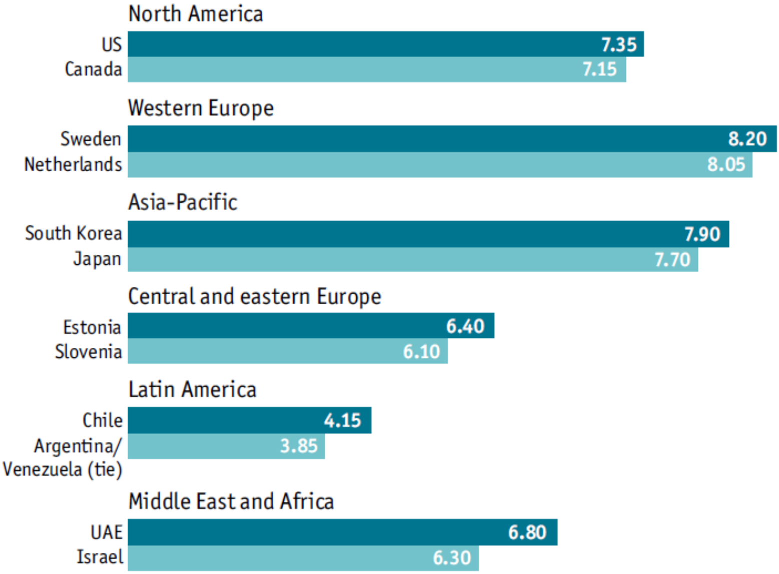


Figure -5: Regional digital economy rankings leaders: connectivity and technology infrastructure [27]

[18] Fibre optic connections enable almost unlimited volumes of digital data to be transmitted using pulses of light. The technology is replacing traditional copper wiring for broadband internet networks.

3.2.4. E-Government And The National Identity Management Infrastructure

To meet the growing need to integrate citizens into e-government initiatives, the smart citizen ID card initiatives adopted by many countries are meant to provide reliable methods for identifying and authenticating citizens availing e-services. An earlier research study in which the author participated and published in 2007 indicated that if essential components are integrated with such systems, such programs have the potential to address key challenges facing e-government initiatives, specifically those related to G2C [29-30].

The new National Identity Card Scheme rolled out in the UAE in 2005 is one of the largest federal government programs in the country to provide a cost effective, multi-functional, robust and secure national identity management infrastructure. The program is considered to mark a major milestone in the development of e-government; allowing citizens to authenticate themselves in an easy and comprehensively secure and electronic way whenever they access e-government applications.

The government announced recently the kickoff of a Public Key Infrastructure (PKI) and a Federated Identity Management (FIM) project to complement the existing identity management infrastructure and provide extended services to federal and local e-government authorities in the UAE [31]. The project aims to develop a comprehensive and integrated security infrastructure to enable a primary service of confirmed digital identities of UAE ID card holders on digital networks; primarily on the internet. The project has two strategic objectives: (1) to enable verification of the cardholder's digital identity; (authentication services) by verifying PIN, biometric, and signature and (2) provide credibility (validation services) through the development of a Central Certification Authority.

PKI is regarded as a crucial component to provide higher security levels in digital forms, and may have a multiplier effect if integrated with the existing government trusted identity management systems. To support and enhance this capability many folds, this research study puts forward an innovative framework, referred to here as CIVIC IDEA, an abbreviation for "Citizen Inclusive Vision realized through ID Card Integrated Delivery of E-government Applications."

The approach is envisaged to support the government of the UAE in achieving its vision of e-government transformation, while leveraging the strengths of the UAE national ID card initiative i.e., building upon the capabilities provided by the new smart ID card relating to the authentication capabilities of individuals over digital networks. The following section will shed light on the research and development methodology, and the proposed framework is discussed afterwards.

4. RESEARCH AND DEVELOPMENT METHODOLOGY

This research is more qualitative than quantitative in nature, although it relies on extensive analysis of case studies related to federal e-Government strategies through literature review. The analysis involved mapping of the federal e-Government strategies and the countries ranking in the overall e-Government index of UN survey with focus on the United Arab Emirates. This provided some thoughts related to what strategies could yield more successful results to enhance the UAE's position in the UN rankings. The study tried to balance the intensity of data collection of the case studies. Too many constructs could have led to a complex framework. Inadequate volume of data or sparse variation on the other hand might have failed to capture the whole picture in its entirety.

The researchers were aware of these potential risks and worked to avoid them. Components and layout of the framework have converged from accumulated evidence (qualitative data). Gradually, a generic framework began to emerge. The researchers also compared the emergent framework with evidence collected from the multiple cases one at a time. We continued this iterative process until the data corroborated well the evolving framework.

Finally, we consulted literature for contradiction or agreement. In many cases this helped form more perspectives. The following formatting rules must be followed strictly. This (.doc) document may be used as a template for papers prepared using Microsoft Word. Papers not conforming to these requirements may not be published in the conference proceedings.

5. PROPOSED FRAMEWORK

From the extensive literature review conducted and the analysis of the UN e-government survey reports, it was amply clear that the political leadership and e-government leaders need simpler and effective tools for visualizing and conveying the strategies. Based on this need, this study was focused on developing simplified models and tools for understanding and managing e-government initiatives. These models design containing key information resembles the issues and challenges faced by e-government initiatives that can then become the focal point around which decisions for business change and/or improvement of operations are made.

Curtis [32] identified five different components that need to be considered in a modelling effort: (1) facilitation of human understanding and communication, (2) support for process improvement, (3) support for process management, (4) automated guidance in performing a process, and (5) automated execution support. Given our stated scope in this research study, the first three objectives are addressed.

This research paper also attempted to model a suitable technology centric approach to support decision makers in UAE and realize the vision of e-government transformation. The proposed framework was developed based on revisions of various international practices already carried out in the area of citizen-centric e-government initiatives.

We refer to the framework here as CIVIC IDEA, an abbreviation for "Citizen Inclusive Vision realized through ID Card Integrated Delivery of E-government Applications." The approach is envisaged to support the government of the UAE in achieving its vision of e-government transformation, while leveraging the strengths of the

UAE national ID card initiative. Figure-6 summarizes the different components of the framework, each of which will be discussed in the following sections.

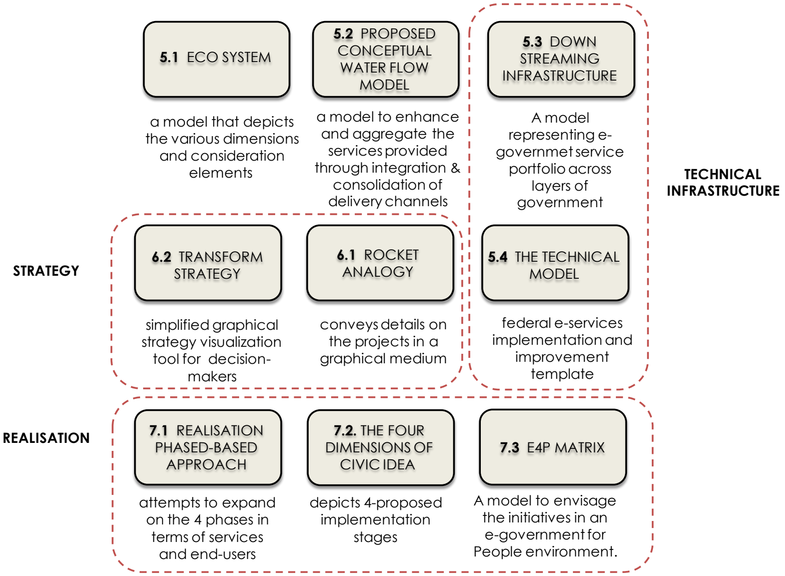

5.1 ECO SYSTEM
a model that depicts the various dimensions and consideration elements
5.2 PROPOSED CONCEPTUAL WATER FLOW MODEL
a model to enhance and aggregate the services provided through integration & consolidation of delivery channels
5.3 DOWN STREAMING INFRASTRUCTURE
A model representing e-governmet service portfolio across layers of government
TECHNICAL INFRASTRUCTURE
STRATEGY
6.2 TRANSFORM STRATEGY
simplified graphical strategy visualization tool for decision-makers
6.1 ROCKET ANALOGY
conveys details on the projects in a graphical medium
5.4 THE TECHNICAL MODEL
federal e-services implementation and improvement template
REALISATION
7.1 REALISATION PHASED-BASED APPROACH
attempts to expand on the 4 phases in terms of services and end-users
7.2. THE FOUR DIMENSIONS OF CIVIC IDEA
depicts 4-proposed implementation stages
7.3 E4P MATRIX
A model to envisage the initiatives in an e-government for People environment.

Figure-6: CIVIC IDEA Framework Components

5.1. CIVIC IDEA Ecosystem

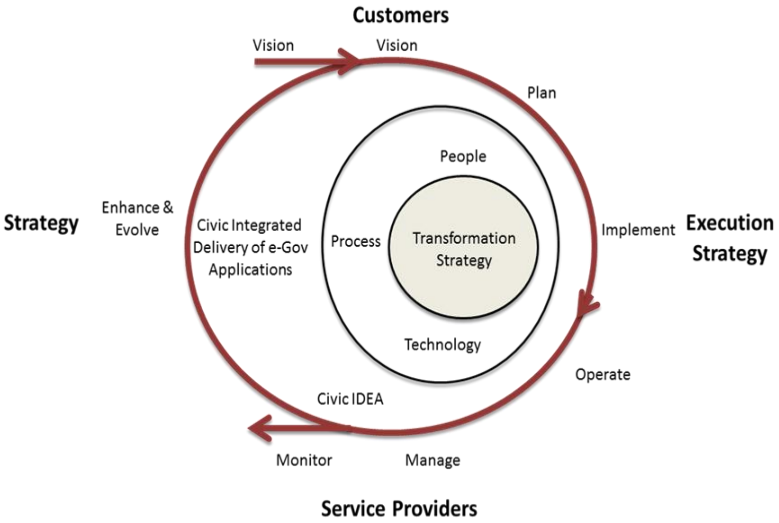


Figure-7: CIVIC IDEA Ecosystem

In an eco system of e-government, strategy and execution are equally critical. Therefore the challenge lies more in collective execution, taking into consideration the dimensions of people, processes and technology towards building an effective and integrated delivery of e-government applications. The following diagram (Figure-7) depicts the overall ecosystem for the CIVIC IDEA concept.

In the diagram, we can see two sets of dimensions. The first dimension maps strategy versus execution. The key message of the above visualization is that both strategy and its execution are equally important and that neither a good strategy implemented poorly, nor a poor strategy implemented well, serves the overall objectives of e-government transformation. The other dimension in the above diagram maps service providers versus their customers. As with the former dimension, the key message of the latter dimension is also that both elements are equally important, in that innovation of new services without convenient delivery channels and tools for customer interactions, are as good as having no e-services to offer your customers. At the core of the eco system, is the transformation strategy, addressing the key elements of people, process and technology and its outer layer is comprised of citizen centric e-government applications implemented based on this new strategy.

The evolution of the ecosystem consists of defining a new vision, goals, plan for the implementation of the plan, post implementation operations of the solution, monitoring of service usage and finally, the evolution of services based on the new requirements. Having explained the eco system, we will now delve into the conceptual models that form the foundation for CIVIC IDEA realization.

5.2. Conceptual Model

While attempting to build the solution models, it is important to have a conceptual foundation that conveys the various components of the solution. In doing so, we envisage e-government through a water flow model. In such a model, the overarching federal e-government strategy needs to be comprehended by federal and local agencies who will in turn translate these strategies into e-services for the citizens.

Figure-8 illustrates the proposed conceptual model for e-government. The assumption here is that the execution based on this conceptual model will help enhance and aggregate the services offered by the service providers through integration and consolidation. Such a transformation will also require a strong focus on delivery channels to allow services to be taken to the door steps (or fingertips) of citizens.

Such a transformation would also require an increase in citizen capabilities to consume these services and enjoy their benefits. During this entire process, the government need to obtain feedback and input, in the form of Business Intelligence (BI), thereby enabling the government to fine tune its policies and strategies. Service down-streaming is one of the important foundations of CIVIC IDEA. The e-government service portfolio of the UAE consists of various layers and specializations and these services are constantly refined. However, in order to achieve uniformity across the various layers of government, it is important to have a standardized federal service template which acts as the blueprint for the implementation and improvement of e-services. See also Figure-9.

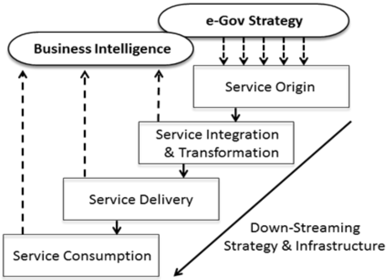


Figure-8: proposed conceptual model for e-government

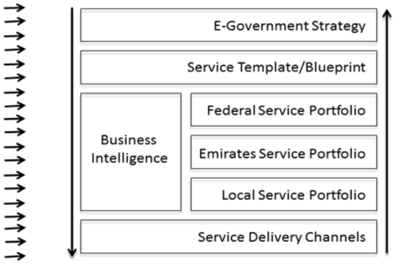

E-Government Strategy
Service Template/Blueprint
Business Intelligence
Federal Service Portfolio
Emirates Service Portfolio
Local Service Portfolio
Service Delivery Channels

Figure-9: the "Down Streaming" infrastructure

In our opinion, successful realization of CIVIC IDEA depends on the down streaming of infrastructure and standardized service templates. These service templates would act as the blueprint for the service portfolio at federal, emirate and local levels to standardize the types of services offered. As the service template allows specialization and fine-tuning at each level, a service gets refined as it passes through many levels of specialization before it reaches the end customer via distinct delivery channels.

5.3. CIVIC IDEA Technical Model

The translation of the above conceptual model into the enterprise architecture is the next step in the CIVIC IDEA realization. The development of the model took the following entities as primary design elements:

1. Service Providers
2. Support Service Providers
3. Existing E-Gov Systems
4. CIVIC IDEA Infrastructure ●
    - 4.1 Core Platform
    - 4.2 Integration Channels
    - 4.3 Delivery Channels
5. Front Ending Organizations
6. End Customers

Figure-10 presents the enterprise level integrated view of the CIVIC IDEA in the context of the UAE. This model envisages the technological requirements of realizing the "Down Streaming" infrastructure in the conceptual framework discussed earlier. In the following sub-sections, we will elaborate and explain the main components of the proposed CIVIC IDEA infrastructure platform.

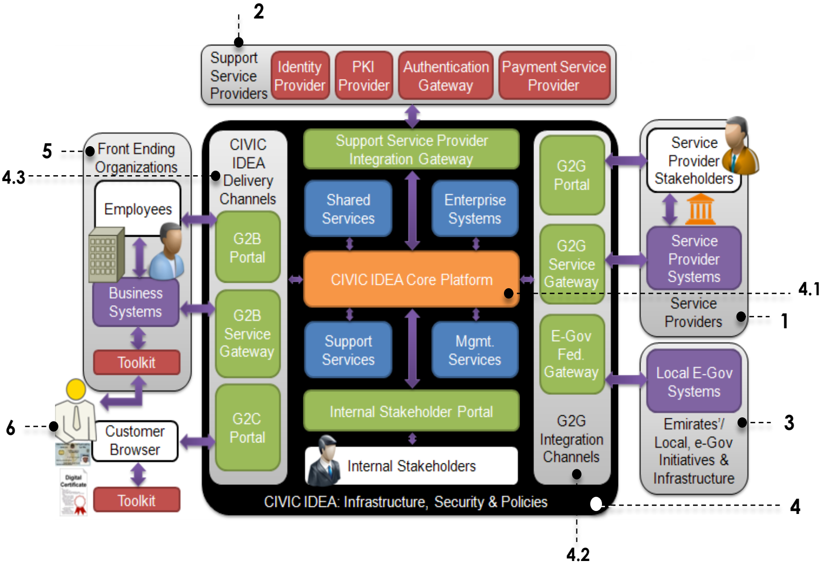


Figure-10: Enterprise level integrated view of the CIVIC IDEA

5.3.1. CIVIC IDEA Core Platform

A key intention of the CIVIC IDEA platform is to enable faster and seamless integration of service providers and delivery channels. The core platform for this is envisaged to be built around a Service Oriented Architecture[19] (SOA) that leverages cloud computing[20] and virtualization[21] technologies. This would ensure the scalability

[19] Service Oriented Architecture is a flexible set of design principles used during the phases of systems development and integration to support communications between services. A system based on a SOA architecture will package functionality as a suite of interoperable services that can be used within multiple separate systems from several business domains.

[20] Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service.

[21] Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources. There are

and cost effectiveness of such a transformation. SOA technologies such as Enterprise Service Bus[22] (ESB) and enterprise messaging framework[23] can enable large scale integrations and communication in a standard manner. The entry points into the CIVIC IDEA platform are through standardized integration gateways and portals (highlighted in **green** in Figure-10).

Such architecture would leverage reliable asynchronous messaging between service providers and the platform, whereby the synchronous real-time communication is used to ensure responsiveness. There are four categories of services (highlighted in **blue** in Figure-10) built on top of the CIVIC IDEA platform to facilitate the service integration and management, which are discussed in the following sections.

5.3.2. Shared Services

Shared services are value added services that can be leveraged by the service providers to achieve inter agency collaboration. Examples of shared services are audit, alert and workflow management.

three areas of IT where virtualization is making headroads, network virtualization, storage virtualization and server virtualization. Virtualization can be viewed as part of an overall trend in enterprise IT that includes autonomic computing, a scenario in which the IT environment will be able to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed. The usual goal of virtualization is to centralize administrative tasks while improving scalability and workloads.

[22] Enterprise Service Bus is a software architecture construct which provides fundamental services for more complex architectures.

[23] Enterprise messaging framework is a set of published Enterprise-wide standards that allows organizations to send semantically precise messages between computer systems. They promote loosely coupled architectures that allow changes in the formats of messages to have minimum impact on message subscribers. EMS systems are facilitated by the use of XML messaging, SOAP and web services.

5.3.3. Enterprise Systems

The platform is envisaged to use Enterprise Systems such as directories, databases, email and storage servers as its back-end.

5.3.4. Support Services

Following are the support services (highlighted in **red** in Figure-10) that would be leveraged by the CIVIC IDEA platform:

- Identity Services from identity providers such as Emirates Identity Authority to identity attribute queries;
- Public Key Infrastructure Services from nationally recognized Certificate Authorities, for certificate based authentication and digital signatures;
- Authentication Gateway services for authenticating the users transacting through CIVIC IDEA; and
- Payment Service Providers for processing fees for receipt of services.

Currently, there are many initiatives in the UAE for each of these support services and the platform that can be leveraged in the transformation process.

5.3.5. Management Services

Management services help to publish services from various service providers, monitor their usage and effectiveness, define and manage business processes, in addition to gaining valuable Business Intelligence (BI).

5.4. Standards

CIVIC IDEA assumes that the core platform should be benchmarked against global standards to ensure high degree of interoperability with open systems and commercial off the shelf (COTS) components. In general, e-government specifications must be developed based on an open integration platform and to facilitate the unification of interrelated business systems from providing applications development, operating infrastructure middleware to the application platform. Thus, and in order to meet the evolving needs of e-government, we need to use technologies complying with international technical standards in terms of policies and frameworks that facilitates interoperability between different systems. Some of the relevant and common standards are listed in Table-3 below.

Table-3: International standards

Platform Component	**Standards**
Architectural standards	• Service Oriented Architecture (SOA) • Enterprise Integration Patterns like Enterprise Service Bus (ESB)
Technology standards	• Enterprise Messaging (JMS) • Web services, Federation, SAML, XACML, UDDI, etc.
Process standards	• Business Process Execution Language (BPEL), bXML, OASIS DSS.
Communication & Protocols	• SOAP, HTTPS, IPv6, etc.
Security Standards	• SSL v3, PKI, etc.

The following section introduces an interesting framework developed as a part of this study, with the aim of graphically representing an overarching e-government strategy.

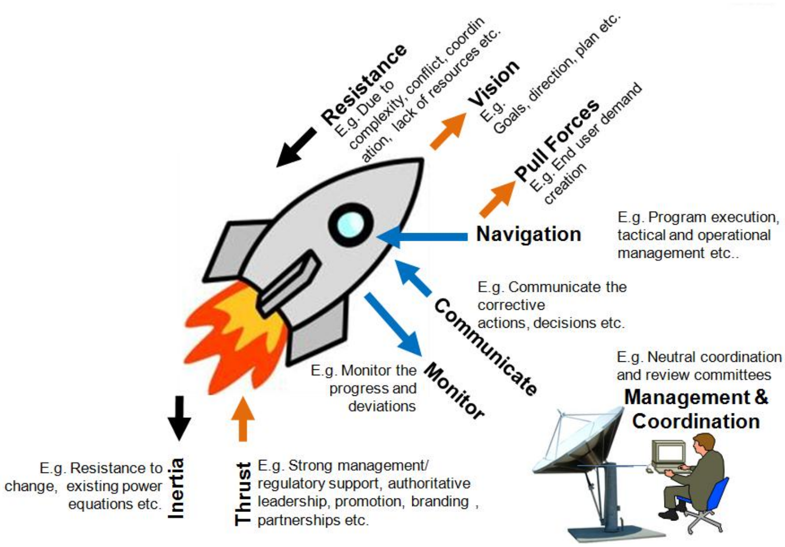
6. CIVIC IDEA: STRATEGY

The process of adopting advanced ICT solutions for the transformation of e-government faces many challenges. Due to the complex nature of these projects and the sheer number of stakeholder's involved, effective visualization and management of such initiatives is highly critical but needs to be simple in order to accelerate understanding off and buy in into the framework. However it is important that the framework represent all important aspects of the e-government strategy. That said, despite years of governmental efforts to implement e-government initiatives, there are no commonly established methods and frameworks for the visualization of an overarching e-government strategy.

A comprehensive framework needs to account for how the different supporting and impeding forces impacting projects being implemented as a part of such a strategy. Given that such a framework will also have a long lifecycle and encompass a broad scope, the framework also needs to remain applicable regardless of changes in the environment. As most projects go through many iterations of technical and process changes, any changes within the ecosystem should not risk the validity of the strategy framework. Hence the framework needs to be adaptable to changing environments and should be defined in a technology neutral manner. Such an approach will also allow the framework to act as the bridge between decision makers and implementers, thus reducing the mismatch between the expected versus realized outcomes.

6.1. Rocket Analogy

A good analogy which is well understood by key decision makers can convey more information than lengthy text based description (see also Figure-11).


Resistance
E.g. Due to complexity, conflict, coordin ation, lack of resources etc.
Vision
E.g. Goals, direction, plan etc.
Pull Forces
E.g. End user demand creation
Navigation
E.g. Program execution, tactical and operational management etc..
E.g. Communicate the corrective actions, decisions etc.
Communicate
E.g. Monitor the progress and deviations
Monitor
E.g. Neutral coordination and review committees
Management & Coordination
E.g. Resistance to change, existing power equations etc.
Inertia
Thrust
E.g. Strong management/ regulatory support, authoritative leadership, promotion, branding , partnerships etc.

Figures-11: Rocket Analogy

However it is important to note that an analogy cannot replace the formal definition of a strategy, but can only be used as a means of easily conveying the key messages. Primarily the analogy selected should be able to convey maximum details about the project being considered through a graphical medium so as to save time as well as enable better coordination and reduce ambiguity. Looking at the below diagram we can identify the forces that act on the rocket. Inertia is an opposing force that is commonly encountered in a project requiring change. In order to overcome inertia, one needs to apply heavy thrust till the rocket (project) gains significant momentum. Once in motion (execution) the rocket faces continuous opposing forces which though not as strong as the inertia, can still slow down the projects or take it off course. These resistances can be in the form of coordination issues, technical issues, lack of standards, etc.

For a rocket to overcome these opposing forces, thrust must be applied. The thrust can come as a push from the management or pull from the customer side. During the course of flight there is a need to continuously monitor the flight path to detect any deviations. These deviations once identified need to be communicated to the rocket navigation system to take controlling actions.

6.2. TRANSFORM Strategy

From the analogy described above, we derived a model that maps to the e-government domain artifacts and problem statements. This model named as Thrust, Resistance And Navigation Strategy Form or in short as **TRANSFORM** is illustrated in Figure-12. Such graphical visualization of the strategy is likely to be beneficial to decision makers, as it provides a non-technical visualization. It provides a simplified yet a comprehensive conceptualization of what e-government strategy is all about. Table-4 provides a short highlight on each of the key focus areas within the TRANSFORM strategy.

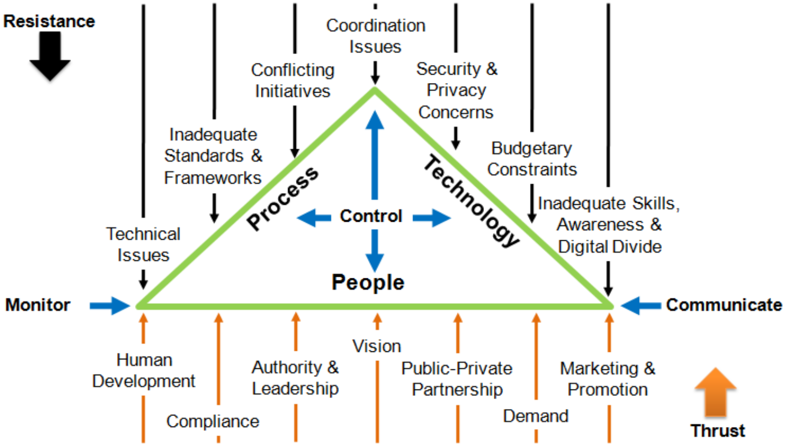


Figure-12: TRSNAFORM Strategy

Table 4: Major Resistances and Thrust areas in e-Government

Resistance	Thrust:
Coordination Issues: Variations in legal, regulatory and administrative regimes on different sides of these boundaries can inhibit and block the flow of information and services.	Vision: quantifiable strategic outcomes, periodic reviews and progress assessment.
Budgetary Constraints: Difficultly in quantifying and measuring the cost/benefits of e-government initiatives.	Authority and Leadership: lack of authority and leadership
Digital Divide: Social and economic divides – demarcated by wealth, age, gender, disability, language, culture, geographical location, size of business and other factors.	Demand: lack of perceived benefits resulting in inadequate motivation for citizens to avail e-government services.
Security and Privacy Concerns:security and privacy individual's data and the risk of information and identity theft	Public Private Partnership: poor definition of policies enabling such partnerships
Technical Issues & Inadequate	Human Development: Inadequate

Standards: inappropriate user interfaces to e-government systems and interoperability issues.	skilled resources
Resistance to Change: inadequate staff skills, lack of training and investment in enhancement of ICT knowledge and the fear of change.	Marketing and Promotion: Lack of marketing and branding strategies to gain wide visibility, recognition and demand.
Conflicting Initiatives: competition between initiatives to achieve similar outcomes.	Compliance: lack of common standards, agreed procedures and methodologies, e.g., legal and regulatory policies and guidelines as well as technical and operational standards

To understand how we propose to define the navigation strategy for our framework, let us first revisit Figure-7, which illustrates an e-government project as an ecosystem of people, processes and technologies. These three components work in close coordination in the implementation of any project. To ensure their alignment with common goals and meeting defined performance criteria, it is a common practice to have an independent review committee which periodically monitors and reviews the progress of each project.

Observations from such reviews can then be communicated to the project leadership to enact specific controls to implement any necessary corrections and re-alignment. The proposed TRANSFORM strategy framework presented here is a visual tool that represents the e-government projects in a technology neutral and abstract manner, using an analogy that is widely familiar and simple. This should enable strategic decision makers in seeing through the challenges faced by the initiatives and provide them with the necessary thrust needed to overcome their challenges. This can also greatly bridge the gap between policy makers and implementers, as a common representation of the projects resulting in higher clarity and reduced misalignment.

7. CIVIC IDEA: Realization Approach

The earlier sections in this study discussed the models and strategy for the realization of the proposed framework of CIVIC IDEA. However such large scale transformation cannot be achieved in one go and needs to be deployed in phases, with each phase initiated based on the successful achievement of outcomes in earlier phases.

7.1. Stages of CIVIC IDEA Realization

There are four key stages to realizing CIVIC IDEA. The following diagram (Figure-13) depicts four key focus areas to drive through the four phases, with each phase trying to expand the coverage in terms of services and end users. In summary, the enable phase is more of a preparatory phase where the foundation for transformation is laid. The enhance phase is used to develop blue prints, standards and basic infrastructure. Having created the basic infrastructure, smart projects are initiated in the establish phase with the aim of gaining wider support, increasing visibility and creating demand. All through the first three phases, the overall strategy gets refined and is now ready for expansion to reach maximum coverage.

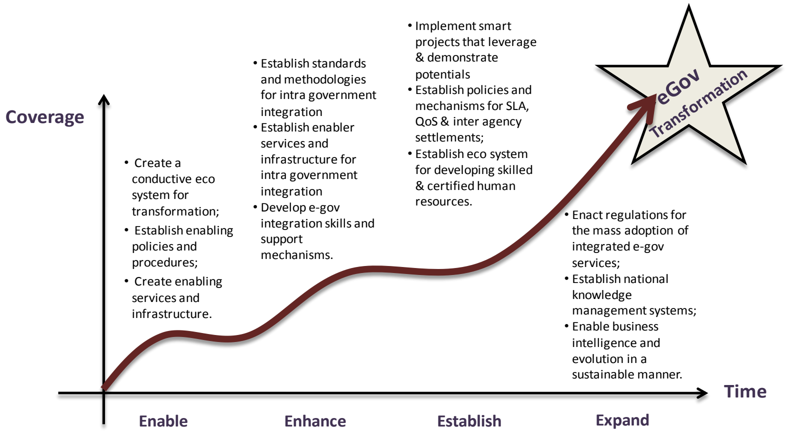

Coverage
• Create a conductive eco system for transformation;
• Establish enabling policies and procedures;
• Create enabling services and infrastructure.
• Establish standards and methodologies for intra government integration
• Establish enabler services and infrastructure for intra government integration
• Develop e-gov integration skills and support mechanisms.
• Implement smart projects that leverage & demonstrate potentials
• Establish policies and mechanisms for SLA, QoS & inter agency settlements;
• Establish eco system for developing skilled & certified human resources.
eGov Transformation
• Enact regulations for the mass adoption of integrated e-gov services;
• Establish national knowledge management systems;
• Enable business intelligence and evolution in a sustainable manner.
Time
Enable
Enhance
Establish
Expand

Figure -13: Driving through CIVIC IDEA

7.2. Dimensions of CIVIC IDEA

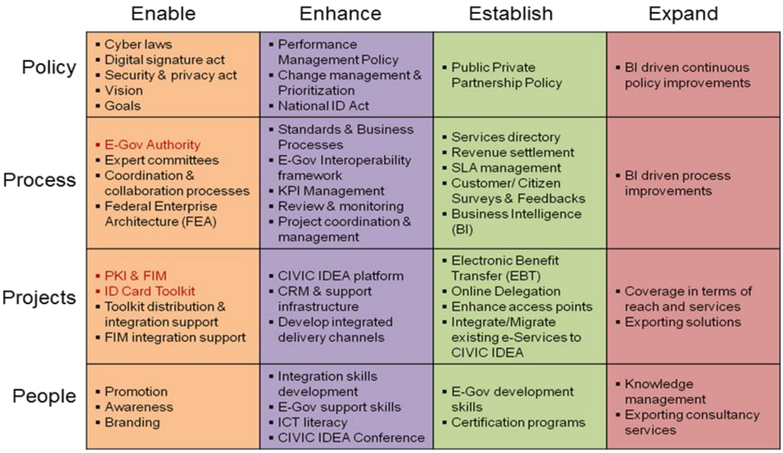
The stages in the CIVIC IDEA realization define the stages in the timeline. The following diagram (Table-5) lists the four dimensions of CIVIC IDEA with core focuses. At each of the stages, we need to achieve higher maturity in each dimension of Policies, Processes, Projects and People.

Table 5: The four dimensions of CIVIC IDEA

Policies	Processes
• e-Gov authority and leadership; • regulatory acts and laws towards enforcement; • public private partnership.	• Standards & guidelines; • Reviews & coordination mechanisms; • Project management & PKI monitoring.
• Projects	• People
• Specific project covering the areas of infrastructure building, solutions, communications, delivery channels, service access points, supporting mechanisms, etc.	• Human resource development towards e-Gov resources; • Awareness, promotion, marketing, branding.

7.3. Profile of Initiatives

Based on the realization stages and dimensions we then arrive at a model to envisage the initiatives in an E4P (this also represents E-government for People) matrix which is shown in Figure-14 below.



	Enable	Enhance	Establish	Expand
Policy	▪ Cyber laws ▪ Digital signature act ▪ Security & privacy act ▪ Vision ▪ Goals	▪ Performance Management Policy ▪ Change management & Prioritization ▪ National ID Act	▪ Public Private Partnership Policy	▪ BI driven continuous policy improvements
Process	▪ E-Gov Authority ▪ Expert committees ▪ Coordination & collaboration processes ▪ Federal Enterprise Architecture (FEA)	▪ Standards & Business Processes ▪ E-Gov Interoperability framework ▪ KPI Management ▪ Review & monitoring ▪ Project coordination & management	▪ Services directory ▪ Revenue settlement ▪ SLA management ▪ Customer/ Citizen Surveys & Feedbacks ▪ Business Intelligence (BI)	▪ BI driven process improvements
Projects	▪ PKI & FIM ▪ ID Card Toolkit ▪ Toolkit distribution & integration support ▪ FIM integration support	▪ CIVIC IDEA platform ▪ CRM & support infrastructure ▪ Develop integrated delivery channels	▪ Electronic Benefit Transfer (EBT) ▪ Online Delegation ▪ Enhance access points ▪ Integrate/Migrate existing e-Services to CIVIC IDEA	▪ Coverage in terms of reach and services ▪ Exporting solutions
People	▪ Promotion ▪ Awareness ▪ Branding	▪ Integration skills development ▪ E-Gov support skills ▪ ICT literacy ▪ CIVIC IDEA Conference	▪ E-Gov development skills ▪ Certification programs	▪ Knowledge management ▪ Exporting consultancy services

* The initiatives highlighted in red are already undertaken by UAE.

Figure-14: The e-government for people matrix

8. Key thoughts and considerations

Having presented the proposed framework, this section outlines some key thoughts, considerations and recommendations for practitioners in the field of e-government. Together they are meant to raise awareness, aid the building of resilient plans, and enable the "endogenization" of institutions and the creation of a favorable implementation environment.

8.1. Key Success Factors of Citizen Centric E-government

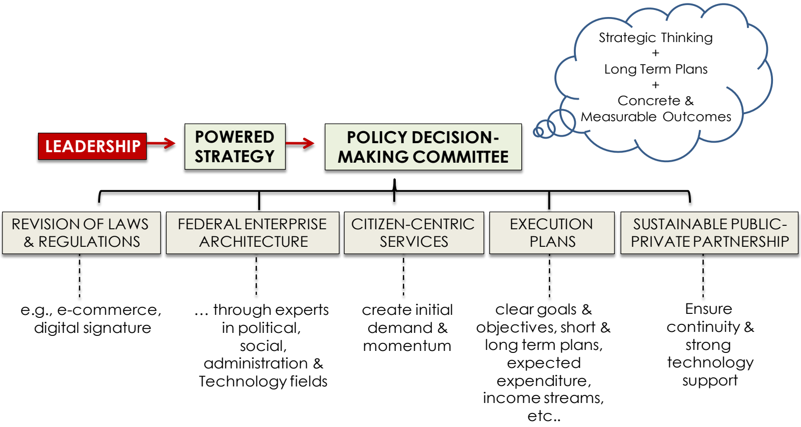

Strategic Thinking
+
Long Term Plans
+
Concrete &
Measurable Outcomes
LEADERSHIP
POWERED STRATEGY
POLICY DECISION-MAKING COMMITTEE
REVISION OF LAWS & REGULATIONS
FEDERAL ENTERPRISE ARCHITECTURE
CITIZEN-CENTRIC SERVICES
EXECUTION PLANS
SUSTAINABLE PUBLIC-PRIVATE PARTNERSHIP
e.g., e-commerce, digital signature
… through experts in political, social, administration & Technology fields
create initial demand & momentum
clear goals & objectives, short & long term plans, expected expenditure, income streams, etc..
Ensure continuity & strong technology support

Figure-15: Key success factors for citizen centric e-government

Success of citizen centric government depends on many factors as depicted in Figure 15. Primarily, strong e-government leadership is essential for uniform and centralized decision making on e-government initiatives [33]. Such an approach should consist of a high powered strategy and policy decision making committee with strategic thinking and sustainable long term plans.

These plans should encompass aligned e-government projects, each having concrete and measurable outcomes. E-government leadership should also be enabled by revision of laws and regulations e.g. e-commerce and digital signature acts, in line with government process reforms [34-36]. Adoption of federal enterprise architecture arrived at with the help of experts in political, social, administration and technology fields, is also vital to the success of e-government initiatives [35,37-38]. Engaging in these activities would provide the necessary direction and structured thinking necessary to launch programs that complement one another in achieving national goals.

On the flip side, citizen demand for e-government services is essential for the success of e-government initiatives. Hence e-government initiatives should ensure citizen centric e-services which can be accessed through convenient channels of delivery. Governments need to look at ways to create the initial demand and momentum, through services that delivers direct benefit to citizens. Such services can be in the field of health, education, social affairs (e.g. subsidies and pension) etc. where the citizen can see a tangible benefit which in turn spurs demand for e-services.

E-government projects and programs should be performance oriented with measurable outcomes [39-41]. Clear goals, objectives, short and long-term plans, with expected expenditure, income streams and deadlines are some of the attributes that should be defined for such projects [42] and performance criteria should include both qualitative and quantitative measures.

Sustenance is the last word in e-government. Hence e-government leadership should provide an ecosystem for sustainable public private partnership, which is revenue generating and evolving to ensure continuity and strong technology support for the envisaged initiatives. That all said, the following sub-section presents some key thoughts around improvement opportunities in the field of e-government in the United Arab Emirates.

8.2. Key Improvement Areas for UAE

Branding is an important aspect of the UAE's e-government strategy that needs further attention. Though the UAE has undertaken numerous steps in the field of e-government, its efforts needs to be documented in a consolidated knowledge base and disseminated via for example presentations at international conferences and publications in leading industry journals. Such steps would allow the UAE to gain broader visibility for its work, increased opportunities for peer reviews and in turn feedback and input from experts in this field. Another area for improvement is Service Coverage.

There is an imminent need to create integrated and shared services that would demonstrate the potential of transformed government and thus leads to demand creation. Coverage should ensure that all services within each line of businesses are covered and that there is also coverage across lines of business. Another dimension that should be addressed here is the inclusiveness of access to ensure that all the stakeholders are uniformly covered.

There is also a need to consolidate e-government initiatives and increase focus on enhancing quality of life. This could be achieved through provision of convenient access channels that are accessible around the clock or via personalized e-government portals. Such changes will help accelerate citizen usage of government services as citizens will now be able to access services via fast and convenient methods and via reduced effort and time investment.

A prerequisite for such uniform access to e-services would be unified identification and authentication. Having implemented a smartcard based national identity scheme, UAE should leverage it as a medium for citizen identification and for citizens to access all the aforementioned e-services. However, successful realization of unified e-government initiatives needs resources and capacity building. The UN e-government index highlights the lack of skilled manpower to implement and operate technology intensive e-government initiatives. A prerequisite is the requirement for technology literacy among citizens, so as to maximize the benefits off and fully leverage e-government services. E-government efforts result in tremendous knowledge creation and consolidation and require centralized coordination and management so that all stakeholders can access and leverage the insights and experiences of one another. Having said this, the next section concludes this research report.

CONCLUSIONS

Governments around the world have pursed e-government programs seeking to electronically govern internal and external operations and to provide coherence between the various administrative government units so that they work to complement and complete each other. However, and despite the fact that many governments have injected substantial investments, most e-government initiatives in our view have not delivered the transformation environment sought from their implementation. This research study was developed to support the United Arab Emirates in pursuing its objective towards e-government transformation.

It presented an innovative framework developed from a government practitioner's viewpoint and in light of the existing literature in the field. The recommended approach is an amalgamation of learnings from various e-governments initiatives across the globe. The presented framework in this research study was particularly designed to support decision makers and present them with key information and focus areas in e-government initiatives. The framework proposed incorporates some significant conceptual models to enhance leadership understanding and their ability to respond to challenges. It defines a comprehensive approach addressing technology, strategy and the broader approach to realizing e-government transformation. It proposes many innovative models to support the visualization of numerous dimensions of transformed e-government. In the hands of strong e-government leadership, this is envisaged to act as a powerful tool to communicate and coordinate initiatives.

Assessment of the success of this proposed framework was beyond the scope of this research study. Certainly, further research and application is needed to examine the practicality of the proposed framework and its components and the mechanics by which it may be practiced. Last but not least, the maturity of e-government requires significant efforts by both practitioners and researchers to support the development of horizontal and vertical e-government integration. From this standpoint, this research study attempted to make a contribution in this critical and imperative area of knowledge and practice.

ACKNOWLEDGEMENTS

The work presented in this study is an extension to a previous research study published in the Journal of Computer Science and Network Security, under the title: "A strategy framework for the risk assessment and mitigation for large e-Government project." Vol. 10 No. 10, November 2010. The author would like to thank Mr. Dennis DeWilde and Mr. Adeel Kheiri from Oliver Wyman for their feedback on this study, and their assistance in improving the overall structure and quality of the article.

REFERENCES

[1] Atkinson, R.D. and Castro, D. (2008) "Digital Quality of Life," The Information Technology and Innovation Foundation, pp. 137–145.

[2] Mälkiä, M., Anttiroiko, A. and Savolainen, R. (eds.) (2004) E-Transformation in Governance: New Directions in Government. Hershey, PA: Idea Group Publishing.

[3] Melville, A. (2007) "E-Government and Organisational Transformation: Lessons Learnt from Liverpool and Hertfordshire," New Local Government Network. June 7.

[4] Martin, G. (2009) "Government's Response to Financial Crisis will Change the Role of the Public Sector Around the World," Deloitte Touche Tohmatsu [Online]. Available from: https://www.deloitte.com/vie-w/en_G-X/global/press/global-press-releases-en/06ab63ec49101210VgnVCM100000ba42f00aRCR-D.htm. Accessed [4 October 2010].

[5] OECD (2009) Report on the Impact of Financial Crisis on e-Government in OECD Countries. 5th Ministerial eGovernment Conference, 19-20 November – Malmö, Sweden, Available from: http://www.oecd.org/dataoecd/57/57/44089570.pdf.

[6] Stoica, O. (2010) "Implementing e-government with financial constraints", The Network of Institutes ad Schools of Pubic Administration in Central and Eastern Europe [Online]. Available from:http://www.nispa.org/_portal/files/conferences/2010/papers/201004221034060.StoicaOvidiu.doc [Accessed 3 July 2010].

[7] Lapsley, I. (2010) "New Public Management in the Global Financial Crisis-Dead, Alive, or Born Again?" UK: University of Edinburgh Business School.

[8] Abhichandani, T. (2008) Evaluation of E-Government Initiatives for Citizen-Centric Delivery: Analysis of Online Public Transit Information Services. Germany: VDM Verlag Publishing.

[9] Chhabra, S. and Kumar, M. (2009) Integrating E-business Models for Government Solutions: Citizen-Centric Service Oriented Methodologies and Processes. Hershey, PA, USA: Information Science Reference.

[10] Hewson, W., Jones, R., Hunter, D. and Meekings, A. (2004) Towards a Citizen-centric Authority: Beyond CRM, E-Government and the Modernising Agenda in the UK Public Sector. UK: Hewson Consulting Group.

[11] Bimber, B. (1999) "The Internet and citizen communication with government: Does the medium matter?" Political Communication, Vol. 16, pp. 409-428.

[12] Curtain, G.G., Sommer, M.H. and Vis-Sommer, V. (2004) The World of E-Government. New York: Haworth Press.

[13] Tubtimhin, J. and Pipe, R. (2009) Global e-Governance: Advancing e-Governance through Innovation and Leadership, Volume 2 Global E-Governance Series. IOS Press.

[14] Mansell, R. (2002) Inside the Communication Revolution: Evolving Patterns of Social and Technical Interaction. Oxford, UK: Oxford University Press.

[15] Wilhelm, A.G. (2004) Digital Nation: Toward an Inclusive Information Society. Cambridge, MA: The MIT Press.

[16] Nixon, P.G., Koutrakou, V.N. and Rawal, R. (eds) (2010) Understanding E-Government in Europe: Issues and Challenges. London: Routledge.

[17] Shapiro, A.L. (1999) The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know. New York: Century Foundation.

[18] Gronlund, A. (2002) Electronic Government: Design, Applications and Management. Hershey, PA: Idea Group Publishing.

[19] Garson, D.G. (1999) Information Technology and Computer Applications in Public Administration: Issues and Trends. London: Idea Group Publishing.

[20] Kamarck, E.C. and Nye, J.S. (eds.) (2002) Governance.Com: Democracy in the Information Age, Visions of Governance in the 21st Century. Washington, D.C.: Brookings Institution Press.

[21] Mitrakas, A., Hengeveld, P., Polemi, D. and Gamper, J. (2007) Secure E-Government Web Services. Hershey, PA: Idea Group Publishing.

[22] Mendes, M.J. and Suomi, R. Passos, C. (eds.) (2004) Digital Communities in a Networked Society: E-Commerce, E-Business, and E-Government: The Third IFIP Conference on E-Commerce, E-Business, and E-Government, International Federation for Information Processing (Series), Kluwer Academic Publishers.

[23] UN (2010) "UN E-government Survey – 2010: Leveraging e-government at a time of financial and economic crisis", UNDESA [Online]. Available from: http://unpan1.un.org/intradoc/groups/public/doc-uments/un-dpadm/unpan038855.pdf. [Accessed 2 April 2010].

[24] UN (2008) "UN E-government Survey – 2008: From E-government to Connected Governance", UNDESA [Online]. Available from: http://unpan1.un.org/intradoc/groups/public/documents/un/un-pan028607.pdf [Accessed 2 April 2010].

[25] Layne, K. and Lee, J.W. (2001) "Developing Fully Functional E-Government: A Four Stage Model," Government Information Quarterly, vol. 2, pp.122-36.

[26] Fu, W. and Jain, S. (2009) "Global Broadband Quality Study Shows Progress," Saïd Business School, Oxford University, UK. [Online]. Available from: http://www.sbs.ox.ac.uk/newsandevents/Docu-ments/BQS%202009%20final.pdf [Accessed 1 December 2010].

[27] EIU (2010) "Digital economy rankings 2010, Beyond e-readiness," Economist Intelligence Unit [Online]. Available from: http://graphics.eiu.com/upload/EIU_Digital_economy_rankings_2010_FINAL_WEB.pdf [Accessed 1 December 2010].

[28] http://www.ftthcouncil.eu/documents/studies/FTTHCE_AnnualReport_2009-2010.pdf

[29] Al-Khouri, A.M. and Bal, J. (2007) "Digital identities and the promise of the technology trio: PKI, smart cards, and biometrics", Journal of Computer Science, Vol.3, No. 5, pp.361-367.

[30] Al-Khouri, A.M. and Bal, J. (2007) "Electronic Government in GCC Countries", International Journal Of Social Sciences, Vol. 1, No. 2, pp.83-98.

[31] Duncan, W. & Al-Khouri, A.M. (2010) "Supporting e-Government in the United Arab Emirates," Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

[32] Curtis, W., Kellner, M.I. and Over, J. (1992) "Process Modelling". Communications of the ACM, 35, 9, pp. 75-90.

[33] Drucker, P. (2003) The New Realities. New Brunswick, U.S.A.:Transaction Publishers.

[34] Boyle, J. (1997) Shamans, Software & Spleens: Law and the Construction of the Information Society. USA: Harvard University Press.

[35] Eifert, M., Püschel, J.O. (eds.) (2004) National Electronic Government: Comparing Governance Structures in Multi-Layer Administrations. London: Routledge.

[36] Prins, J.E.J., Eifert, M.M., Girot, C., Groothuis, M. and Voermans, W.J.M. (eds.) (2002) E-Government and Its Implications for Administrative Law - Regulatory Initiatives in France, Germany, Norway and the United States. The Hague: T.M.C. Asser Press.

[37] Garson, G.D. (2006) Public Information Technology and E-Governance: Managing the Virtual State. London: Jones & Bartlett Publishers.

[38] West, D.M. (2007) Digital Government: Technology and Public Sector Performance. Princeton,. NJ; Oxford: Princeton University Press.

[39] Anheier, H.K. (2004) Civil Society: Measurement, Evaluation, Policy. London: Earthscan Publications.

[40] Kaylor, C., Deshazo, R. and Van Eck, D. (2001) "Gauging e-government: A report on implementing services among American cities", Government Information Quarterly, Vol. 18, pp. 293–307.

[41] Shark, A.R. and Toporkoff, S. (2010) Beyond eGovernment - Measuring Performance: A Global Perspective. Washington, DC.: Public Technology Institute and ITEMS International.

[42] Gore, A. (1993) From Red Tape to Results: Creating a Government that Works Better & Costs Less: The Report of the National Performance Review. New York: Plume.

PKI In Government Identity Management Systems[24]

DR. ALI M. AL-KHOURI

ABSTRACT: The purpose of this article is to provide an overview of the PKI project initiated part of the UAE national ID card program. It primarily shows the operational model of the PKI implementation that is indented to integrate the federal government identity management infrastructure with e-government initiatives owners in the country. It also explicates the agreed structure of the major components in relation to key stakeholders; represented by federal and local e-government authorities, financial institutions, and other organizations in both public and private sectors. The content of this article is believed to clarify some of the misconceptions about PKI implementation in national ID schemes, and explain how the project is envisaged to encourage the diffusion of e-government services in the United Arab Emirates. The study concludes that governments in the Middle East region have the trust in PKI technology to support their e-government services and expanding outreach and population trust, if of course accompanied by comprehensive digital laws and policies.

Key words: *E-government, E-service, PKI, Identity Management, ID Card.*

[24] Al-Khouri, A.M. (2011) "PKI in Government Identity Management Systems", **International Journal of Network Security & Its Applications**, Vol.3, No.3, pp. 69-96.

1. INTRODUCTION

MANY Many countries around the world have invested momentously in the development and implementation of e-government initiatives in the last decade. As of today, more and more countries are showing strong preference to develop "the 24-hour authority" [1] and the delivery of further self-service models via digital networks [2]. However, from a citizens angle, and although individuals with higher levels of education are in general more open to using online interactions, there is a stronger preference among the majority for traditional access channels like in person or telephone-based interactions with government and private organisations, [2,3].

Our research shows that governments in most parts of the world have been challenged in gaining citizen engagement in the G2C transactions. Our earlier study pointed to the fact that e-government initiatives around the world have not succeeded to go to the third and forth phases of e-government development [4,5] (see also Figure 1). In this earlier study, we referred to the need of fundamental infrastructure development in order to gaining the trust of citizens, and hence expanding outreach and accelerating e-government diffusion. One of the key components we highlighted there was the development and integration of a government identity management system with PKI technology to enable stronger authentication of online users.

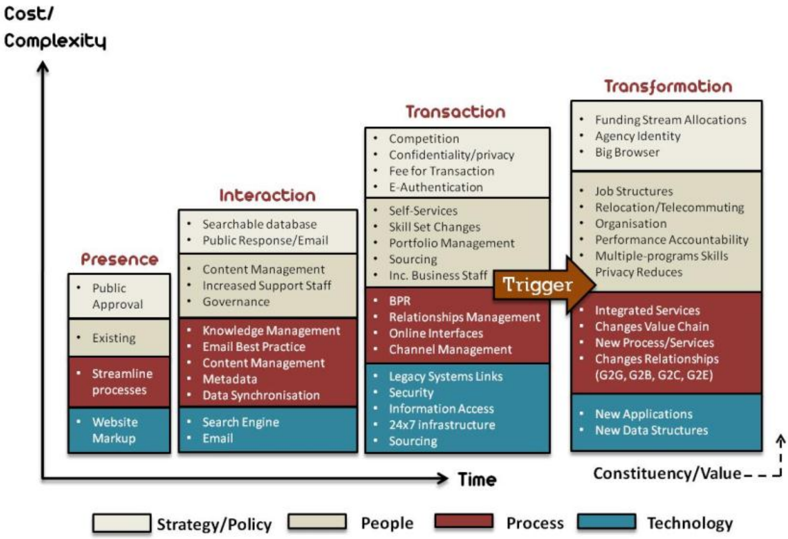


Figure 1. Four Phases of e-Government – [6]

The purpose of this article is to describe the UAE government approach of incorporating PKI into their ID card architecture. It explains the major components of the project related to e-government G2C progress. In doing so, we seek to make a contribution to the available research literature on the implementation of PKI in national identity management systems, and its role in the diffusion of e-government and outreach. This article is structured as follows. Some background introduction on PKI is provided first. The UAE PKI project is introduced next, and a highlight is provided on its major components. Some reflection is provided on key management considerations, before the paper is concluded.

2. DIGITAL IDENTITIES AND PKI IN E-GOVERNMENT

For the past ten years, governments around the world have been vitally concerned with the establishment of secure forms of identification and improved identity management systems, in order to ascertain the true identities and legitimacy of their population. Yet, many organizations both in public and private sectors still rely heavily on their own constructed models of relevant online identities, which are based on captured data from single or multiple sources and transforming them into own data structures within their information systems.

With the revolution of digital networks, governments are realizing their roles to develop foundational infrastructure for digital identities. The term "digital identity" refers to a set of attributes and properties about an individual that are associated together and available in an electronic form to construct trusted digital credentials.

Evidently, governments have long played an authoritative role in identity provision in the physical world, and are now faced with demands to establish digital societies and identities in order to support e-government and e-commerce initiatives. It is the role of the government to associate digital identities to specific persons who will be authorised to perform certain actions in physical or digital forms.

This association is facilitated through digital certificates and digital signatures that altogether construct the digital identity [7]. Thus many governments have considered PKI technology to establish and implement this binding through registration and digital certificate issuance process. In basic terms, PKI attaches identities to digital certificates for the purpose of assured, verifiable, and secure digital communications.

Table 1. Basic PKI Components

Component	Description
Digital Certificates	Electronic credentials, consisting of public keys, which are used to sign and encrypt data. Digital certificates provide the foundation of a PKI.
Certification Authoritie(S) – CAs	Trusted entities or services that issue digital certificates. When multiple CAs are used, they are typically arranged in a carefully prescribed order and perform specialised tasks, such as issuing certificates to subordinate CAs or issuing certificates to users.
Certificate Policy and Practice Statements	Documents that outline how the CA and its certificates are to be used, the degree of trust that can be placed in there certificates, legal liabilities if the trust is broken, and so on.
Certificate Repositories	A directory of services or other location where certificates are stored and published.
Certificate Revocation Lists (CRL)	List of certificates that have been revoked before reaching the scheduled expiration date.

Public key infrastructure commonly referred to as PKI is an Information Technology (IT) infrastructure and is a term used to describe the laws, policies, procedures, standards, and software that regulate and control secure operations of information exchange based on public and private keys cryptography [8]. Table 1 summarizes the primary elements that make up the PKI components. The term PKI is used in this article to refer to the comprehensive set of measures needed to enable the verification and authentication of the validity of each party involved in an electronic transaction.

PKI offers high levels of authentication of online users, encryption and digital signatures , which also support the maintenance of elevated echelons of data privacy, streamline workflow and enable access. The cornerstone of the PKI is the concept of private keys to encrypt or digitally sign information. One of the most significant contributions a PKI has to offer is non-repudiation. Non-repudiation guarantees that the parties involved in a transaction or communication cannot later on deny their participation.

PKI, in general, has grown both more slowly and in somewhat different ways than were anticipated [7]. It has had some success stories in government implementations; the largest PKI implementation to date is the Defense Information Systems Agency (DISA) PKI infrastructure for the Common Access Cards program [9]. See Also Appendix-1. Many researchers pointed out the complexity of PKI, and that it is only sound in theoretical terms [10].

We definitely do not agree with those who claim that PKI cannot be practiced and yield effective results. As with any technology, PKI is not without its own security risks due to its complex architectures. Indeed, there is no bullet-proof technology that could provide us with a fault free solution and meet all of our security needs.

In fact, studies conducted by academics and practitioners remain passionate about the promises of PKI to revolutionise electronic transactions (see for example: [4,5,8,11]. Undoubtedly, published studies in the existing literature contributed significantly to the development of the technology and explaining its benefits. Nonetheless, those studies are believed to remain very much handy to technical researchers.

This is to say that although an awful lot of articles were written on this topic, they seem to be written to improve and develop theoretical frameworks while others tackle narrowed technological issues. See for example: [12-22].

Looking at these studies, we note that although such research efforts have been comprehensive in specific areas, they do not assume a standard or a uniformed PKI approach. Interestingly, some researchers pointed to the fact that this field lacks fundamental theories to guide the development of clear path for PKI practice in our world [23].

Others explain lack of adoption and wide failures in PKI industry to be due to not having enough PKI applications with clear business cases to support the roll out of the infrastructure [24]. Therefore, many implementations reported to have produced unnecessary costs when implemented without clear business cases [25]. Apparently, with the increasing complexity, the implementation of PKI systems becomes extremely challenging in light of the limited documented experiences that have included inefficient and short living implementations, with no clear ROI cases.

3. MOTIVATION AND EXPECTED CONTRIBUTION OF THE WORK

In the age of supercomputing, secure communication is becoming a need and a necessity. PKI is being recognized as an important security component in digital infrastructures to support authentication, integrity, confidentiality, and non-repudiation. Organisations that deployed PKI have reported substantial economic savings [26]. Although PKI is reported to gaining wide popularity, it is still implemented in its very basic form and protocols e.g., secure sockets layers are the most common application of PKI. From our perspective, existing literature still does not explain important implementation areas for practitioners in the field.

This article was developed to provide insights of PKI implementation in a government context and from a practitioner viewpoint. Our main motivation is to explain how PKI could be diffused in modern national identity management systems to outline and address appropriate security requirements. Our contributions are related to a PKI implementation model from one of the most pioneering governments in technology adoption in the Middle East.

We believe that PKI deployment can evolve double the speed if adopted and owned by governments as trusted third parties. See also [27]. The role of the trusted third parties would be to verify the identities of the parties wishing to engage in a secure online communication. PKI, particularly in combination with smart ID cards, can provide robust user authentication and strong digital signatures.

Existing PKI deployments have limited customers. The use of PKI in ID card schemes for example, would enjoy larger customer base. It is our belief that such systems have the potential to raise the awareness of both governments and citizens trust levels in electronic transactions with such advanced technologies. These technologies are thought to pave the way for government transformation from service delivery perspectives and introduce new communication and service delivery channels that should replace government traditional physical counter interactions.

Successful PKI implementation cases would put higher pressures on both government officials and private sector to develop killer applications to revolutinsie public service sectors. In brief, this article does not intend to explain detailed implementation questions, although it can serve as a primer for government officials and researchers who are interested in PKI implementations in government sectors.

4. THE UAE PKI PROJECT

Emirates Identity Authority [28] is implementing PKI and a Federated Identity Management (FIM) solution to complement the existing identity management infrastructure and provide extended services to federal and local e-government authorities in the UAE. The project aims to develop a comprehensive and intergraded security infrastructure to enable a primary service of confirmed digital identities of UAE ID card holders on digital networks; primarily on the internet.

The project has two strategic objectives: (1) to enable verification of the cardholder's digital identity; (authentication services) by verifying PIN Code, biometric, and signature certificate and (2) provide credibility (validation services) through the development of a Central Certification Authority. See also Figure 2 below.

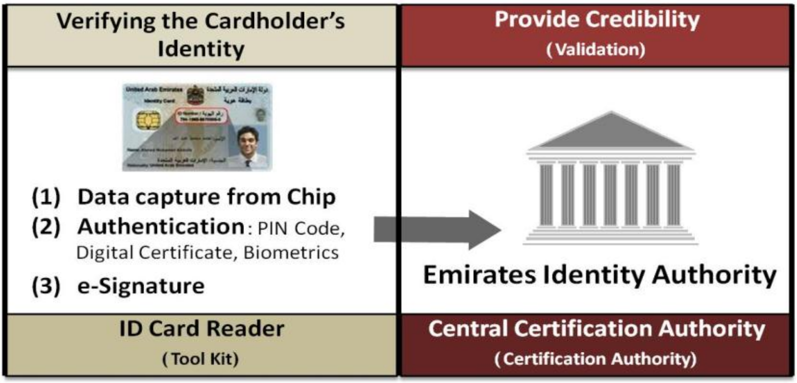

Verifying the Cardholder's Identity
Provide Credibility
(Validation)
(1) Data capture from Chip
(2) Authentication: PIN Code, Digital Certificate, Biometrics
(3) e-Signature
Emirates Identity Authority
ID Card Reader
(Tool Kit)
Central Certification Authority
(Certification Authority)

Figure 2. UAE PKI project primary objectives

The PKI project will support the issuance of identity, digital signature and encryption certificates as well as key recovery for private keys associated with encryption certificates. It will also issue different types of certificates to support the requirements of other business sectors and communities. An example of such custom certificates is attribute (role-based) certificates used for example by e-government, healthcare and justice sectors who may require their own role-based access control and administration such as the management of CA permissions, performing specific CA tasks, etc.

Apart from issuing and managing digital certificates, the PKI project will enable business applications to use certificates by making available the proper means to validate PKI-based transactions. It will provide high levels of security infrastructure having the service integrity and assurances required to support the distribution and verification of public key certificates.

We attempt to outline the three main components of the UAE Identity Management Infrastructure project related to G2C e-government:

(1) issuance of smart cards as means to users authentication capability;

(2) card readers and toolkit dissemination to enable smart card applications; and

(3) the development of central certification authority to provide online validation services.

These are discussed next.

4.1. Smart Cards and Online Users Authentication

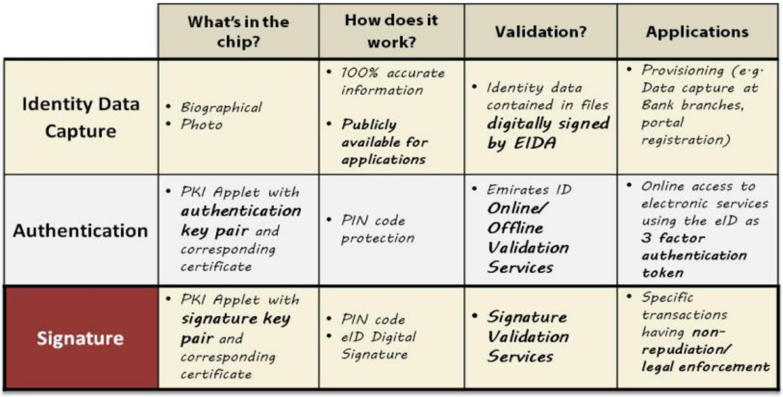
Authentication is the process by which an entity identifies itself prior to network logon is permitted. Smart card authentication is one of the strongest user authentication mechanisms available today in the market. Unlike ordinary cards like those used in banks, smart cards can defend themselves against unauthorized users as it uses complex and high level security measures.

Smart cards are considered to represent a breakthrough solution for maximizing security, efficiency and interoperability in a wide range of e-government and e-commerce applications such as strong authentication, identity management, data management, customer support, and communications [29-33].

It is envisaged that the new smart ID card issued by the government to all citizen and resident population in the UAE and as part of the ID card scheme launched in mid-2005 will gradually be the only acceptable token to access e-government portals. Out of an estimated 8.2 million UAE population, more than 3.7 million people already posses smart ID cards, and it is planned that towards the end of 2014 all population will be enrolled.

The latest generation of UAE smart ID cards (144K Contactless) contain multiple credentials, including unique RFID, MRZ barcode, photo ID, and biometric information (fingerprints), along with microprocessor and crypto keys and certificates. There are key primary services that can be provided by the UAE ID card in terms of e-government applications, some features of which are currently in use as explained next (See also Table 2).

Table 2. UAE ID Card Capabilities and Features Basic.



	What's in the chip?	How does it work?	Validation?	Applications
Identity Data Capture	• *Biographical* • *Photo*	• *100% accurate information* • ***Publicly available for applications***	• *Identity data contained in files* ***digitally signed by EIDA***	• *Provisioning (e.g. Data capture at Bank branches, portal registration)*
Authentication	• *PKI Applet with* ***authentication key pair*** *and corresponding certificate*	• *PIN code protection*	• *Emirates ID* ***Online/ Offline Validation Services***	• *Online access to electronic services using the eID as* ***3 factor authentication token***
Signature	• *PKI Applet with* ***signature key pair*** *and corresponding certificate*	• *PIN code* • *eID Digital Signature*	• ***Signature Validation Services***	• *Specific transactions having* ***non-repudiation/ legal enforcement***

- **Trusted Personal Data:** available in an electronic form which allows applications to capture data directly from the smart ID card chip.

  The integration of the capability of reading data electronically from the chip in some public sector applications have introduced significant contributions in terms of speed and accuracy and the elimination of the traditional ways of data capture and entry procedures. The use of the smart ID card for physical authentication and data capture has shortened for example the process cycle of service delivery at one public sector organizations (i.e., Dubai Courts) to less than 7 seconds from 7 to 10 minutes taken previously [34]. Similar success stories were repeated in many of the public sector organisations in the country that contributed to raising awareness of the smart card capabilities.

- **Multi-Factor Authentication:** support varying strengths of authentication i.e., pin code, biometrics, digital certificates.
  The multi-factor authentication feature is a major capability that the ID card provides for e-government applications. For example, Abu Dhabi e-government portal [35] uses the UAE smart ID card to provide higher levels of assurance and confidence in the digital identities that interact with the portal. A two factor authentication (PIN and Offline Certificate validation) capability of the ID card has been integrated to support and enhance the security for different e-service access models.

- **Digital Signature:** personal digital certificates that allow users to digitally sign documents and applications.

  Data integrity and non-repudiation capability of signed documents and applications is another benefit. Since access to the private key component needed to perform digital signatures is restricted to the person who possesses an ID card who has knowledge of its associated user PIN (and biometrics), it becomes increasingly difficult for an individual to later deny (repudiate) participation in transactions involving his or her digital signature. The digital signature is projected to replace the pen-and-ink signatures in both government and private sector transactions. This capability inserted into the card should also further support the development of e-government and e-commerce environments.

4.2. Smart Card Development Toolkit / Reader

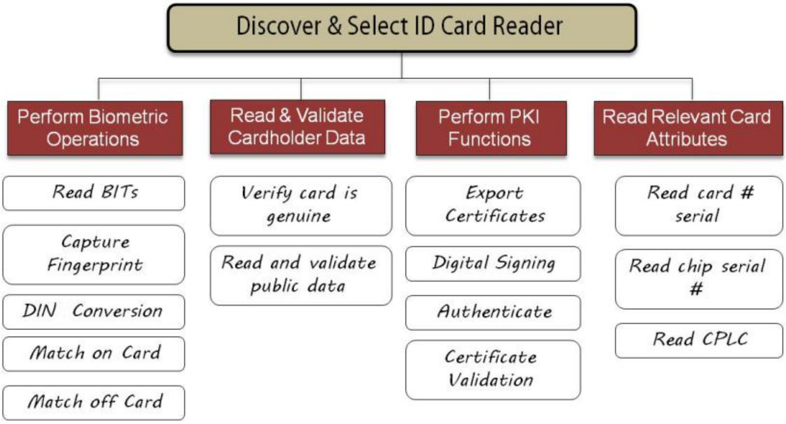


Figure 3. ID Card Toolkit Functions

To use a smart card in an e-government G2C environment, computers are needed to be equipped with smart card readers in order to enable the capabilities specified in section 3.1 above. See also Figure 3. A software toolkit was developed to enable integration with e-government applications which included smart card interface standard and the driver software used for managing the smart card and the card reader. In short, the smart card development toolkit aims to demystify the application of the smart card in e-government transactions, and also strengthen the understanding of all those involved in the planning and the execution of e-government initiatives.

From our research in the field, we noted that smart card manufacturers normally provide their own read and access communication protocols which may raise up some integration limitation issues. Therefore, the development toolkit in the UAE was designed to be free of any proprietary features, and to allow a simple plug-and-play functionality from both the user and service provider perspectives. The type of the reader terminal is dependent on the security access models specified by the service providers. For instance, less sophisticated and cheaper card terminals are available if no biometric authentication is required.

Overall, the developed toolkit was designed to support desktop, client-server, web applications and multiple development environments such as Java, C#, .Net. Figure 4 depicts the internal toolkit structure. See also Appendix-B for further information on the toolkit capabilities supported in offline and online modes.

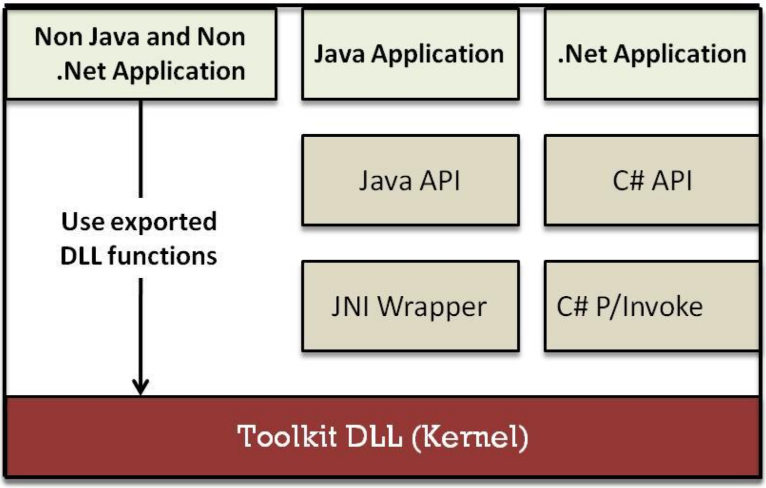


Figure 4. Toolkit Structure

Having said this, the next section explores the major component of this article related to the implementation of a central certification authority in the country and its overall architecture that will be integrated with the above two components to enable online (stronger) credential authentication.

4.3. Central Certification Authority

The Central Certification Authority also referred to as the Government Root Certification Authority is intended to be the highest Certification Authority in the hierarchical structure of the Government Public Key Infrastructure in the UAE. The high level UAE PKI architecture depicted in Figure 5 will encompass a root and multiple certified subordinate CAs' to support own PKI policy and function.

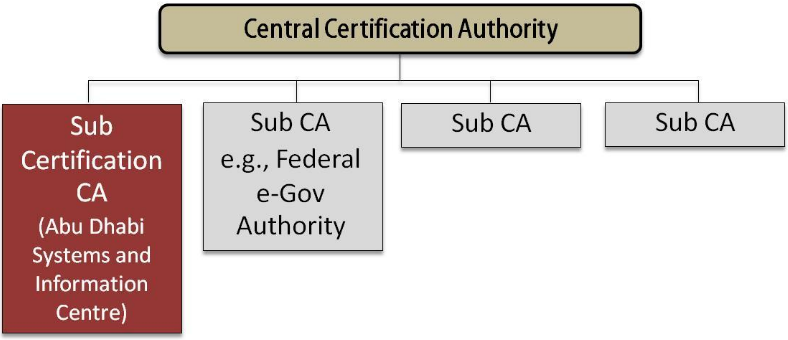

Central Certification Authority
Sub Certification CA (Abu Dhabi Systems and Information Centre)
Sub CA e.g., Federal e-Gov Authority
Sub CA
Sub CA

Figure 5. Certifications Authorities Structures

The architectural design of the certification authority infrastructure was discussed and refined at different business and technical levels with key stakeholders representing public and private sectors. The PKI management model was designed to complement existing security management practices followed by those involved in e-government and e-commerce initiatives by providing them with online validation services. As some e-government authorities required their own Certification Authority (CA), it was important for the implemented system to support such requirements. Figure 6 depicts the overall structure of the root CA.

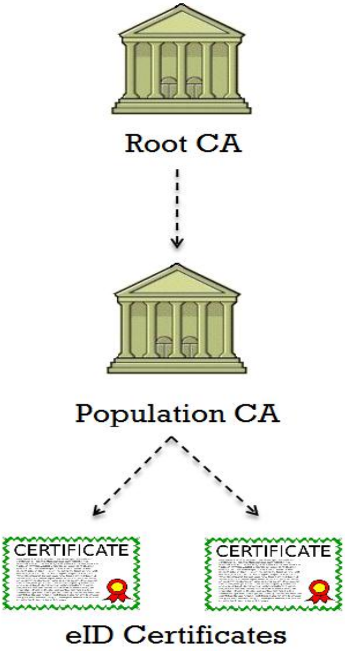


Figure 6. Root CA Structure

The PKI architecture was designed to support two operational models for the implementation of a third party sub CA. In the first option, an e-government authority may implement its own CA including the required software and hardware infrastructure. It will rely on the same PKI infrastructure to certify its Public CA using own Root certificate. Figure 7 below illustrates this solution.

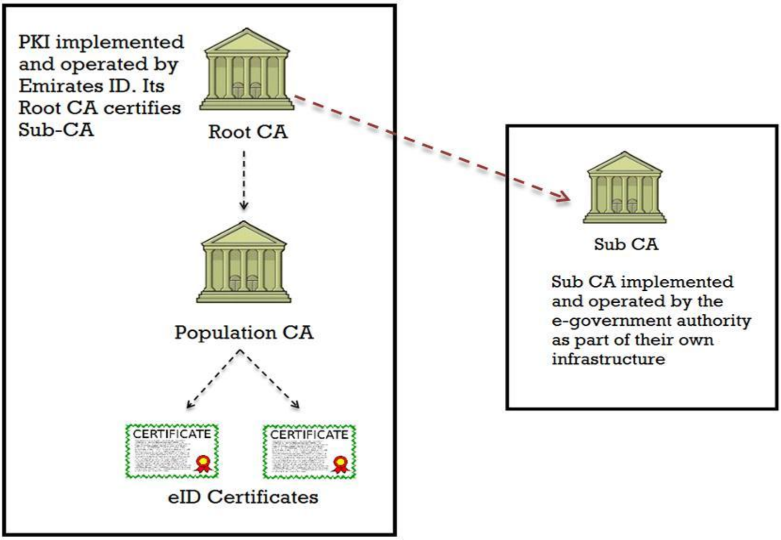

PKI implemented and operated by Emirates ID. Its Root CA certifies Sub-CA
Root CA
Population CA
CERTIFICATE
CERTIFICATE
eID Certificates
Sub CA
Sub CA implemented and operated by the e-government authority as part of their own infrastructure

Figure 7. PKI Implementation option 1

The second option assumes that a given e-government authority CA is setup as part of the same PKI infrastructure. A virtual partition is implemented on the Population CA. The e-government CA will be initialized and configured on this new virtual partition. A virtual key container is created on the HSMs so that the Sub CA key pair and corresponding certificates are separated completely from the Root keys. The solution of this second option is illustrated in Figure 8 below.

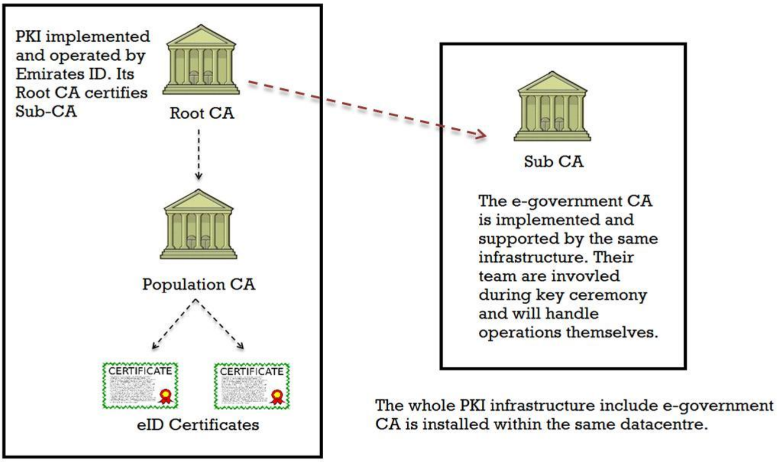
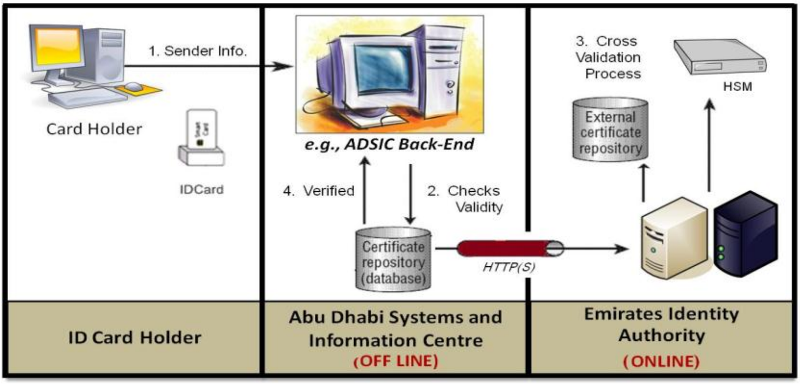

PKI implemented and operated by Emirates ID. Its Root CA certifies Sub-CA
Root CA
Population CA
CERTIFICATE
CERTIFICATE
eID Certificates
Sub CA
The e-government CA is implemented and supported by the same infrastructure. Their team are invovled during key ceremony and will handle operations themselves.
The whole PKI infrastructure include e-government CA is installed within the same datacentre.

Figure 8. PKI Implementation option 2

Deciding on which option to opt for depends entirely on the e-government authorities' requirements and their readiness to use or operate a PKI infrastructure. The first option meant no particular investments as e-government authorities would rely on the developed PKI infrastructure in the ID Card project to certify their CA public key with their Root CA. The second option involved the implementation and operation of Sub CA by the same root CA authority. The Certificate Policy (CP) needed to be specified for the e-government CA and simply for any CAs certified by the Root CA. The CP which was specified by the Policy Authority described the requirements for the operation of the PKI and granting of PKI credentials as well as the lifetime management of those credentials.

So in practice, after the completion of the authentication process which may include pin and biometrics verification, the transaction is checked for validity. At this stage, and depending on the available infrastructure, a local CRL and/or Certificate Repository database may be consulted. Another cross validation process could take place through connecting to the central certification authority to provide services of authentication and validation. A PKI based workflow depicted in Figure 9 explains how users carrying smart identity cards will interact within a PKI environment.


1. Sender Info.
Card Holder
IDCard
e.g., ADSIC Back-End
4. Verified
2. Checks Validity
Certificate repository (database)
HTTP(S)
3. Cross Validation Process
HSM
External certificate repository
ID Card Holder
Abu Dhabi Systems and Information Centre
(OFF LINE)
Emirates Identity Authority
(ONLINE)

Authentication Validation

Figure 9. Authentication and Validation (PKI) Workflow

Having said this, the next section attempts to provide a short reflection on some key management considerations to provide guidance to government agencies contemplating the development and deployment of smart ID cards and PKI solutions.

5. REFLECTION

5.1. ISSUES RELATED TO SCALABILITY, OPERATIONAL COSTS, AND INTEGRATION

Our research on PKI included the evaluation of various commercial software products available in the market. After rigorous benchmarks, the major components of the PKI solution were selected from leading international products. The following three issues needed careful attention:

Scalability - The PKI functionality should scale well to handle millions of certificates and accommodate separate large-scale projects (such as the upcoming UAE biometric e-Passport project, e-Gate project at airports, e-Services project by the various e-government authorities in the country, etc.).

Operational Costs - Certificate Authorities and Repositories will need continual operations and maintenance, especially with the increased number of customers and large-scale projects to be supported. PKI structure options should pinpoint associated costs of operations and maintenance.

Integration – Applications using PKI (i.e. PKI-enabled applications) shall integrate with central certification authority systems which shall answer the following questions:

- What is the best integration model we can offer to PKI-enabled applications?
- How can such integration with external applications be performed so that a high degree of security can be guaranteed against unauthorized access?
-

Stavrou [36] identified five key risks associated with PKI implementation; trust establishment, private key protection, CRL availability, key generation, legislation compliance. Table 3 describes how these elements were addressed in the UAE project.

Table 3. Key security issues in PKI addressed in the UAE project.

Key Risks	Description
Trust establishment	The procedures followed to verify the individuals identities, before issuing identity certificates. The issuance of certificates is linked with the ID card enrolment process. Individuals go through vivid registration process that includes: biographical data capture, portrait, fingerprint biometrics capture, verification with civil and forensic biometric databases, biographical data verification with the Ministry of Interior's database and other black-listed lists. The certification revocation procedures are linked mainly with Ministry of Interior's database and strict policies and procedures.
Private key protection	The infrastructure is hosted in a highly secure physical location, that is ISO 27001 certified.
CRL availability	A list of serial numbers of all the digital certificates that have been cancelled; CRL (Certification Revocation List) to allow other institutes verify the status of any presented digital certificate, is designed for 24/7 availability and to maintain a strong and secure architecture to avoid security breaches and a comprehensive fail-over plan that provides a secondary in infrastructure to maintain availability of services in the case of failure of the primary

	infrastructure.
Key generation	Public and private keys of the certifying authority are generated using proprietary cryptographic algorithms. The user certificates are generated using market standard cryptographic algorithms. The technical key lengths are 2048, where as the user keys are 4096.
Legislation compliance	The government is currently working on developing the legal framework to recognise the operation of the PKI and the usage of digital certificates and digital signatures. International guidelines concerning PKI are being consulted such as (EU Electronic Signatures Directive, EU Data Protection Directive). The UAE government issued a low on electronic transactions, however here is not legal act concerning the usage of digital certificates and signatures.

5.2. Management Involvement: Shifting the Focus from PKI as a Technology to a Business Enabler

The adoption of PKI has the potential to deliver significant benefits to many sectors including e-Government, healthcare and banking. However, for such adoption to happen, it was important to understand and appreciate the business value, business requirements and business integration issues [37] relevant to potential PKI customers in the above mentioned example sectors.

As part of our strategy to implement a nation-wide PKI, it was seen important to consult potential customers across many sectors including e-government authorities both on the federal and local levels. In doing so, potential customers would see the benefits of PKI as a business enabler. We paid much attention to collect the necessary business requirements that would help tightening the future PKI functional requirements. See also Appendix-C.

Undoubtedly, deployment of a functioning PKI is extremely difficult in practice [7,8,36-38]. Weak understanding of the PKI technology by top management and lack of qualified resources in the field will always be a challenging factor. Before we reached to a consensus on the PKI design and functions, there was much confusion about the full scope of this project.

We noted that practitioners in the field of government identity management systems who are interested in PKI applications have deep-seated narrowed focus when thinking about such technologies. They tend to limit their focus purely on PKI services such as digital certification and electronic signatures in the context of e-government and e-commerce, without much comprehension of how PKI could be integrated with their business needs and practices. The aggressive marketing promises by private sector consultants and vendors have contributed somehow to some misconceptions in the minds of government officials of PKI applications.

Management involvement was important in some of the regular review meetings that required restating project objectives in a user friendly terms. It was common for the technical teams in the project to fell victims of technical-driven discussions and away from the global business objectives. It was important to remind the teams to reflect the interests of stakeholders in the government rather than just the interest of the implementing organization.

From a management standpoint, we tried to stop attempts of innovation as people tend to act sometimes in complex projects, and keep them focused on the business requirements, and the overall PKI functions. Stakeholders on the other hand needed several awareness sessions of the scope and deliverables of the project. It was important to visualize and present cases of how their applications will be integrated with PKI, and highlighting the immediate benefits. High attention was given to the development of Government-2-Citizen PKI enabled applications.

5.3. Implementation Approach

An agile but incremental phased implementation approach was followed, that emphasized the delivery of functionalities that could meet the immediate demands of local e-government authorities. The earlier workshops concentrated on discussing and refining business and technical requirements with the relevant stakeholders. Specific attention was given to the development of the interfaces required to integrate the ID card system with the PKI solution, and allowing at the same time, agreement among the stakeholders on business and technical requirements. This allowed e-government authorities to experiment the authentication capabilities offered by the ID card including the online validation process.

This allowed the different groups in the organization to concentrate on the other building blocks of the PKI project, as they were running in parallel; such as technical workshops related to integration needs, testing, documentation, enforcement of policies, guidelines and compliance, digital signature laws, etc.

5.4. PKI Workflow and Lifecycle

It was important that we go through the full lifecycles of digital certificate-based identities, and how encryption, digital signature and certificate authentication capabilities are mapped to business needs and translated into real applications. See also [37,38]. It was also important to set clear procedures to handle smart card life cycle management requirements; renewal, replacement, revocation, unlocking, and the overall helpdesk and user support requirements.

Another issue that was considered in the PKI workflow was related to the incremental size of the Certificate Revocation List (CRL) which must be maintained and updated for proper validation of each transaction which occurs using the ID card certificate. An unverified transaction can provide important information or access for a potential intrusion. Thus, CRL is a significant security flaw in the operation of the PKI, and the maintenance of this list is one of the most strenuous challenges facing any CA.

The list of revoked certificates was envisaged to be well over multi gigabytes of size, and searching the list for invalid certificates will result in long delays as it will force some applications to forego a comprehensive check before carrying out a given transaction. Therefore, a Positive Certification List (PCL) was also implemented to avoid this challenge in the future.

5.5. Legal Framework

It was important that the PKI deployment is associated with a legal framework to regulate the electronic authentication environment and support the provision of online services in the public sector. See also [39]. The following items were key preparation issues addressed through intergovernmental working groups:

1. Well-documented Certificate Policies (CPs) and Certification Practice Statements (CPSs). CPs and CPSs are tools that help establish trust relationships between the PKI provider, the subscribers (end-users) and relying parties (i.e. implementers of PKI-enabled applications).
2. PKI assessment and accreditation were seen as an important trust anchor, as it will determine compliance to defined criteria of trustworthiness and quality. Such assessment and audit was set as a prerequisite to be included in the trusted root CAs program. As part of the implementation of the future PKI applications, it was recommended that an assessment of the existing Certificate Policies (CPs) is conducted. This resulted in RFC 2527 compliant CPs and CPSs [40].
3. A digital signature law that would define the meaning of an e-signature in the legal context. The law needed to recognize a digital signature in signed electronic contracts and documents as legally binding as a paper-based contracts.

CONCLUSIONS

Public Key Infrastructure has proven itself invaluable in e-government and e-commerce environments despite the complexity and associated risks that may stem from its application. We observe that many of the current PKI projects have limited applications in e-government domain because it is mainly sponsored and managed by private sector organizations. Telecom companies in many countries in the Middle East region for example have implemented PKI systems but face challenges to expanding their limited user community.

Establishing and using a government based certification authority, would logically acquire higher levels of trust in the certificate issuance process and in the identities of the recipients of the certificates. The integration of PKI into central government identity management systems is believed to support the diffusion and acceleration of e-government progress, that is, the provision of citizen services and outreach over digital networks. The presented case study of the UAE PKI project and the approach the government has followed to integrate it part of its federal identity management system, was aimed to share knowledge and improve understanding of government practices in the field.

Assessment of the success of this proposed structure was beyond the scope of this article, as the implementation was undergoing during the preparation of this article. However, it will be published in a separate article once the full implementation is complete.

Without a doubt, the maturity of e-government requires significant efforts by both practitioners and researchers to support the development of horizontal and vertical e-government integration [41-43]. Governments need to prepare themselves to introduce social changes of work roles, attitudes and new competence needs. Governments are seen to be the entity responsible to lay down and develop the foundation of digital identities.

PKI remains a crucial component to provide higher security levels in digital forms, and will have a triple effect if integrated with the existing government trusted identity management systems. As the adoption of PKI in government projects is likely to continue, opportunities exist for future researchers to examine the success of such implementations.

REFERENCES

[1] Bicking, M., Janssen, M. and Wimmer, M.A.(2006) “Looking into the future: scenarios for e-Government in 2020” In Project e-society: Building Bricks. Soumi, R., Cabral, R., Hampe, J.F., Heikkilä, A., Järveläinen J. and Koskivaara, E. New York: Springer Science & Business Media.

[2] Ebbers, W.E., Pieterson, W.J. & Noordman, H.N. (2008) “Electronic government: Rethinking channel management strategies”, Government Information Quarterly, vol. 25, pp. 181-201.

[3] Streib, G. & Navarro, I. (2006), “Citizen demand for interactive e-Government: The case of Georgia consumer services”, American Review of Public Administration, vol. 36, pp. 288-300.

[4] Al-Khouri, A.M. & Bal, J. (2007) “Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics,” Journal of Computer Science, Vol.3, No. 5, pp.361-367.

[5] Al-Khouri, A.M. & Bal, J.(2007) “Electronic Government in the GCC countries,” International Journal Of Social Sciences, Vol. 1, No. 2, pp.83-98.

[6] Baum, C., & Maio, A.D. (2000) Gartner’s four phases of e-government model. Gartner Group Inc., Stamford.

[7] Wilson, S. (2005) "The importance of PKI today", China Communications [Online]. Available from: www.china-cic.org.cn/english/digital%20library/200512/3.pdf. Accessed: 01 February 2011.

[8] Brands, S.A. (2000) Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press.

[9] The Defense Information Systems Agency is a United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands. The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian

employees, other non-DoD government employees, state employees of the National Guard, and eligible contractor personnel. The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities. It also serves as an identification card under the Geneva Conventions. The CAC enables encrypting and cryptographically signing email, facilitating the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials.

[10] Berinato, S. (2002) Only Mostly Dead. The Resource for Security Executives. [Online]. Available: http://www.cso.com.au/article/120370/only_mostly_dead.

[11] Griffin, D., Trevorrow, P. & Halpin, E. (2007) Introduction e-Government: A welcome Guest or Uninvited Stranger? In Developments in e-Government. A critical Analysis, Griffin, D., Trevorrow, P., & Halpin, E. Amsterdam: IOS Press.

[12] Lee Y.-R. & Lee, H.-S. (2004) An authenticated certificateless public key encryption scheme. Cryptology ePrint Archive, Report 2004/150.

[13] Shi Y. & Li, J. (2005) Provable efficient certificateless public key encryption. Cryptology ePrint Archive, Report 2005/287.

[14] Cheng, Z. & Comley, R. (2005) Efficient certificateless public key encryption. Cryptology ePrint Archive, Report 2005/012.

[15] Bentahar, K., Farshim, P., Malone-Lee, J. & Smart., N.P. (2005) Generic constructions of identity-based and certificateless kems. Cryptology ePrint Archive, Report 2005/058.

[16] Dent W. & Kudla, C. (2005) On proofs of security for certificateless cryptosystems. Cryptology ePrint Archive, Report 2005/348.

[17] Baek, J., Safavi-Naini, R. & Susilo, W. (2005) Certificateless public key encryption without pairing. In Information Security (ISC), volume 3650 of LNCS, pages 134–148. Springer-Verlag.

[18] Hu, B., Wong, D. Zhang, Z. & Deng, X. (2006) Key replacement attack against a generic construction of certificateless signature. In

ACISP, volume 4058 of Lecture Notes in Computer Science, pages 235–246. Springer-Verlag.

[19] Libert & Quisquater, J.-J. (2006) On Constructing Certificateless Cryptosystems from Identity Based Encryption. In Public Key Cryptography (PKC), LNCS. Springer-Verlag.

[20] Al-Riyami, S. & Paterson, K.G. (2003) Certificateless public key cryptography. In ASIACRYPT, volume 2894 of LNCS, pages 452–473. Springer-Verlag.

[21] Castelluccia, C. Jarecki, S. & Tsudik, G. (2004) Secret handshakes from CA-oblivious encryption. In ASIACRYPT, volume 3329 of LNCS, pages 293–307. Springer-Verlag, 2004.

[22] Menezes, A. & Smart, N (2004) Security of signature schemes in a multi-user setting. Designs, Codes and Cryptography, 33:261–274.

[23] Nana, S. & Unhelkar, B. (2003) Progress Report on Development of Investigations Theory of PKI" and its applications to Australian Information Systems.

[24] Ashford, W. (2011) Why Public Key Infrastructure (PKI) has failed. ComputerWeekly [Online]. Available from: http://www.computerweekly.com/blogs/read-all-about-it/2011/02/why-public-key-infrastructure.html. Accessed: 03 March 2011.

[25] Price, G. (2005) PKI Challenges: An Industry Analysis. Proceeding of the 2005 conference on Applied Public Key Infrastructure: 4th International Workshop: IWAP 2005.

[26] Soumi, R., Cabral, R., Hampe, J.F., Heikkilä, A., Järveläinen J. and Koskivaara, E. (eds.) (2006) Project e-society: Building Bricks. New York: Springer Science & Business Media.

[27] Westland, D.D. and Al-Khouri, A.M. (2010) "Supporting Use of Identity Management to support e-Government progress in the United Arab Emirates," Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

[28] Emirates Identity Authority is a federal government organisation in the United Arab Emirates tasked to develop and implement a national identity management infrastructure in the country.

[29] Allen, C. (1995) "Smart Cards Part of U.S. Effort in Move to Electronic Banking", Smart Card Technology International: The Global Journal of Advanced Card Technology, Townsendm R. (ed.), London: Global Projects Group.

[30] Coates, B.E. (2001) "SMART Government on Line, not in Line: Opportunities, Challenges and Concerns for Public Leadership." ThePublic Manager, vol. 30, no. 4, pp. 37-40.

[31] Guthery, S.B. and Jurgensen, T.M. (1998) SmartCard Developer's Kit. Macmillan Technical Publishing.

[32] Kaplan, J.M. (1996) Smart Card: The Global Information Passport, New York: International Thomson Computer Press.

[33] Rankl, W. & Effing, W. (1997) Smart Card Handbook. John Wiley & Sons.

[34] Albayan (2009) "ID Card cuts down process time to 7 seconds at Dubai Courts", Al Bayan Newspaper, [Online]. Website: www.albayan.ae. Issue date: 02 March 2009.

[35] Abu Dhabi eGovernment Portal provides a centralised electronic gateway between the local government in Abu Dhabi and its population. The portal is envisaged to provide a single point of access to more than 600 services in the form of transactional online services. (http://www.abudhabi.ae).

[36] Stavrou, E. (2005) PKI: Looking at the Risks, [Online]. http://www.devshed.com/c/a/Security/PKI-Looking-at-the-Risks/

[37] Deitel, H.M., Deitel, P.J. and Steinbuhler, K. (2001) e-Business & e-Commerce for Managers. USA: Prentice Hall.

[38] Ford, W. and Baum, M.S. (2001) Secure Eletronic Commerce: Building the Infrastructure for Digital Signatures and Encryption 2nd Edition. USA: Prentice Hall.

[38] Shi, Y. & Li, J. (2005) Provable efficient certificateless public key encryption. Cryptology ePrint Archive, Report 2005/287.

[39] Dempsey, J.X. (2003) Creating the Legal Framework for ICT Development: The Example of E-Signature Legislation in Emerging

Market Economies. Washington, DC: Centre for Democracy and Technology.

[40] RFC 2527 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. This document presents a framework to assist the writers of certificate policies or certification practice statements for certification authorities and public key infrastructures. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy definition or a certification practice statement. This memo provides information for the Internet community

[41] Basu, S. (2004) "E-Government and developing countries: an overview". International Review of Law Computers, 18(1), pp. 109-132.

[42] Heeks, R. 2006. Implementing and Managing eGovernment: An International Text. London: Sage Publications Limited.

[43] Schedler, K. and Summermatter, L. (2003) “e-Government: What Countries Do and Why: A European Perspective”. In The World of e-Government Curtin, G.C., Sommer, M.H. & Vis.-Sommer, V. (Eds.). The Haworth Political Press.

APPENDIX-A: MAJOR PKI PROJECTS WORLDWIDE

1. **ICAO PKD (International Civil Aviation Organization Public Key Directory)**

   This is a global PKI directory implementation for achieving interoperable ePassports worldwide. The key benefit of this project is the PKI Validation of ePassport.

   This project allows border control authorities to confirm that:

   - The ePassport document held by the traveler was issued by a bonafide authority.
   - The biographical and biometric information endorsed in the document at issuance has not subsequently been altered.
   - Provided active authentication and / or chip authentication is supported by the ePassport, the electronic information in the document is not a copy (ie clone).
   - If the document has been reported lost or has been cancelled, the validation check can help confirm whether the document remains in the hands of the person to whom it was issued.

2. **SWIFT – PKI at application level (SWIFTNet PKI), and another PKI at network level (VPN)**

   SWIFT's public key infrastructure (SWIFTNet PKI) service issues digital certificates to financial institutions and corporates, thereby enabling a trusted, provable and confidential end-to-end communication over SWIFTNet.

   In addition SWIFT's VPN PKI issues certificates to its network infrastructure to secure all network traffic using VPN protocols.

3. European TLIST of the 27 Member States

On 16 October 2009 the European Commission adopted a Decision setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under the Services Directive. One of the measures adopted by the Decision consisted in the obligation for Member States to establish and publish by 28. 12.2009 their Trusted List of supervised/accredited certification service providers issuing qualified certificates to the public. The objective of this obligation is to enhance cross-border use of electronic signatures by increasing trust in electronic signatures originating from other Member States. The Decision was updated several times since 16.10.2009, the last amendment was made on 28.7.2010

The EU Trusted Lists benefits above all to the verification of advanced e-signatures supported by qualified certificates in the meaning of the e-signature directive (1999/93/EC) as far as they have to include at least certification service providers issuing qualified certificates. Member States can however include in their Trusted Lists also other certification service providers.

Member States had to establish and publish their Trusted List by 28.12.2009 at least in a “human readable” form but were free to produce also a "machine processable" form which allowed for automated information retrieval. In order to allow access to the trusted lists of all Member States in an easy manner, the

European Commission has published a central list with links to national "trusted lists" (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf).

4. **ERCA (European Root Certification Authority)**

The main ERCA deliverables are the Member State Authority [MSA] policy review and the Key generation for Member State Authority CAs. During an ERCA signing session, countries receive the symmetric and asymmetric encryption keys for use by their Member State Authority.

The Member State Authorities will issue certificates on smart cards required for the operations of the tachograph which a device that records a vehicle's speed over time, monitor driver's working hours and ensure that appropriate breaks are taken.

5. **TSCP PKI (Transatlantic Secure Collaboration Program)**

TSCP program involves leading aerospace & defense companies in the USA and Europe including Boeing, BAE Systems, EADS, Lockheed-Martin, Northrop Grumman, Raytheon and Rolls-Royce. Supporting Governments include the US DoD, the UK MoD and the Government of Canada.

The challenge addressed by TSCP PKI is the increasing reliance on the electronic creation, transmission and manipulation of information in order to meet schedule and efficiency objectives. The emerging business environment requires that this occur with an international workforce subject to multiple jurisdictions. This presents significant business risk to the companies involved, in terms of compliance with national laws and regulations on data transfer, increased complexity of governance and oversight, and IT security.

The TSCP PKI represents the bridge CA that allows interoperability between the program members CAs.

6. FBCA - US Federal bridge CA

The main objective of this bridge CA is to provide one CA for cross-certification between main CAs in the US and avoid complicated mesh cross-certification. FBCA is designed to create trust paths among individual PKIs. It employs a distributed and not a hierarchical model.

The FPKISC, Federal Public Key Infrastructure Steering Committee, oversees FBCA development and operations including documentation, enhancements and client-side software. The FBCA operates in accordance with FPKI Policy Authority and FPKISC directions.

FBCA is in charge of propagating policy information to certificate users and maintain a PKI directory online 24 X 7 X 365.

APPENDIX-B: TOOLKIT CAPABILITIES

Toolkit Function	Require Secure Messaging?	Require Online Validation Service from EIDA?	What kind of validation is required?
Read Public Data	**No**	No	Public data files (read from the card) are signed. The Toolkit function "**Read Public Data**" verifies the signature on these file as part of the reading process. The verification process happens locally on the end user environment and as such it is an offline process that does not require any online additional service from EIDA.
Authentication (with PKI)	**Yes** The justification is as follows: • Firstly, the authentication process involves the PKI applet where the authentication key pair (and corresponding certificate) is stored • The ID card (actually the PKI applet) requires PIN verification prior to authorizing the usage of the authentication key pair. • PIN verification requires secure messaging with the PKI applet.	PKI authentication requires the following steps: - Secure Messaging with the PKI applet - PIN Verification - Authentication process through which the cardholder authenticate certificate is validated. Establishing a Secure Messaging with the PKI applet of the ID card does not require being online with EIDA. This is due to the fact that the SAGEM PKI DLL part of the Toolkit contains the keys that enable establishing a Secure Messaging with the PKI applet locally (**offline process**). Regarding certificate validation, EMIRATES ID does as part of the PKI solution an online service (OCSP) that offers real time verification of certificate status. Whether the Service Provider business application will use this service depends basically on their will to rely all the time on an **online service** for certification validation. The alternative for them would be to download CRLs frequently from the CA repository and to process certificate and CRLs locally (**offline process**).	Authentication certificate validation is a pre-requisite to complete the authentication process. Two modes are available for certification validation: 1. Using CRLs: in this case, CRLs are downloaded by the business application regularly. However the actual processing of certificate validation is an offline process that happens locally on the end-user's environment. 2. Using EMIRATES ID OCSP server: This is an online service that relieves the business application from the complex processing of CRLs and provides real time validation of certificate revocation status.
Biometric Match-Off-Card	**Yes** The Match-Off-Card requires reading the	It depends on the business application architecture and deployment channel. The possible options are as follows: 1. The business application is offered as an online service (e.g.	No validation is required as part of the Off-Card-Biometric apart from performing the actual verification process that involves the fingerprint

	fingerprint from the ID card which is protected data that requires Secure Messaging with the ID Applet.	ADSIC e-services portal, e-services kiosks). In this case, the business application relies on an **online service** from EMIRATES ID that enables setting a Secure Messaging session with the ID applet. 2. The business application is deployed on user sites (e.g. municipalities) that are visited by end-users. The application deployed on user sites has a dedicated SAM device connected to it. Therefore Secure Messaging with the ID applet can be established using the SAM. The process is **offline** and does not require online connectivity to EIDA. 3. The business application is deployed on alternative channel such as kiosks. The kiosk would have an integrated SAM device and the processing is therefore **offline** and is similar to the 2nd point above. 4. The business application is deployed on standalone/**offline** devices such as Handhelds with integrated SAM.	template read from the ID card. The verification happens locally on the end-user environment and does not require online connectivity to EIDA.
Biometric Match-On-Card	**Yes.** The Match-On-Card requires an interaction with the MOC applet of the ID card. The overall process for Match-On-Card can be summarized as follows: 1. Setup a Secure Messaging Session with the MOC Applet of the ID card 2. Perform the actual MOC verification after capturing the end-user fingerprint	By definition, the Match-On-card process is an **offline process** that shall not require online connectivity to EIDA. Therefore, the MOC process is typically used in situations where the business application has a connected SAM. Examples of such a deployment would be: 1. The business application is deployed on user sites (e.g. municipalities) that are visited by end-users. The application deployed on user sites has a dedicated SAM device connected to it. Therefore Secure Messaging with the MOC applet can be established using the SAM. 2. The business application is deployed on standalone devices such as Handhelds with integrated SAM.	No validation is required as part of the On-Card-Biometric apart from performing the actual verification process that happens locally on the end-user environment and does not require online connectivity to EIDA.
Digital (Transaction)	**Yes.**	The digital signature verification process by the business application involves the following steps:	Authentication certificate validation is a pre-requisite to complete the

Signature	Justification is similar to the Authentication process with PKI.	1. Signature Verification 2. Certificate Path Build 3. Certificate Path validation (where certification revocation status is checked) EMIRATES ID offers 2 online services to business partners. - Online certificate validation through the OCSP server. The discussion on this is similar to the one provided for the Authentication process with PKI (see Authentication entry). - Online Signature Validation: In this case the whole signature verification process is outsourced to EIDA.	authentication process. The two modes discussed under Authentication with PKI are application (see Authentication entry above). If the business partner decides to use EMIRATES ID **online service** for signature validation, then this requires an online connectivity to EIDA.

APPENDIX-C: SUMMARY OF BUSINESS REQUIREMENTS AND PKI FUNCTIONAL REQUIREMENTS

	Concept	Description	Opportunities	Challenges
EMIRATES ID as the PKI provider for the UAE e-Government	Only CAs operated by EMIRATES ID are recognized by stakeholders in the eGovernment sector.	EMIRATES ID is already managing the PKI for the eID card issuing project (i.e. population CA). This PKI will be upgraded including the implementation of validation services (CRL, OCSP). Future UAE eGovernment PKI projects will take advantage of the new PKI to be implemented by EIDA. Finally, existing EMIRATES ID PKI applications (including the eID card issuing project) will be migrated to the future EMIRATES ID PKI.	• EMIRATES ID being the main PKI provider in the UAE and the recognized one for eGovernment projects • EMIRATES ID becomes a revenue driven organization	• Lack of support from Stakeholders
Offering Managed PKI services	EMIRATES ID to cross-certify other government and commercial CAs and to offer managed PKI services for these.	EMIRATES ID will offer Managed PKI services aimed at enterprises planning to establish a Certification Authority (CA) for addressing their particular business needs. Organizations that might be interested in such services are banks and governmental organizations (e.g. healthcare, education). Also EMIRATES ID can	• Establish EMIRATES ID credibility as the trusted PKI provider in the UAE • An additional revenue stream for EIDA	• More operational and infrastructural requirements • EMIRATES IDdiversifying into a business stream unrelated to EMIRATES IDcore business

		cross-certify (acting as a root) other CAs.		
Supporting encryption certificates	EMIRATES ID PKI to support issuing encryption certificates with key backup	EMIRATES ID can establish CA for encryption certificate issuing with key escrow. Each encryption key pair will be issued under the control of the certificate holder of the organization to which he belongs.	• Full range of certificate types offered to EMIRATES ID potential customers • Support the eID card issuing project in case encryption certificates are needed	• Maintaining and backing up keys is a liability issue and additional operation overhead • Encryption tend to be seen as a threat to national security
Supporting multi purpose certificates	PKI to support the issuance of multi purpose certificates	EMIRATES ID PKI will support issuing and managing different types of certificates such as certificates for: • VPN devices • Web servers (SSL certificates) • Simple Certificate Enrolment Protocol (SCEP) devices • Attribute (role-based) certificates • Certificates for professionals (e.g. doctors) • Anonymity certificates (e.g. by omitting first and last names from the certificate) EMIRATES ID PKI will offer the enrolment methods needed to issues these types of certificates by the relevant organizations.	• Support PKI-enabling in the UAE by providing certificates that fulfill the requirements of different sectors • Full range of certificate types offered to EMIRATES ID potential customers • Additional revenue streams	• Eventually additional CAs and CPs to manage
Promote electronic signatures law	promote electronic signatures law	EMIRATES ID will define an e-Signature law that will define the legal framework for electronic signature as well as set EMIRATES ID as the regulatory authority (root CA) accrediting and certifying other organizations.	• Promote digital signature and eID card usage in the UAE • Establish EMIRATES ID as the regulatory authority responsible for the secure PKI usage in the UAE	• Citizen reaction to be legally liable for digitally signing documents
Trusted Time-stamping	provide trusted time-stamping service (RFC 3161-compliant)	The time-stamping services will allow EMIRATES ID enforcing and offering non-repudiation services so that a signature remains valid long-term after	• Enforcing non-repudiation services (long-term validity of e-documents) • Additional revenue stream • Establish EMIRATES ID position as the	• Time-stamping servers rely on the availability of a trusted time source (e.g. NTP server)

	(RFC 3161 is Time-stamping protocol)	it has been created. Time-stamping general added-value is to provide an irrefutable proof that a document existed at a certain point in time.	trusted PKI provider in the UAE	• Time-stamping is an online service, therefore EMIRATES ID need to adhere to SLAs defined for its customers
Online Validation Services	to support Online Certificate Status Protocol (OCSP)	OCSP allows providing timely secure information on certificate revocation status.	• Timely access to certificate revocation status information • Easier PKI-enabling compared to relying on CRLs only • Eventually additional revenue streams • Simpler integration models with e-Government projects • Establish EMIRATES ID position as the trusted PKI provider in the UAE	• OCSP is an online service, therefore EMIRATES ID need to adhere to SLAs defined for its customers •
Long-term Archive Services (LTA)	to provide/promote long-term archive services (LTA)	EMIRATES ID will provide/promote long-term archive services (LTA) which will enable the preservation of data integrity over the time. The LTA service will be particularly useful with signed documents whose validity shall be preserved over time.	• Enforcing long-term non-repudiation services offered by EIDA • Additional revenue stream • Establish EMIRATES ID position as the trusted PKI provider in the UAE	• additional operation costs for EIDA • relatively complex IS • Operating the LTA might be out of scope for EMIRATES ID as e-Identity authority
E-Notary services	E-Notary services promoted/provided by EIDA	An e-notary is a PKI based application that allows adding trust in digital transactions (i.e. such as e-commerce transactions). Such services provides guarantee to the parties involved in the transaction that they can trust each other and provides the proofs needed to establish that a transaction took place. Potential customers for such services are e-Justice and e-Commerce sectors.	• Facilitating and enabling trusted e-commerce transactions • Additional revenue stream for EIDA	• Typically e-Notaries applications are bespoke • No successful implementation (e.g. lessons learned) worldwide so far • Current e-commerce law does not define what an e-Notary stands for • Lack of adoption of e-commerce implies the lack of adoption of an e-Notary application
eID starter kit for citizens	will provide an	To support using of PKI, EMIRATES ID will create and provide a package that	• Simple adoption of PKI and eID card by citizens and residents	• Lack of IT knowledge among citizens

(certificate holders)	eID starter kit	will facilitate the installation of everything needed for using the eID card by the cardholder.	• Promote the usage of the eID card within the UAE • Strengthen the position of EMIRATES ID as the promoter of the eID card in the UAE • Promoting the upgrade of the existing PCs park in the UAE	• Existing PCs park not supporting the installation of the package to be installed by the citizen • Expensive operation in case EMIRATES ID targets additional platforms (e.g. UNIX) other than Microsoft Windows • Flooding of the EMIRATES ID helpdesk when the roll-out of this package starts
eID development kit	EMIRATES ID will provide an eID development kit for eID (e.g. PKI) applications developers	As opposed to the eID starter kit used by citizens, the eID development kit will be used by whoever will be interested in developing eID and PKI enabled applications. The kit includes code samples, APIs, access to EMIRATES ID test PKI infrastructure, sample eID cards, etc.	• Quick adoption of PKI by relying parties (i.e. by the implementers of • Trigger for EMIRATES ID to implement a fully-fledged PKI in development environment to service PKI applications implementers • Additional revenue stream for EIDA	• The toolkit is useless if EMIRATES ID does not target the right platforms • Lack of EMIRATES ID experienced staff to support the organizations using the kit
Third party PKI modules/application type approval (i.e. certification)	Third party PKI and eID application certification	EMIRATES ID will help the developers of eID applications promoting their applications. This includes testing and the type approval of their applications so that they get accredited as authorized to process eID cards.	• Enable the implementation of secure eID-enabled applications • Build confidence of citizens (eID card holders) in business applications using the ID card • Establish EMIRATES ID position as the trusted party around eID-enabling	• Testing applications requires lots of skills (including PKI, eID and testing skills). People having these skills shall be available • Liability issue for EMIRATES ID in case security holes are found in some applications (that did receive type approval from EIDA)

Certified mailbox service	EMIRATES ID to implement and operate a certified mailbox service	Such service would allow each citizen/resident to have a certified mailbox (of the form firstname.lastname@mymailbox.ae) where we would receive official courier from governmental organization. The mailbox could also be used to receive any useful courier (including bills, etc).	• Business case application for using the eID card • Promoting G2C and B2C markets • Additional income streams • Government being closer to citizens • New business stream for commercial organizations	• Citizens may find that such service is a threat against their privacy • Liability issue for EMIRATES ID in case a threat agent breaks into one mailbox • Lack of adoption by citizens unless the service is mandatory
Card Validation Gateway	Implement an access control server for eID cards	The Validation Gateway maintains a "hotlist" of cards that has been temporarily or permanently blocked. Such service could be useful for specific public services such as police and kiosks. The Validation Gateway is also needed in case EMIRATES ID implements Post Issuance Personalization (PIP) of card applications.	• Support post-issuance personalization of eID cards • Providing a trusted gateway responsible for providing a blacklist of revoked cards • Easier integration models between EMIRATES ID and eID applications implementers	• The Validation Gateway can be seen as a single point of attacks by threat agents • The validation gateway being developed without thinking the right integration interfaces with eID enabled applications

PKI Technology:
A Government Experience[25]

DR. ALI M. AL-KHOURI

ABSTRACT: As government operations are moved online, information technology security services based on cryptography become essential. Public key cryptography can play an important role in providing enhanced security services related to data protection and strong credentials for identity management. This article attempts to contribute to the limited domain of knowledge available about government practices and projects. The purpose of this article is to provide an overview of the public key infrastructure (PKI) components deployed in the United Arab Emirates national identity system. It provides a comprehensive overview of PKI technology and its primary components. It then provides an overview of the existing cryptographic components and the digital certificates stored in the PKI Applet of the smart ID card, with the purpose of shedding light on what is needed to fulfill the needs for future e-government requirements in the country.

Key words: *UAE PKI, e-government, e-commerce, digital signature, encryption.*

[25] Al-Khouri, A.M. A (2012) "PKI Technology: A Government Experience", International **Journal of Computer Science Engineering and Information Technology Research**, Vol. 2, No. 1, pp. 115-141.

1. INTRODUCTION

MANY governments in the past decade have initiated advanced identity management systems that incorporated PKI technology. This global interest in the technology is based on the need to meet the requirements for higher levels of authentication, confidentiality, access control, non-repudiation, and data integrity. Perceptibly, governments have been under tremendous pressure to deliver internet-based electronic services in light of increasing citizens' demands for improved and more convenient interaction with their governments.

Many researchers argue that PKI is a key pillar for e-government transformation and e-commerce enablement. Although the concept of PKI may sound simple, many deployment experiences have shown catastrophic results from both technical and operational standpoints (GAO, 2001; Judge, 2002; Pluswich and Hartman, 2001; Rothke, 2001; Schwemmer, 2001). There are still ruthless attempts by government-backed projects to introduce PKI in their identity systems. This outlines the need for sharing knowledge of implementation experiences from various government projects. This is article is written with this scope of need.

The government of the United Arab Emirates initiated its major PKI initiative as part of its national identity management infrastructure development program in 2003. This project is considered to be one of the early systems in the Middle East region, and with the objective to issue 10 million digital identities by the year 2013. This article discusses key components of the PKI project related to private key activation, certificate validation, and encryption, in the context of e-government applications. This article is primarily structured into two sections. The first section provides an overview of PKI technology, describing its key components and how it provides security. The second section discusses the cryptographic components of PKI in the UAE project in light of e-government and e-commerce future requirements.

2. PUBLIC KEY CRYPTOGRAPHY

Cryptography is the branch of applied mathematics concerned with protecting information. Confidentiality is the protection of data against unauthorized access or disclosure through application of functions that transform messages into seemingly unintelligible forms and back again. These processes are called encryption and decryption. One kind of cryptography that can provide confidentiality, authentication, and integrity is symmetric key cryptography, in which an algorithm makes use of a single key used to encrypt data. The same key is also used to decrypt or return the encrypted data into its original form. This one key, called the symmetric key, is very efficient in terms of processing speed and using minimal computing resources, but is limited in the sense that (1) it is difficult to exchange the key securely without introducing public key cryptography, and (2) because both the sender and the receiver of a message share the same symmetric key, the authentication and integrity is not provable to a third party who does not also hold the key—thus, symmetric cryptography cannot provide the additional security service called non-repudiation.

Public key cryptography is an attempt to solve these particular shortcomings of symmetric key cryptography (Ferguson et al., 2010). Public key cryptography employs an algorithm using two different but mathematically related keys, one for creating a digital signature or decrypting data, and another key for verifying a digital signature or encrypting data.

Computer equipment and software utilizing such key pairs are often collectively termed an asymmetric cryptosystem. The complementary keys of an asymmetric cryptosystem for PKI technology are arbitrarily termed the private key, which is known only to the holder, and the public key, which is more widely known. If many people need the public key for various PKI applications, the public key must be available or distributed to all of them, perhaps by publication in an online repository or directory where it is easily accessible.

Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely it is computationally infeasible to derive the private key from knowledge of the public key. Thus, although many people may know the public key of a given holder, they cannot discover that holder’s private key. This is sometimes referred to as the principle of irreversibility.

Another fundamental process, termed a hash function, is used in PKI technologies. A hash function is an algorithm that creates from a message a digital representation or fingerprint in the form of a hash value or hash result of a fixed length (Spillman, 2005). The hash result is usually much smaller than the message, but nevertheless substantially unique to it. Any change to the message produces a different hash result when the same hash function is used; the hash is unique to a given message for all practical purposes. In the case of a secure hash function, sometimes termed a one-way hash function, it is computationally infeasible to derive the original message from knowledge of its hash value. Hash functions therefore enable the PKI application software to operate on smaller and more predictable amounts of data, while still providing robust correlation to the original message content.

Table 1: Mapping of Security Services to Cryptographic Techniques

Cryptography Techniques/ Security Services	**Encryption /Decryption**	**Message Authentication Codes/Keyed Hash**	**Digital Signature Generation /Verification**
Confidentiality	Symmetric or Asymmetric	-	-
Authentication	-	Symmetric or Asymmetric	Asymmetric only
Integrity	-	Symmetric or Asymmetric	Asymmetric only
Non-Repudiation	-	-	Asymmetric only

2.1 Digital Signatures

Digital signatures are created and verified by public key cryptography. The signer has a key pair consisting of a private key and a public key. The signer holds a private key known only to the signer, which the signer uses to create the digital signature. The signer also has a public key, which is used by a relying party to verify the digital signature. Relying parties must obtain the signer's public key in order to verify the signer's digital signature. As applied here, the principle of irreversibility means that it is computationally infeasible to discover the signer's private key from knowledge of the public key and use it to forge digital signatures. The digital signature cannot be forged unless the signer loses control of the private key by divulging it or losing the media or device (smart card) in which it is contained, or an attacker is, through the application of massive computing resources-performing cryptographic analysis, able to derive the private key from the public key.

This impossibility for retrieval of the input message is pretty logical if we take into account that a message's hash value could have a hundred times smaller size than the input message. Actually, the computing resources needed to find a message by its digest are so huge that, practically, it is infeasible to do it. It is also interesting to know that, theoretically, it is possible for two entirely different messages to have the same hash value calculated by some hashing algorithm, but the probability for this to happen is so small that in practice it is ignored (see also Stallings, 2006). From a technical point of view, the digital signing of a message is performed in two steps, and as depicted in Figure 1.

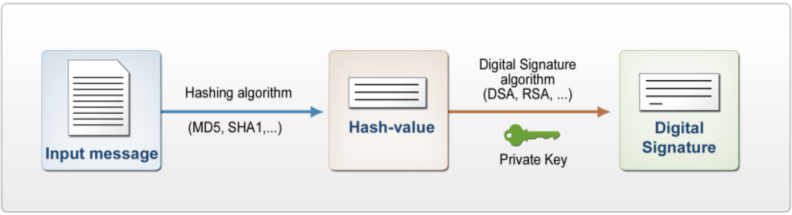


Figure 1: Digital Signing Process

2.2.1 Calculating the Message Digest

In the first step of the process, a hash value of the message (often called the message digest) is calculated by applying some cryptographic hashing algorithm (e.g., MD2, MD4, MD5, SHA1, or other). The calculated hash value of a message is a sequence of bits, usually with a fixed length, extracted in some manner from the message. All reliable algorithms for message digest calculation apply mathematical transformations such that when just a single bit from the input message is changed, a completely different digest is obtained.

2.2.2 Calculating the Digital Signature

In the second step of digitally signing a message, the information obtained in the message's first-step hash value (the message digest) is encrypted with the private key of the person who signs the message and thus an encrypted hash value, also called digital signature, is obtained. The most often used algorithms are RSA (based on the number theory), DSA (based on the theory of the discrete logarithms), and ECDSA (based on the elliptic curves theory). Typically, a digital signature (the transformed hash result of the message) is attached to its message and stored or transmitted with its message. It may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message.

2.2.3 Verifying Digital Signatures

Digital signature technology allows the recipient of given signed message to verify its real origin and its integrity. The process of digital signature verification is designed to ascertain if a given message has been signed by the private key that corresponds to a given public key. The digital signature verification cannot ascertain whether the given message has been signed by a given person. If we need to check whether some person has signed a given message, we need to obtain his real public key in some manner.

This is possible either by getting the public key in a secure way (e.g., on a floppy disk or CD) or with the help of the public key infrastructure by means of a digital certificate. Without having a secure way to obtain the real public key of given person, we are not able to check whether the given message is really signed by this person. From a technical point of view, the verification of a digital signature is performed in three steps as depicted in Figure 2.

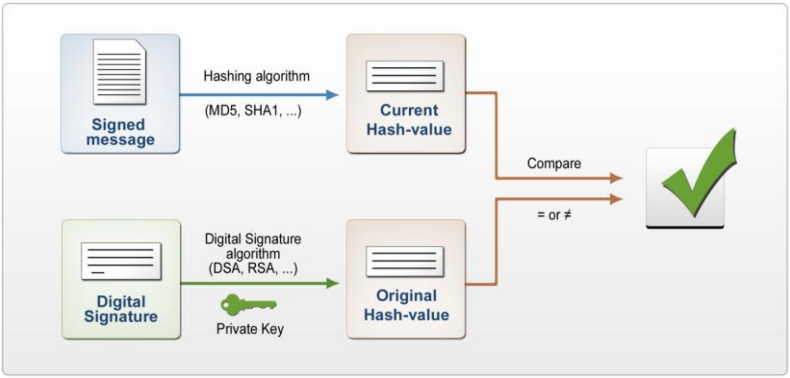


Figure 2: Digital signature verification process

Step 1: Calculate the Current Hash Value

In the first step, a hash value of the signed message is calculated. For this calculation, the same hashing algorithm is used as was used during the signing process. The obtained hash value is called the current hash value because it is calculated from the current state of the message.

Step 2: Calculate the Original Hash Value

In the second step of the digital signature verification process, the digital signature is decrypted with the same encryption algorithm that was used during the signing process. The decryption is done by the public key that corresponds to the private key used during the signing of the message. As a result, we obtain the original hash value that was calculated from the original message during the first step of the signing process (the original message digests).

Step 3: Compare the Current and the Original Hash Values

In the third step, we compare the current hash value obtained in the first step with the original hash value obtained in the second step. If the two values are identical, the verification is successful and proves that the message has been signed with the private key that corresponds to the public key used in the verification process. If the two values differ from one another, this means that the digital signature is invalid and the verification is unsuccessful.

2.2.4 Reasons for Invalid Signatures

There are three possible reasons for getting an invalid digital signature:

- If the digital signature is adulterated (it is not real) and is decrypted with the public key, the obtained original value will not be the original hash value of the original message but some other value.

- If the message was changed (adulterated) after its signing, the current hash value calculated from this adulterated message will differ from the original hash value because the two different messages correspond to different hash values.

- If the public key does not correspond to the private key used for signing, the original hash value obtained by decrypting the signature with an incorrect key will not be the correct one.

If the verification fails, in spite of the cause, this proves only one thing: The signature that is being verified was not obtained by signing the message that is being verified with the private key that corresponds to the public key used for the verification.

Sometimes, verification could fail because an invalid public key is used. Such a situation could be obtained when the message is not sent by the person who was expected to send it or when the signature verification system has an incorrect public key for this person. It is even possible that one person owned several different valid public keys with valid certificates for each of them and the system attempted to verify a message received from this person with some of these public keys but not with the correct one (the key corresponding to the private key used for signing the message).

In order for such problems to be avoided, most often when a signed document is sent, the certificate of the signer is also sent along with this document and the corresponding digital signature. Thus, during the verification, the public key contained in the received certificate is used for signature verification; if the verification is successful, it is considered that the document is signed by the person who owns the certificate.

2.2 Digital Certificates

The description of the use of digital signatures above leaves open one security question that must be resolved in an infrastructure for secure electronic commerce: How can the verifier obtain the alleged signer's public key in a way that ensures that the public key is, in fact, that of the signer? Some mechanism is necessary to avoid the scenario of an attacker intercepting the message, rewrapping the plaintext of the message with his own digital signature, and giving the verifier his own public key.

The attacker could pass off his own public key as if it were the public key of the intended signer. The verifier, using the attacker's public key, will find that the public key is able to process the digital signature on the message he received. Moreover, the verifier will think that the message originated with the signer, not the attacker. The verifier needs a mechanism to obtain the public key of the signer in a reliable way to avoid this kind of substitution.

Within a PKI, the method for preventing this kind of substitution attack is the digital certificate (Barr, 2002). A certificate is a message stating that a public key belongs to or is associated with a given individual, organization, or device. The party issuing the certificate is a certification authority, or "CA," and the party receiving it is called the subscriber. A digital certificate is itself a digitally signed message. The issuing CA signs the message with its private key.

The digital signature on the certificate itself provides assurances of the origin of the CA signing it, and the fact that the certificate has not been tampered with since issuance. Thus, the certificate is the CA's signed assertion that a particular public key belongs to a specific individual, organization, or device.

To the extent the relying party trusts the CA, the relying party can trust in this binding and use the public key in the certificate with confidence to verify digital signatures of the subscriber. Of course, if the certificate is a digitally signed message binding a subscriber to a public key, it is also necessary to obtain the CA's public key, or root certificate, to verify the digital signature on the certificate.

If the verifiers that need the root certificate are small in number, it is possible to distribute the root in person. Root certificates may also be distributed on media using trustworthy non-Internet delivery mechanisms, such as reputable courier services or even postal mail. While this option may be satisfactory for small communities, it is difficult to scale this solution to large populations. As a result, many CAs have arranged with software manufacturers to embed their roots within the software itself. Under this solution, when a verifier needs to refer to a root certificate, the root certificate is already within the verifier's software and is available for use. To date, this solution has proved to be the most effective method of distributing roots widely.

2.3 Data Encryption

In addition to digital signatures, public key technology may be used to encrypt messages in order to protect the confidentiality of the information contained within them. In the encryption process, the sender of the data to be kept confidential uses the recipient's public key to encrypt the data. The recipient uses the recipient's private key to decrypt the data. The principle of irreversibility here means that it is computationally infeasible for anyone intercepting the message and having knowledge of the recipient's public key to derive the private key and decrypt the data. Moreover, only the recipient, who holds that private key, will have the ability to decrypt the data.

Widely deployed encryption software, such as e-mail clients, can perform these encryption functions. This software, however, does not use the asymmetric key to encrypt the entire plaintext of the message. Asymmetric key operations tend to be costly in terms of time and computing power. Therefore, software commonly uses a symmetric key used only for this one operation (called a "session key") to encrypt the plaintext message and then, in turn, uses the recipient's public key to encrypt the symmetric session key.

The message sent to the recipient includes the encrypted message and the encrypted session key. The recipient then uses the recipient's private key to decrypt and recover the session key. The session key is then used to decrypt the message itself. As with digital signatures, a sender of a confidential message can obtain the public key of the recipient using the recipient's certificate.

2.4 Secure Sockets Layer (SSL)

One of the best-known uses of public key technology is the protocol known as the Secure Sockets Layer (SSL), which protects the communications between a browser on a client machine and a server over an insecure network, such as the Internet. People every day access e-commerce sites to purchase goods and services over the Internet, and wish to secure their sessions with these sites to protect the confidentiality of information such as credit card numbers. The magnitude of this everyday use of SSL to protect these sites indicates that SSL is by far the most widespread commercially deployed PKI technology. An SSL session consists of the following procedures:

- A browser sends a request to connect to a site that has a server certificate. The user performs this request by clicking on a link indicating that it leads to a secure site or the user types in a URL with an "https" protocol specifier.

- The server responds and provides the browser with the server's certificate.
- The browser verifies the digital signatures on the server certificate with reference to a certificate chain leading to a trusted root certificate.

- The browser also compares the server's domain with the domain listed in the certificate to ensure that they match. If these steps are successful, the server has been authenticated to the user, providing assurances to the user that the user is accessing a real site whose identity was validated by a CA. This process is called server authentication.

- Optionally, the server may request the user's certificate. The server can use the user's certificate to identify the user, a process called client authentication.

- The browser generates a symmetric session key for use by the browser and server in encrypting communications between the two.

- The browser encrypts the session key with the server's public key obtained from the server certificate and sends the encrypted key to the server.

- The server decrypts the session key using its private key.

- The browser and server use the session key to encrypt all subsequent communications.

Following these procedures, the user may notice a padlock symbol appearing on the screen. In addition, the user will be able to inspect the certificate on the site using the browser.

2.5 Biometrics

Biometrics is a term referring to the measurement of one or more biological characteristics of an individual, such as fingerprints, voice recognition, eye imaging, hand geometry, and the like. Primarily a form of identification and authentication, biometrics can enhance PKI and can be enhanced by PKI.

- A biometric can augment or replace the access control placed over a subscriber's private key.

- The integrity and authenticity of the biometric template can be ensured via digital signature and can even be enveloped within a digital certificate.

- The biometric reader device can be authenticated via PKI (similar to existing mechanisms used for point of sale (POS) and automated teller machines (ATM).

2.6 Key Management

Because cryptographic keys are very special pieces of data that require extraordinary handling, the subject warrants particular attention. Symmetric and asymmetric algorithms and their cryptographic keys all have different strengths, weaknesses, and properties that require distinct policy and practices to protect them.

The controls over the asymmetric private and public keys inherent in a properly deployed PKI ensure its reliability. For the public key, a digital certificate ensures the integrity and authentication of the subscriber's public key and provides the cryptographic binding between the subscriber's identity (and/or other attributes) and public key.

Key recovery is the ability to reconstitute a decryption key for the purposes of recovering encrypted data. This may be necessary in the event of a hardware failure, where the key has been lost, the untimely death of a person when the PIN guarding access to the key is no longer available, or other circumstances where encrypted data must be recovered.

In order to provide key recovery services, the PKI service provider may store activation data or the decryption key itself. The design and implementation of a storage and retrieval process will usually be specific to the PKI service provider and may involve a combination of chain of custody, dual control, split knowledge, encryption, and other techniques by the parties involved to provide procedural protections for the private key.

Private key recovery presents the security risks of unauthorized access to the private key, which can be used to decrypt sensitive information. In the case of single key pair schemes, in which one key services both signature creation and decryption purposes, there may be reasons for escrowing or managing the single key.

When such systems are used, unauthorized access to a private key also entails the risk that an attacker could create digital signatures using the recovered key and thereby impersonate the subscriber. Consequently, there is a business need to limit the circumstances under which a private key can be recovered and also control access to the private keys to prevent unauthorized private key recoveries. Circumstances under which recovery is appropriate or required generally fall into two categories: voluntary requests from the subscriber and requests for a subscriber's private key that originate from another responsible and authorized party, which are likely to be involuntary from the perspective of the subscriber.

2.7 Certificate Revocation List (CRL)

A CRL is a digitally signed list of revoked certificates' serial numbers that is generally issued by the CA that issued the (revoked) certificate. CRLs provide information regarding a certificate's status. CRLs are issued periodically and downloaded to relying party systems on a scheduled basis (e.g., every twenty-four hours. CRLs contain an issue date as well as the date that the next CRL should be issued.

The frequency of CRL issuance tends to reflect the risks and assurances associated with the certificates. In some cases, unscheduled "interim" or "delta" CRLs may be issued, particularly in the event of key compromises. CRLs have other advantages, and they have disadvantages as well. In addition to the short response time that a local CRL provides, a CRL may be a cost-effective means to validate certificates in low-value transactions in which the infrequent revocation of a certificate keeps the CRL relatively small. In such situations, the relying party's system can be designed to check for and pull down updated CRLs as often as convenience and risk management dictates. However, a CRL may only be considered valid at the time it is published. As the size of the CRL and the value of the underlying transaction grow, the CRL becomes a less cost-effective solution.

The solution chosen in some situations might include a combination of both CRL and status checking (for example, Online Certificate Status Protocol). Online mechanisms are capable of communicating the current (real-time or near real-time) status of a certificate. These mechanisms eliminate latency issues affecting CRLs, although they may introduce other risks (certificate status responder and Internet connection downtime). The predominant online revocation/status-checking mechanism is the IETF Online Certificate Status Protocol (OCSP). OCSP provides a standardized protocol for online status requests for specific certificates. Upon request, an OCSP "responder" provides a signed status response message that reflects the current status of the certificate. The responder's signature can be verified by the relying party.

The timeliness of any certificate status information depends on the implementation. Some OCSP responders are merely front-ends for CRL-based revocation systems or base their response on the most current operational records of the CA. In these cases an OCSP response will not contain more current information than the CRLs. Relying parties may need to retain OCSP responses used to verify signatures, since each response is unique to a particular transaction. OCSP is only one of many types of online checking mechanisms.

3. UAE PKI SYSTEM

During the early phases of the project, the PKI Applet on the card was a contentious issue. Although the purpose of the PKI applet was understood and the need for e-services realized, the application and services associated with it were only broadly understood at the time. It was decided to have a container that would have three key pairs, one for logical access or authentication, one for digital signing, and a third reserved for possible future use for data encryption and decryption. The container was designed to be personalized with the rest of the card and protected with a user PIN. The validity of the digital certificates (keys) in the card has the same lifetime as the card, which could be a maximum of up to five years. A new set of keys would need to be reissued with a new card and the expired public key certificates published in a revocation list.

From a system perspective, no copy is kept of the keys that are generated for an ID card. The keys are generated by the HSM and securely exported and loaded onto the card, after which the keys are deleted from the system. No key backup or archival (except for the CA root key) is done. Due to the fact that no data encryption and decryption is done, there was no need for key recovery at that stage. However, if a third certificate is implemented for data encryption and decryption, the need for key recovery has to be investigated. Not only is private key recovery important for data decryption purposes, but also public key archival might be needed for digital signature certificates. For example, when a legal document is signed and has a lifespan that exceeds the validity period of the card and therefore the certificates, the signature can no longer be verified unless the public key of the original digital signature is archived with the document or available from the CA authority for verification.

It is clear that the use and application of the PKI component of the ID card needs to be well defined and communicated in the Certificate Practice Statement. All partners and role players will also play a significant role in determining the scope and parameters of PKI use of the ID card.

Finally, federal and international law will dictate certain aspects of PKI usage and aspects like key recovery, usage, and conditions for non-repudiation will determine implementation requirements. Taking all this into account, the current PKI is only in its beginning phase. In order to fulfill the usage requirements of the PKI component on the ID card, it will be necessary to plan a proper and well-designed architecture for the PKI needs in context of other government departments and GCC[26] countries. The following subsections elaborate on the primary components of the UAE PKI project.

3.1 ID Card PKI Applet

The PKI applet provides the digital signature and authentication features in the form of digital certificates. The applet can accommodate three separated key sets and their associated digital certificates, as well as a user PIN code to prevent unauthorized use of these functions. One certificate is for authentication, one is for the digital signature, and one free empty key container is for future use. With the installed certificates and keys the user can be authenticated and can digitally sign e-commerce and e-government applications.

The certificates are in accordance with the X.509 standard. Together with the PKCS#11 cryptographic library and a CSP (cryptographic service provider for Microsoft Cryptographic API) the user uses Web Browsers (SSL v3 sessions), e-mail (S/MIME), VPN, and other PKI applications securely. For the hashing function SHA-1 is used and for asymmetric cryptographic functions the RSA algorithm is used.

During card personalization, the digital signature and the authentication certificates are loaded onto the ID card chip. The keys on the ID card are able to perform cryptographic functions but

[26] GCC is the acronym for Gulf Cooperation Council, also referred to as the Cooperation Council for the Arab States of the Gulf (CCASG). It includes six countries: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. The number of GCC population is estimated to be around 40 million people.

the decryption function is blocked. The blocking is necessary so that a key cannot be misused for a decryption function. For additional encryption and decryption and/or digital signature keys, the additional container can be used, but the keys are not loaded during the personalization. If the keys for encryption/decryption are loaded, a mechanism of key recovery must be implemented to guarantee that the private key can be restored in case of a lost or damaged card. Otherwise, the user would not be able to decrypt any data that has been encrypted previously.

The private keys for the digital signature and authentication functions are not held in the system, but are loaded once into the smartcard. It cannot be offloaded later on and will be used by the smartcard to perform cryptographic functions. If a card has been damaged, lost, or renewed, the user should be issued with a new card with new certificates.

3.2 UAE PKI Infrastructure

The UAE system employs multiple Certificate Authorities (CAs) to deal with key requirements for the population, time, and technical aspects of the system. For the purpose of this discussion we are concerned with the population CA, which issues and sign keys and certificates for use in the ID card. The next subsections highlight possible caveats of the PKI infrastructure.

3.2.1 Activating the Private Key

The private key is the most important piece of data that needs to be protected. For the CA, the private key security is so important that it is physically stored on a hardware cryptographic module and protected by split authentication and various other physical access controls. Compromise of this key invalidates all the issued certificates by the CA and thus any digital transaction performed with the keys and certificates in question. The CA private key is stored in a hardware security module and protected adequately through various means.

The ID cardholder's private key is generated in the HSM and transferred to the ID card during personalization. The private key is activated through the use of a user PIN. This means that the most important piece of data, as far as an ID cardholder is concerned, is currently only protected by a minimum four-digit numeric password, better known as a PIN. If the ID card is stolen and the PIN very easily stolen through mechanisms like social engineering or shoulder surfing, the private key is compromised.

A more secure way to protect a private key is to activate it using a biometric instead of a PIN—in some cases using both. Match-on-card technology is a great way to authenticate a cardholder using his smartcard without having to have a complex online system available. Because the cardholder can be uniquely authenticated using his biometric, it serves as the best way to unlock protected information on his/her card (like the private key). In the UAE system, the match-on-card functionality is separate and serves no access control purpose, only cardholder authentication.

There is always a balance between security, ease-of-use, and functionality in any system—increase one and the other two will decrease. By using the biometric to activate the private key will provide the ultimate security but will limit the use of the PKI services to match-on-card-only applications and readers. The decision to use the biometric as access control mechanism for the PKI applet instead of a PIN can only be made once the nature of e-services is better defined and the requirements from partners and role players better understood.

3.2.2 Verifying Digital Signatures

As already explained, digital signatures are verified with a signer's public key and the public key certificate is verified with the CA's root certificate. Furthermore, the validity of both the public key certificate and the CA root certificate is verified against the CRL. Off hand, there is some serious infrastructure needed to fulfill the requirements just mentioned.

First of all, public key certificates must be distributed to all partaking entities to verify digital signatures. Depending on the application, the public keys might be queried from a central repository or embedded as part of the signed transaction and thus verified without any additional infrastructure. This is the preferred way but is not always supported by the application software of a specific digital signature application. The problem with the central repository for public keys is not only the fact that it requires infrastructure but also heavy maintenance: Once cards get renewed there will be more than one version of a public key for a particular cardholder; transactions signed must be verified with the correct version of the public key; obsolete public keys must be removed, and so on.

Secondly, the public key certificate of a cardholder must be verified against the CA root certificate. This is to ensure that the cardholder is whom he says he is and his certificate has indeed been issued and signed by the Identity Authority. In a commercial scenario the root certificates of the most popular CAs are embedded in software like browsers, but for standalone CAs the root certificate has to be made available to any entity that requires validation. The pitfall is that the certificate itself does not need to be secure (it has already been signed with the CA's private key) but the mechanism in obtaining It has to be secure. This is because a fraudulent certificate, checked against the correct CA but fraudulent one, will validate correctly.

Many organizations embed their root certificates as part of the PKI-enabled applications. Although this mostly solves the problem, it is difficult to keep up to date as to the correct version of the root certificate (if it was renewed or compromised). Other organizations prefer to publish the certificate on their corporate websites. This might sound like the best and simplest idea, but it is not secure and an entity may never be sure whether it is referring to the correct site and correct certificate. The alternative is to install the root certificate on the card, together with the cardholder's certificates. This way, the root certificate is always accessible and up to date because when the card gets replaced so does the root certificate. It travels with the cardholder and can always be verified without any external checking.

Thirdly, both the public key certificate and the CA root certificate have to be validated against the CRL. The CRL simply keeps a list of certificate serial numbers and whether they are valid or not. Currently the CRL is published and stored as a single file in the Demilitarized Zone (DMZ).[27] However, no infrastructure currently exists to access and check against this file from an external entity. The CRL will be explained later in more detail.

3.2.3 Verifying Access Control Certificate

The second certificate in the card is used for authentication, or more technically, logical access control. This includes things like SSL client authentication, for example. Because logical access is one-time only or while a session exists, it is considered temporally and therefore does not have the certificate lifetime and archival issues associated with digital signature certificates and data encryption certificates. Instead, the only issues are validating the CA root certificate and CRL-related issues, as explained in the previous section with digital signature validation.

3.2.4 Certificate Validation

Certificate validation is what it is all about. Verifying the authenticity and validity of a certificate (it is the public key) is a crucial process in ensuring the integrity of a PKI system. The CRL performs this function and the CRL is generated on a daily basis and stored in a single file output and transported to the DMZ. There are basically three problems to address when dealing with CRL information:

[27] The Demilitarized Zone (DMZ) is a physical or logical sub-network that contains and exposes an organization's external services to a larger un-trusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

A single CRL file grows too big—as certificates gets added to the CRL the file will grow in size, and each time a client requires the CRL information it will attempt to download the file in order to check it. In a relatively small environment this will still suffice, but dealing with thousands of certificates will make the single file solution inadequate. In the context of the UAE system, in which millions of certificates will eventually end up on the revocation list, a single file will grow up to hundreds of megabyte and will be impractical to use in this environment.

A single file is not suitable for a distributed environment—accessing a single file is fine when the environment and the number of CRL queries are fairly small. However, from industry evolution it is clear that a single file solution for any scenario has its limitations and cannot scale very well. Take Windows NT and its single authentication file in the form of a SAM file: It was just a matter of time before Microsoft had to replace this technology with something that could scale and be distributed across a large infrastructure. The answer was a directory service, and Active Directory (like NetWare, iPlanet, IBM, and others) is a lightweight directory access protocol (LDAP). A LDAP is usually implemented with an online certificate status protocol (OCSP). A directory service with an access protocol makes the update and query much more efficient and reliable.

A CRL is accessed by both the secure CA as well as the less secure client queries—with a single CRL file, both secure agents, like the CA and less secure agents such as clients, require access to the CRL file. This is not the ideal way to maintain the level of security usually associated with a CA environment.

As the CRL grows in size and the number of requests increases, a distributed environment is the only proper solution for the demands of such an infrastructure. In a distributed environment multiple nodes, called responders, provide up-to-date CRL information in multiple points across the PKI footprint. Security is also addressed in the sense that the responders live in an unsecured environment but receive signed copies of the revocation information from the secured LDAP and distribution server, which can either be online or offline. With the size of the UAE PKI infrastructure in the form of number of certificates and role players in the future, this is definitely a recommended option to look at in order to comply with scalability, reliability, and security needs.

3.2.5 Level of Trust

As already mentioned, validating the CA certificate is an important part of the trust associated with a PKI infrastructure. The identity issuing authority implemented a standalone CA, which does not have a trusted path associated with the commercial CAs. This in itself is not a problem, but it means that the root CA certificate of the issuing authority has to be distributed to all entities that will require CA certificate validation. This becomes a challenge, as other departments or even other countries use their own CAs with their own infrastructure. In the commercial world, cross-certification is the way to carry the trust of one CA over to another CA, resulting in implied trust through a trust path.

Due to security, autonomy, and other considerations, this might not be an appropriate solution, especially not when other countries are involved. Using a concept called bridge-CA might be a better solution, in which different departments or countries may use a joint bridge-CA instead of explicitly signing each other's root certificates. With the focus on GCC cooperation and interoperability, this solution might be considered in the future and is recommended above cross-certification.

3.2.6 Data Encryption

The final point to discuss is that of data encryption services, the one thing that currently does not exist in the UAE PKI infrastructure. Although a third certificate slot has been reserved in the PKI applet of the ID card for future purposes of data encryption/decryption, a very important aspect of the PKI infrastructure needs to be considered first—that of key recovery.

In an environment in which data is encrypted for storage—not only for the duration of a session like with the authentication certificate—key recovery becomes an issue. First of all, a private key holder (typically a cardholder) may lose his/her card or damage it. In this scenario the private key is lost and any data encrypted with the particular person's public key can no longer be decrypted. The ramifications might be huge if large amounts of sensitive information and even personal information are lost this way.

Second, in today's information age, in which criminal activities usually have a digital footprint and trail, the necessity for authorities to have access to data of any organization or individual when the need arises is crucial. Having no way to access encrypted information literally puts a blindfold on law enforcement activities.

It is clear that both from availability and law enforcement points of view, the need for key recovery has to be evaluated and considered very closely. An issue with having a form of private key backup is the fact that these keys need to be protected very well and the process of recovery has to be well defined and justified. This aspect of any PKI infrastructure has to be communicated to all certificate holders in very clear terms in the certificate practice statement. The certificate holder should have the confidence that he/she may be able to recover lost data in the event of a lost private key, but also that the Certificate Authority will not abuse its position of maintaining a copy of the backup keys.

A very important point to highlight is that the keys for digital signatures and data decryption will preferably not be the same keys. This might sound strange, but think of it for a moment. If the private key is backed up or escrowed (managed by a third party), the non-repudiation associated with a digital signature is no longer valid. This is because another private key exists, which is fine for recovering encrypted data in the event of key loss, but not fine when it comes to ensuring non-repudiation with singed transactions. This is the reason why there are two distinct certificates—digital signature certificates require archival of the public keys while data encryption certificates require archival/back-up of the private keys. In the UAE system no key recovery or private key escrow exists. It was very important that key recovery requirements be understood before attempting to implement data encryption services within the

ID card. It is recommended to have the architecture in place before any decisions are made as to making data encryption/decryption available on the ID card.

CONCLUSION

This article has presented an overview of the major PKI components deployed in the UAE national identity management infrastructure, with emphasis on the practical side of the implementation. The UAE PKI infrastructure is only in its beginning phase and will grow as the need for e-services increases. It was important to understand all the aspects of the infrastructure and what the limitations and strengths of various implementations and uses are. It was also very important to get the architecture right up front before implementing the bulk of e-services.

Due to the complex nature and security requirements of a PKI infrastructure, mistakes in the architecture cannot be easily rectified at a later stage and proper planning is of the utmost importance. There was a clear need to understand the full specifications of CA, its supported standards, and related services. This should facilitate the development of e-service applications and extending the existing infrastructure.

Furthermore it was recommended to establish and maintain a regular interaction with other e-government role players, Etisalat, which the local telecom operator in UAE that is in charge of the commercial CA, and any UAE lawmakers as far as e-commerce and digital communications security is concerned. The proposed approach was to have a forum in which role players can share knowledge and experience, and in which the future roadmap of requirements and interoperability is discussed on a regular basis.

REFERENCES

[1] Barr, T.H. (2002). Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall.

[2] Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. New York: John Wiley & Sons.

[3] GAO (2001) "Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology", United States, General Accounting Office report GAO-01-277, February 2001.

[4] Judge, P. (2002) PKI is failing, say Sun and Microsoft, ZDNet.com.au. [Online]. Available from: http://www.zdnet.com.au/pki-is-failing-say-sun-and-microsoft-120268957.htm

[5] Kuhn, D.R.; Hu, V.C.; Polk, W.T. and Chang, S.J. (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure, National Institue of Standards and Technology (NIST) [Online]. Available from: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf Accessed [12 October, 2011].

[6] Lloyd, S. and Adams, C. (1999) Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations. Sams Publishing.

[7] Pluswich, L. and Hartman, D. (2001) "Prime-Time Player?", Information Security Magazine, March.

[8] Rothke, B. (2001) "PKI: An Insider View", Information Security Magazine, October 2001.

[9] Schwemmer, J. (2001) Solutions and Problems - (Why) It's a long Way to Interoperability. Datenschutz und Datensicherheit 25(9).

[10] Spillman, R.J. (2005). Classical and Contemporary Cryptology. Upper Saddle River, NJ: Pearson Prentice-Hall.

[11] Stallings, W. (2006). Cryptography and Network Security: Principles and Practice, 4th ed. Englewood Cliffs, NJ: Prentice Hall.

Article 7

The Role of Digital Certificates in Contemporary Government Systems:

The Case of UAE Identity Authority [28]

DR. ALI M. AL-KHOURI

ABSTRACT: Digital certificates provide advanced instruments for confirming identities in electronic environments. The application of digital certificates has been gaining global acceptance both in public and private sectors. In fact, the government field has witnessed increasing adoption of cryptographic technologies to address identity management requirements in cyberspace. The purpose of this article is to provide an overview of various governmental scenarios on the usage and application of digital certificates in the United Arab Emirates. The UAE government integrated public key infrastructure (PKI) technology into its identity management infrastructure since 2003. The article also explores the UAE digital identity issuing authority's position regarding government-to-government transactions and the prospective role of digital certificates.

Key words: *Public key infrastructure, digital certificates, UAE Identity Management Infrastructure, e-government.*

[28] Al-Khouri, A.M. A (2012) "The Role of Digital Certificates in Contemporary Government Systems: the Case of UAE Identity Authority", **International Journal of Computer Science Engineering and Information Technology Research**, Vol. 2, No. 1, pp. 41-55.

1. INTRODUCTION

INFORMATION and communications technology has demonstrated the engine capacity to transform the way businesses operate, the way that government can deliver, and the way scientific research is undertaken to improve society. In an ever-changing world, being able to respond rapidly to new opportunities and challenges is crucial to the future economic and social prosperity of the world (Greenstein & Vasarhelyi, 2002; Shaw, 2006). The rapid development of Information and Communication Technologies (ICT) is forcing governments to adopt more rigorous development plans to revolutionize their operations, service delivery channels, and the way they interact with citizens.

Virtual space, electronic banking, and other electronic services are becoming more commonplace, offering the convenience and flexibility of round-the-clock service direct from the comfort of home. However, there is an increasing concern both from individuals and organizations about the privacy and security associated with electronic transactions (Germain, 2003). Encryption seems to be insufficient by itself because it provides no proof of the identity of the sender of the encrypted information. Digital certificates have emerged as a compelling technology, able to provide higher levels of security and assurances of electronic identities and content integrity.

This article provides an overview of a government program and the potential use of digital certificates. We attempt to outline the different scenarios formulated during discussions in the implementation phases of the UAE national identity management infrastructure, which was first launched in 2003. The main purpose of this article is to explore the UAE digital identity issuing authority's position with regards to G2G e-government transactions and the prospective role of digital certificates. This article is structured as follows: The first section provides a short overview of the digital certificates and their role in electronic transactions. The second section provides an overview of the UAE Identity Authority and digital certificates. It outlines the possible scenarios of the application of government issued digital certificates, and outlines the general architecture of UAE identity infrastructure and the technical components related to digital certificates.

2. DIGITAL CERTIFICATES

Digital certificates are digital files that certify the identity of an individual or institution seeking access to computer-based information. By enabling such access, they serve the same purpose as a driver’s license or library card. Digital certificates bind the identity of an individual or institution to a digital public key, i.e., to a pair of electronic keys that can be used to encrypt and sign digital information. The combination of standards, protocols, and software that support digital certificates is called a public key infrastructure, or PKI. The software that supports this infrastructure generates sets of public-private key pairs. Public-private key pairs are codes that are related to one another through a complex mathematical algorithm. The key pairs can reside on one’s computer or on hardware devices such as smart cards or floppy disks.

Through digital certificate, it is possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using phony keys, for example, to impersonate other users. Used in conjunction with encryption, digital certificates provide a more comprehensive security solution, assuring the identity of all parties involved in a transaction.

A digital certificate is issued by a Certification Authority (CA) and signed with the CA's private key. A digital certificate typically contains the following elements: (1) owner's public key, (2) owner's name, (3) expiration date of the public key, (4) name of the issuer (the CA that issued the digital certificate), (5) serial number of the digital certificate, and (6) digital signature of the issuer. The most commonly accepted format for digital certificates is defined by the ITU X.509[29] international standard; thus, certificates can be read or written by any application complying with X.509. Further refinements are found in the PKCS[30] standards and the PEM[31] standard.

[29] ITU X.509: a widely used standard for defining digital certificates. X.509 (Version 1) was first issued in 1988 as a part of the ITU X.500 Directory Services standard. When X.509 was revised in 1993, two more fields were added resulting in the Version 2 format. These two additional fields support directory access control. X.509 Version 3 defines the format for certificate extensions used to store additional information regarding the certificate holder and define certificate usage. Collectively, the term X.509 refers to the latest published version, unless the version number is stated. X.509 is published as ITU recommendation ITU-T X.509 (formerly CCITT X.509) and ISO/IEC/ITU 9594-8 which defines a standard certificate format for public key certificates and certification validation. With minor differences in dates and titles, these publications provide identical text in the defining of public-key and attribute certificates.

[30] PKCS: is an abbreviation for Public-Key Cryptography Standards, and it refers to the set of standards for public-key cryptography, developed by RSA Laboratories in cooperation with an informal consortium, originally including Apple, Microsoft, DEC, Lotus, Sun and MIT.

Figure 1 depicts an example of various methods for access control that can be integrated with a digital certificate infrastructure, e.g., Kerberos[32], passwords, and in-person ID (DLF and CREN, 2000).

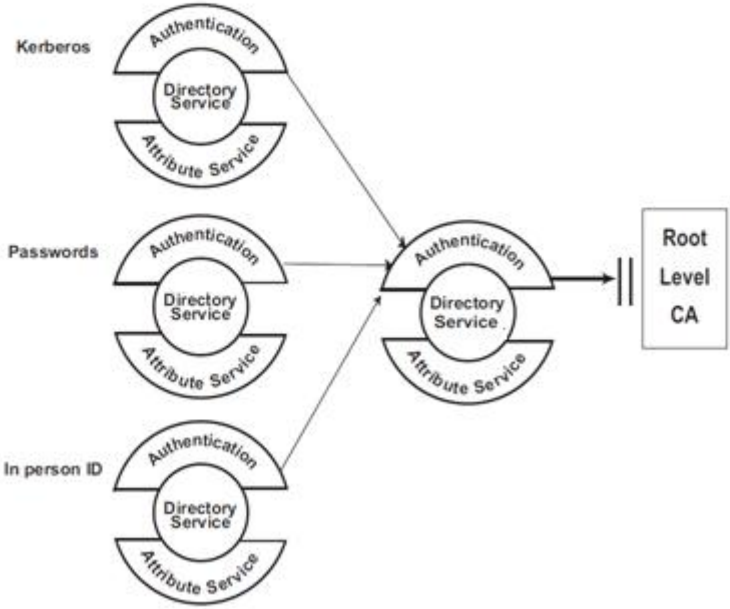


Figure 1: digital certificate application in a university campus

Source: DLF & CREN (2000)

[31] PEM: is an abbreviation for Privacy Enhanced Mail (RFC 1421 - RFC 1424), an early standard for securing electronic mail (IRTF, IETF). PEM never has been as widely adopted as Internet Mail Standard.

[32] Kerberos is a secure method for authenticating a request for a service in a computer network. Kerberos was developed in the Athena Project at the Massachusetts Institute of Technology (MIT). The name is taken from Greek mythology; Kerberos was a three-headed dog who guarded the gates of Hades. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network.

These methods rely on some form of directory service to authenticate a user for access to a service or resource. In this illustration, the Main Directory Service is represented by the LDAP Authentication Database.

Figure 2 depicts an example of the flow of information between a publisher's server and a user's computer using digital certificates. In this example, the client attempts access to a controlled resource from a publisher, such as a database or digital library, usually through a Web interface. The publisher's server asks the client to present a certificate. The client presents a certificate, and the publisher's server verifies that the certificate is authentic and authorizes access to the content.

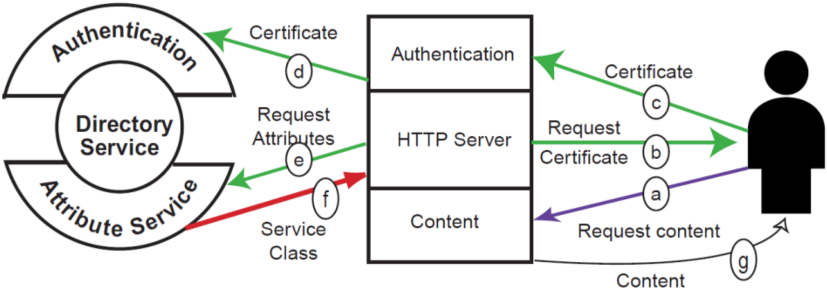


Figure 2: digital certificate authentication process

Source: DLF & CREN (2000)

As governments continue to invest significantly in the development and deployment of e-government solutions, there is a global movement towards using digital certificates to authenticate and authorize secure interactions over virtual networks. This section attempted to outline the application of digital certificates as a method for authentication. The next section looks at the digital certificate infrastructure implementation in the United Arab Emirates.

3. THE UAE IDENTITY AUTHORITY

In 2003, the government of the UAE began the use of digital certificates aspect of its public key infrastructure technology deployment which was integrated with the national identity management infrastructure development program (Al-Khouri, 2011; Westland & Al-Khouri, 2010). A federal Identity Authority was established in 2004 to oversee the implementation of the program and the issuing of digital certificates in the form of smart identity cards to all members of the population. Currently more than half of the population have been registered, and the remaining five million people are expected to be enrolled by 2013.

Each individual goes through a rigorous registration process where fingerprints and photos are captured at one of more than fifty registration centers in the country. The biographical data and biometrics are then processed centrally and go through automated and human validation systems which either grant or reject the issuing of identity cards.

The government is planning to achieve a strategic objective from this project: to support e-government and e-commerce initiatives. The use of public key infrastructure will enable the establishing of a secure channel for communicating any sensitive information between the different parties in an electronic environment.

Generally, once a digital certificate is obtained, one may set up security-enhanced web or e-mail applications to use the digital certificate automatically.

Theoretically speaking, the use of digital certificates in e-government communications is relatively straight forward (Babaoglu, 2003). The UAE Identity Authority is in a position to issue digital certificates to government entities that want to connect to the government Identity Authority. The certificates will be used for establishing secure communications and mutual authentication between the participating parties.

Extension of these services to include secure e-mail and data encryption falls outside the scope of this paper. For the moment, it is assumed that the requirement is only to use digital certificates in secure communication channels; therefore, it was recommended that the existing technical CA be used for such a purpose, which is a matter of issuing the certificates with no additional infrastructure required. The reasons for this are explained in later sections of this article.

3.1 UAE PKI Strategy Overview

As indicated earlier, there have been several discussions during the project implementation about the necessary infrastructure to extend the UAE PKI to facilitate e-services for ID card holders. There are challenges with this requirement since ID card holders will not only authenticate themselves but use digital signatures; possibly encryption at a later stage, and they will travel around and require services from various locations. Each of these requires an extensive infrastructure which includes card readers, access to public key repository, access to the CRL repository, LDAP-accessible directory services, key escrow, etc.

For the purpose of this discussion, this paper will only focus on the need for authentication (using digital certificates) between devices in a government-to-government (or e-government) scenario.

The Political Question

Prior to getting into the technical aspects of the discussion, it was necessary to deal with some political questions in order to understand the various scenarios that might be encountered during the design of the system. Some questions were:

1. Who will be the ultimate certificate authority issuing digital certificates in the UAE?
2. Will the commercial certificate authority be the same as the government certificate authority?
3. What are the roles of commercial CAs offered by the telecom companies in the country and the Identity Authority within the digital certificate space?

3.1.1 Scenario 1 – a single CA for the UAE

Since telecom operators in the UAE run commercial CAs, they have already invested in the infrastructure and conformed to the strict requirements of hosting a trust center. The natural conclusion would be to assume that they are in the best position to provide PKI services for the government as well. This means that the UAE Identity Authority need not concern itself with any additional infrastructure regarding e-government services or ID card holder's e-services. In addition, it need not be concerned with digital certificates all together; they may act as a registration authority for the national CA, only verifying identities and approving certificates on behalf of the national CA. This, however, might not be in the best interest of national security and hence the Identity Authority.

3.1.2 Scenario 2 – separate commercial and government CAs

The second scenario is that of having two separate CAs, one for commercial services and one for government services. These two CAs may autonomously function on their own and on the same level of authority. While telecom companies can perform the function of commercial CAs, the Identity Authority may perform the function of the government CA.

The UAE Identity Authority is already issuing certificates for ID card holders but require the necessary infrastructure to facilitate the PKI services beyond the boundary of the national identity management infrastructure. In addition, the necessary legislation needs to be in place to have the Identity Authority function as the official government CA.

3.1.3 Scenario 3 – hybrid CAs

The third scenario is to have the government Identity Authority provide limited PKI services in the form of ID card holder certificates and some e-government certificates, but to let the telecom companies provide integration and necessary infrastructure services. The details of such a hybrid solution are not important now, but such a solution may prove to be the best strategy for the short term. The technical discussion will resolve around the assumption that this scenario is the current way forward.

3.2 The UAE Identity Infrastructure

3.2.1 Identity System Technical CA

From the definition, a Certificate Authority (CA) is a trusted organization that maintains and issues digital certificates. The UAE Identity Authority currently has two root CAs: the Population CA and the Technical CA.

The Population CA is used to issue and sign the ID card holders' certificates, which are exported to the ID cards. The Technical CA is used to issue and sign various certificates used in the national identity management system: web servers, administration tools, network appliances, fingerprint devices, etc. A few subordinate CAs exist in a hierarchy below the Technical CA: the Timestamp CA, Server CA, Admin CA, and MSO CA. The following diagram depicts a logical representation of the UAE identity management system CA design:

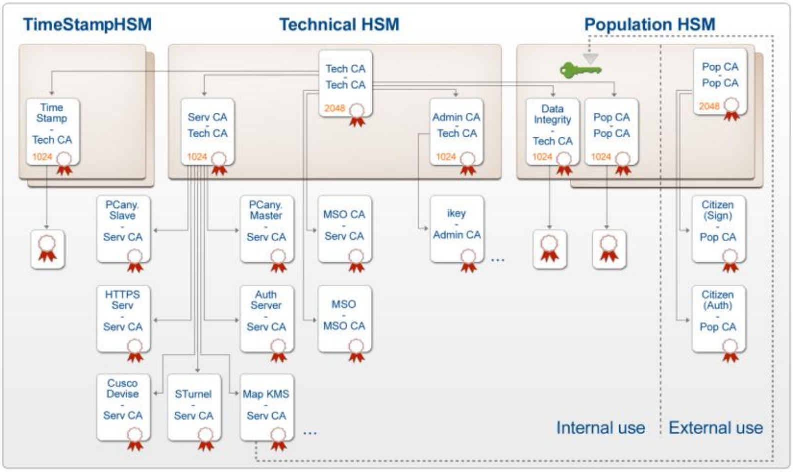


Figure 3: logical CA design

In order to accommodate the issuance of third-party certificates (e.g., that of other government departments), the certificates can simply be issued from one of the existing subordinate CAs, or a new subordinate CA can be created just for that purpose. In this case, it is recommended that a third-party CA be created under the Technical CA on the same level as the Server and Admin CAs. The process would typically work as follows:

1. A government entity wants to connect to a server in the Identity Authority DMZ.
2. The connection and associated infrastructure is provided by the government entity and installed in accordance with the Identity Authority security policy.
3. The government entity applies for a server (or client) certificate from the Identity Authority.

4. The Identity Authority issues the certificate from the technical CA.
5. The certificate gets installed in the device / client / server of the government entity.
6. The connection between the government entity and the Identity Authority can now be mutually authenticated and encrypted on the upper layers of the protocol stack (i.e., SSL, SSH, etc.)
7. The CRL is made available in the DMZ, so no need for further infrastructure.

This is a simplified process, but it demonstrates the use of digital certificates that are issued from the Identity Authority to authenticate and encrypt communications between the Identity Authority and other government departments. The number of such certificates will be much less than the ID card holders' certificates. Therefore the need for OCSP and a LDAP-accessible CRL is not necessary. This simplifies the solution even further.

3.2.2 Level of Trust

Validating the CA certificate is an important part of the trust associated with a PKI infrastructure (Mohapatra, 2001). The Identity Authority uses a stand-alone CA, which does not have a trusted path associated with the commercial CAs. This in itself is not a problem, but it means that the root CA certificate (public key) of the Identity Authority has to be distributed to all entities to provide CA certificate validation. This is not a problem as long as it has control over the distribution and use of the issued certificates, meaning that whenever a certificate is issued, the root CA certificate is installed with it. If, however, the certificates will be used among government entities other than the Identity Authority, the root CA certificate must be published in a central location for everyone to access or be distributed to all government entities on a per request basis.

3.3 Certificate Uses

The scope of the e-government certificates will determine the extent of the PKI infrastructure required. The use of certificates for session authentication (e.g., SSL), as opposed to digital signatures and file encryption, allows for a much simpler infrastructure. The current infrastructure supports the use of digital certificates for this purpose within the national identity management system environment. Extending this to other government departments will be technically straight forward and will not require major changes or additions, assuming that it does not involve digital signatures and data encryption.

3.3.1 Secure Sockets Layer (SSL)

One of the best-known uses of public key encryption is the protocol known as the Secure Sockets Layer (SSL), which protects the communications channel. Every day, people access e-commerce sites to purchase goods and services over the Internet, and wish to secure their sessions with these sites to protect the confidentiality of information such as credit card numbers. The magnitude of this everyday use of SSL to protect these sites indicates that SSL is by far the most widespread commercially employed PKI technology. A typical SSL session consists of the following procedures:

- A browser sends a request to connect to a site that has a server certificate. The user performs this request by clicking on a link indicating that it leads to a secure site, or the user types in a URL with an "https" protocol specifier.

- The server responds and provides the browser with the server's certificate.

- The browser verifies the digital signatures on the server certificate with reference to a certificate chain leading to a trusted root certificate.

- The browser also compares the server's domain with the domain listed in the certificate to ensure that they match. If these steps are successful, the server has been authenticated to the user, providing assurances to the user that the user is accessing a real site whose identity was validated by a CA. This process is called server authentication.
- Optionally, the server may request the user's certificate. The server can use the user's certificate to identify the user: a process called client authentication.

- The browser generates a symmetric session key for use by the browser and server in encrypting communications between the two.

- The browser encrypts the session key with the server's public key obtained from the server certificate and sends the encrypted key to the server.

- The server decrypts the session key using its private key.

- The browser and server use the session key to encrypt all subsequent communications.

Following these procedures, the user may notice a padlock symbol appearing on the screen. In addition, the user will be able to inspect the certificate on the site using the browser. SSL with HTTP is the only way to implement the technology. It can be used in many other services as well: SSL / LDAP; SSL / FTP; SSL / SMTP; etc. This will likely be the most used application of digital certificates in e-government implementation.

3.3.2 Secure Shell (SSH)

Secure Shell provides terminal-like access to remote computers by using a tunneling mechanism. It is especially useful in remote maintenance and troubleshooting and provides authentication and secure transmission. SSH is often used to replace Telnet, FTP, and the R-protocols in UNIX (e.g., rlogin, rexec, rsh).

3.3.3 IPSec

IPSec is used to set up a secure channel for protecting data exchange between two devices. It is currently used between sites in the national identity management system network, so it will not be explained in detail. Basically the most common implementation of IPSec is the use of symmetric key encryption rather than asymmetric (public key encryption), due to the speed advantage.

3.3.4 Secure MIME (S/MIME)

Secure MIME is a standard for encrypting and digitally signing electronic mail that contains attachments and for providing secure data transmissions. S/MIME provides confidentiality through the user's encryption algorithm, integrity through the user's hashing algorithm, authentication through the use of X.509 public key certificates, and non-repudiation through cryptographically signed messages. It should be noted that using S/MIME within an e-government scenario will require extension of the PKI infrastructure, especially when e-mail encryption is used.

CONCLUSION

This article has presented an overview of various scenarios of the usage and application of digital certificates in the United Arab Emirates. For the short term, the UAE Identity Authority can extend its technical CA services to third-party government entities with little effort, depending on the scope and configuration of the requirement. For the long term, it needs to position itself strategically. It will be vital to have a roadmap for PKI services in the UAE (the government specifically) and the role of the UAE Identity Authority, in addition to its relationship with telecom operators.

REFERENCES

[1] Al-Khouri, A.M. (2011) "PKI in Government Identity Management Systems", International Journal of Network Security & Its Applications, Vol.3, No.3, pp. 69-96.

[2] Babaoglu, O. (2003) Certificates, Certification Authorities and Public Key Infrastructures [Online]. http://www.cs.unibo.it/babaoglu/courses/security/lucidi/PKI.pdf, Accessed [10 October, 2011].

[3] DLF & CREN (2000) Digital Certificate Infrastructure: FAQ, Digital Library Federation & Corporation for Research and Educational Networking, http://www.diglib.org/architectures/cren-dlf.pdf Accessed [10 October, 2011].

[4] Germain, J.M. (2003) Beyond Biometrics: New strategies for security, E-Commerce Times
Online]. http://www.ecommercetimes.com/perl/story/31547.html Accessed [10 October, 2011].

[5] Greenstein, M. and Vasarhelyi, M. (2002) Electronic Commerce: Security, Risk Management and Control, McGraw-Hill, New York.

[6] Mohapatra, P.K. (2001) Public Key Cryptography, ACM Crossroads Student Magazine [Online]. http://www.acm.org/crossroads/xrds7-1/crypto.html Accessed [10 October, 2011].

[7] Shaw, M.J. (Ed.) (2006) E-Commerce and the Digital Economy. M E Sharpe Inc.

[8] Westland, D. & Al-Khouri, A.M. (2010) "Supporting e-Government Progress in the United Arab Emirates", Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

Identity and Access Management

Article 8

Optimizing Identity & Access Management (IAM) Frameworks[33]

DR. ALI M. AL-KHOURI

ABSTRACT: Organizations in both public and private sectors are realizing the value of identity and access management technology to address mission-critical needs and to ensure appropriate access to resources across heterogeneous technology environments, and to meet rigorous compliance requirements. A well-designed identity management system is fundamental to enabling better information sharing, enhancing privacy protection, and connecting the diverse web of public and private sector agencies involved in the delivery of today's public service. This article provides an overview of identity and access management literature. It attempts to analyze the business drivers, trends, issues and challenges associated with the implementation of such systems. It then presents a strategic framework and an overall ecosystem for the implementation of identity and access management system in different contexts of applications. It also introduces possible strategies and solutions for the development of a federated national identity infrastructure. It finally sheds light on a recent

[33] Al-Khouri, A.M. (2011) "Optimizing Identity and Access Management (IAM) Frameworks", **International Journal of Engineering Research and Applications,** Vol. 1, No. 3, pp. 461-477.

government implementation in the United Arab Emirates that was launched to develop a modern identity management infrastructure to enable digital identities and support their application in e-government and e-commerce context.

Key words: *Identity and access management; federated identity; national identity card.*

1. INTRODUCTION

THE rapid globalization of world commerce, converted conventional businesses that were used to be based on handshakes, into new electronic forms of commerce enabling remote impersonal transactions. This transformation of the way commerce is handled has largely been due to the explosive growth in Information and Communication Technology (ICT). Today's businesses rely solidly on ICT systems for their day-to-day operations. Business challenges that necessitate reaching out to far flung customers are forcing organizations to open up their internal systems to outsiders such as suppliers, customers and partners [1]. This has literally broken down the virtual perimeter conceived as part of the organizations' security strategy [2]. Due to this, many outsiders have now become an integral part of organizations' ICT definitions [3].

On the other hand, governments are enormously investing in ICT to transform the way they deliver services to their citizens, residents and businesses. Convenience of transacting directly with the government and the attempts to reduce the red tape in government services has driven public sector to adapt to a more productive business processes. To many of us today, gone are the days when citizens had to visit a government office for a service. Our expectations of public services have risen to an extent where we expect now services to be delivered at our doorsteps. ICT is envisaged to transform government business and services to meet citizens' expectations for better services, and to create a more open government. These developments necessitate the ability to establish and confirm the identity of remote entities, provide identity assurance and ensure authorized access. Though the priorities and principal drivers of identity management differ from one sector to another, there exists a common foundation for identity and access management that is gradually converging based on trust establishment.

The intent of this article is to provide an overview of the literature surrounding the application of identity and access management. It also aims to establish a link between identity and access management technologies and the role of governments in establishing and managing the identity lifecycle of their citizen and resident population. Such governments' take up, is expected to momentously drive identity and access management developments to higher levels.

This article is structured as follows. First, a short overview of the literature on identity and access management is provided. Associated business drivers, trends, issues and challenges, and opportunities are identified. The value pyramid of identity and access management is explained in the context of an ecosystem. Next, the role of governments' national identity programs and underpinning technologies such as smart cards and PKI technologies in the optimization of identity and access management systems is outlined. Finally, we delineate on a UAE government program that was launched to set up a national identity infrastructure and enable digital identities to support e-government transformation and e-commerce initiatives.

2. IDENTITY MANAGEMENT: AN EMBRYONIC DISCIPLINE

There is an old say we used to hear about trust: "Only a man you trust can breach your trust". This is the irony of trust. Identity has become a new focal point in today's global economy. It forms the basis of social and commercial interactions. As illustrated in Table 1, trust is defined and interpreted differently in various study domains such as computer science, psychology and sociology. Trust involves providing reliable identity assertion of the relevant parties. Achieving such goal requires building a "Trust Framework" for each identity system that addresses both the operational requirements and the legal rules necessary to define a trustworthy identity system [4].

Table 1: interpretation of Trust in different study domains

Trust Domain	Description
trusted systems:	related to security engineering and encompasses areas such as risk management, surveillance, auditing and communications.
"web of trust" systems:	related to cryptography and focuses on technologies like public key infrastructure.
trust metric:	considered within the areas of psychology and sociology and proposes a measure of how a member of a group is trusted by other members.

Source: Choi et al., 2006.

Ever since computing technologies have been applied for business operations, identities were managed in one form or another. Over time, identity management evolved as a separate discipline in line with the growing importance that this technology has gained over the years. There have been endless attempts by researchers and practitioners to construct community-aware identity management systems and for establishing higher trust levels between users of different digital networks [5]. However, the critical issue lies in the fact that there are few implemented systems in practice that provide strong user authentication capabilities and new levels of trust and confidence to how identities are established and verified.

Thus, the industry and governments alike are beginning to realize that trust management is intricately integrated with identity management. This is to say that trusted identity information is a key foundation element to privacy protection and information sharing. Access control is then built on a set of authorizations which are given as directives through the security policy. With the growing needs of security, compliance and newer infrastructure models like cloud platforms, identity and access management has become the corner stone for today's ICT enabled business models [6].

Identity and access management system is considered as a framework for business processes that facilitates the management of electronic identities [8]. The framework includes the technology needed to support identity management. IAM technology is used to establish, record and manage user identities and their related access permissions in an automated approach. This ensures that access privileges are granted according to corporate policy and that all individuals and services are properly authenticated, authorized and audited. Let us look at some surveys related to the domain of trust and access management, which should clarify the seriousness of the topic being discussed here.

2.1 Recent Surveys

A 2009 Data Breach Investigations Report by the Verizon Business RISK shows that almost one third of data breaches were linked to trusted business partners, such as suppliers and contractors [8]. In addition, and according to findings of another recent study conducted by Deloitte and the National Association of State Chief Information Officers (NASCIO), surveyed organizations reported that the majority (55 percent) of internal information breaches were traced to either the malicious or inadvertent behavior of employees [9]. See also Fig. 1.

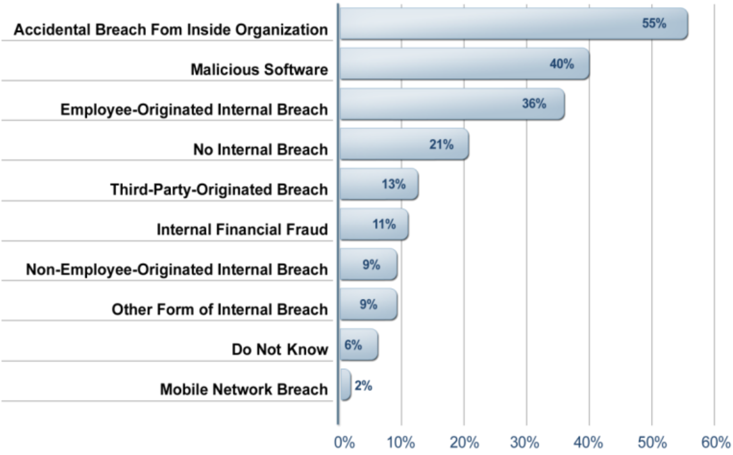


Fig.1: Source of breaches

According to a study conducted to better understand activities affecting information systems and data in critical infrastructure sectors, it was stated that the incidents studied were caused mainly by "Insiders" [10,11]. The study which was collaboratively developed by United States Secret Service's National Threat

Assessment Center (NTAC) and the CERT® Program (CERT) and the Carnegie Mellon University (CMU), revealed that:

- The majority (58%) of insiders were current employees in administrative and support positions that required limited technical skills.
- Financial gain was the motive (54%) for most insiders' illicit cyber activities.
- Most (85%) of the insiders had authorized access at the time of their malicious activity.
- Access control gaps facilitated most (69%) of the insider incidents.
- Half (50%) of the insiders exploited weaknesses in established business processes or controls such as inadequate or poorly enforced policies and procedures for separation of duties (22%).
- Insider actions affected federal, state, and local government agencies with the major impact to organizations being fraud resulting from damage to information or data (86%).

These are indeed very disturbing facts. Today, it does not take a technical wizard to commit frauds in technology oriented systems. There are always opportunities for various technical and non-technical employees to use legitimate and authorized access channels to engage in insider attacks. The insiders involved in the cases studied in the above survey did not share a common profile, and showed considerable variability in their range of technical knowledge. So we argue here that it is the breach of trust that is the root cause for such illicit activities.

In the following sub sections, we will look at how IAM technology have evolved, and outline key business drivers, trends, issues, challenges, and business opportunities of IAM across the globe that contributed to the maturity of this technology. This would give us an overview of the evolving capabilities of IAM solutions that help organizations to address today's challenges.

2.2 Identity and Access Management Evolution

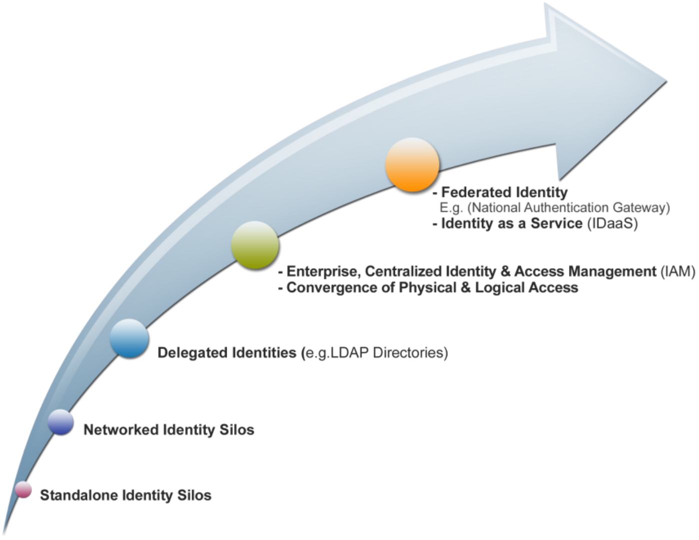

- Federated Identity
E.g. (National Authentication Gateway)
- Identity as a Service (IDaaS)
- Enterprise, Centralized Identity & Access Management (IAM)
- Convergence of Physical & Logical Access
Delegated Identities (e.g.LDAP Directories)
Networked Identity Silos
Standalone Identity Silos

Fig. 2. IAM evolution

Identity and access management technologies arose from the necessity to satisfy basic business needs of improving security and cost savings. At this early stage, IAM existed in standalone identity silos. As businesses began to turn to automation in an effort to cope with market speed and enhance business results, the need to secure transactions became more important, which paved the way for networked access models to appear. As the time went on, IAM technologies were further developed to simplify resource access related processes and as a tool to meet increasing compliance issues surrounding client privacy, data integrity, and security (e.g., LDAP concept, centralized access models).

Larger networks and interconnected systems in a geographically diverse environments resulted in IAM federated identity access models. This approach enables organizations to optimally pursue business automation goals and higher operational efficiencies and market penetration through aligning together their business models, IT policies, security and privacy goals and requirements. In other words, identity federation is referred to the set of business and technology agreements between multiple organizations to allow users to use the same identification data to access privileged information across many disparate network domains.

Obviously, identity federation offers economic savings, security and privacy as well as convenience, to both enterprises and their network users. However, and in order for a federated identity to be effective (i.e., developing an integrated service model in the supply chain), organizations must have a sense of mutual trust. This will be elaborated in more detail in the next section.

2.3 Business Drivers and Trends

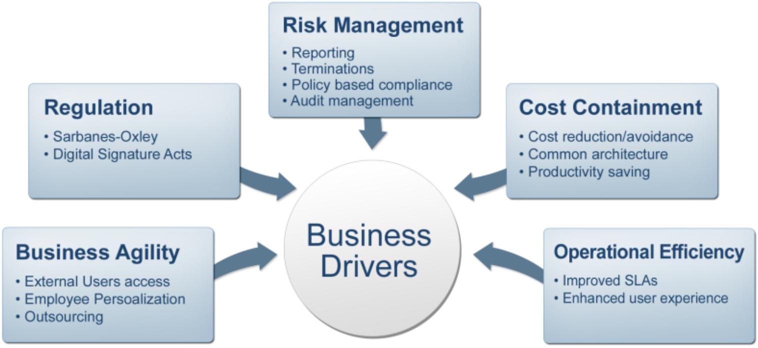


Fig. 3. IAM business drivers

According to a recent Forrester Research [12] identity and access management was identified as a top security issue for 2011 that needed to be considered as a critical component of corporate security strategies [see also 13-15]. Forrester predicted that IT administration efficiency and business agility will become the main drivers for using identity and access management. It also indicated that there will be tighter integration between data security and the identity lifecycle. Along with the requirement to secure mobile devices with second factor authentication, this is expected to drive both on-premises and cloud-based IAM implementations.

Apart from security needs, there are various other factors that influence the adoption of identity and access management. In a survey conducted by KPMG [16] in 2008, it found that the primary reasons to implement IAM solutions were related to business agility, cost containment, operational efficiency, IT risk management and regulatory compliance. Fig. 3 below captures the essence of the business drivers for IAM.

Table 2: IAM Trends

Convergence of Physical & Logical Access Management	• There is a greater level of convergence between physical and Logical access management, through centralization of Identities, policies and credentials management
Authentication & Identity Federation	• Demand for strong authentication is growing as enterprises and government agencies seek to deter cybercrime
Authorization	• Fine grained authorization is increasingly in demand • SAML is a broadly used standard protocol and successful business models have been implemented
Identity Assurance	• National ID initiatives enhances Identity Assurance
Roles & Attributes	• There is a growing acceptance of role based access control in production systems
Regulation	• Government regulations (e.g. SOX, HIPAA/HITECH), will continue to expand, both on national and international levels
Personalization & Context	• Personalization can enhance the value of online user experience. Both identity and context are essential for personalization
Identity Analytics	• Advanced data analytics will bring value to many identity-based activities such as Authentication, Context/Purpose and Auditing • Analytics brings tremendous value in monitoring the key usage patterns and statistics
Internet Identity	• User-centric or user-managed Identity technologies such as Infocard/Cardspace and OpenID, are trying to address the security and ease-of-use requirements
Identity in the Cloud	Identity as a Service (IDaaS) is a critical foundation for Cloud Computing

The ability to on-board different external and internal resources on one integration seamless environment results in high business agility. The need for identity management and access control and authorization cannot be understated in this case. Government and audit regulations stipulate proper controls for audit trail.

Without a proper identity management, no audit trail can be established. Security and risk management dictate the use of identity management. Loss of data results in loss of business. The cost containment due to adoption of IAM technology drives the IAM strategy and architecture to be adopted. Last but not least, is the improvement in operational efficiencies sought to be provided due to identity management. These define the key drivers for IAM.

The KPMG report [16] referred to above indicated that improving compliance was among the main drivers of IAM projects to comply with the increasingly stringent regulatory requirements, posed by laws and legislation. The survey respondents indicated that some of the more prominent benefits that their organizations expected were related to quicker handling of accounts, of authorization of employee, employee lifecycle management, as well as of the automation of associated repetitive manual activities. Such process improvement was envisaged to enhance consumer experience and federate with partners in an efficient, secure business processes that lead to operational efficiency and cost containment.

When IAM is used as a preventive mechanism to enforce polices by automated controls, it is viewed to ensure an organization wide secure access control infrastructure. Table 2 depicts further trends identified by identity and access management vendors as shaping the market in the next five to seven years.

2.4 Issues and Challenges

The implementation of identity and access management possess its own challenges and risks, as it potentially requires capital investment and changes in personnel and existing business operations [17,18]. The introduction of identity and access management processes into an organization can expose it to new risks while mitigating existing ones [19-21]. For instance, as organizations open up their systems to allow more external entities to access sensitive internal data, the risk of breaches from external sources (partner-facing risk) would continue to be a threatening factor.

In practice, identity and access management as a technology must scale to match the need of the heterogeneous ICT environments found in most organizations [22]. As more systems come online and new partnerships are formed, and with systems in numerous locations, the task becomes more and more resource intensive without it [23]. What is more, in recent years regulatory requirements have added complexity and increased external scrutiny of access management processes. Organizations need to develop an understanding of such risks as they implement new or modified identity and access management processes. Table 3 provides an overview of these risks.

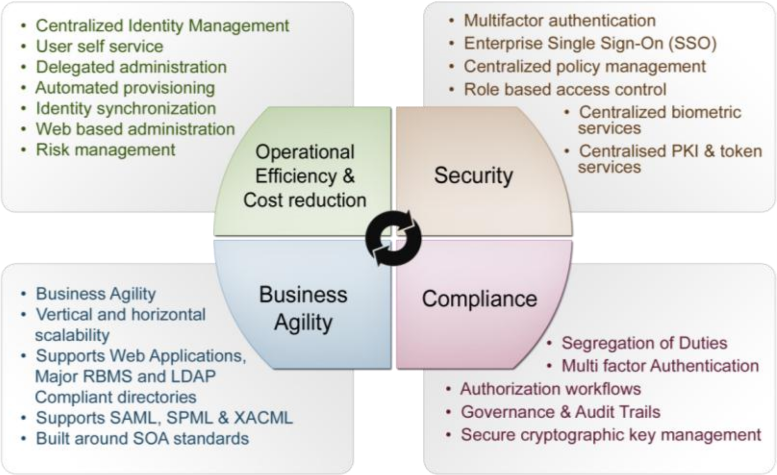
Table 3: Identity and access management risks

Administration Overhead	**Security Risks**
• No centralized user administration process. • Multiple teams are involved in the user administration activities. • Increasing overhead in administration of identities • Administrators spend a lot of time performing routine admin tasks that can be automated • Different administrators often assign different IDs to the same person. This makes it difficult to track activity back to a single source and confuses the customer.	• Potential security risks • Accounts are created with unauthorized system access rights. • Security risks occur when frustrated or overburdened admin staffs may take shortcuts, terminations may not be done as soon as required or permissions granted may be in excess of what is really needed.
Complexity	**Inefficiency**
• The users of the system are located worldwide and can be customers, employees, temporary workers, contractors and external suppliers. • Multiple authentication requirements for applications • Account creation/deletion in repositories is performed by multiple groups • Many systems and applications have different business owners, platforms, administrative tools, and system administrators, leading to slow performance, delayed or unreliable terminations and higher administration costs. • Account creation process requires great coordination, involves many steps, and	• A high number of calls are made to the support center for user provisioning activities including password resets. • Terminating employee accounts is a manual process • The process for business unit managers and application owners to sign off on the privileges of the users is cumbersome and time consuming. • Proliferation of directories and identities: diverse infrastructure has evolved over time • Redundant identity information • Information inaccuracies

involves multiple clients which must remain segregated from each other • Support staff requires advanced training to administer accounts on so many varying systems. • Employees and customers require timely access to applications and systems to perform their jobs.	• Users wait longer than necessary to obtain IDs • Managers spend time chasing a sequence of events to ensure proper approvals. • Authorizations needed to process a request often slow the process of account creation or update and leads to errors and mistakes.
Poor Compliance	**Lack of Long Term Strategy**
• Untimely response to regulations	• Managing for the moment, but not positioned for the future

2.5 Federated identity management

A government organization previously managing access only for its employees now needs to manage access for millions of citizens and a wide range of other agencies accessing information and seeking online services. Federated identity management provides capabilities such as government-to-citizen self-service and federated single sign-on (SSO) support. It allows organizations to centralize fine-grained security policy management to enforce access control across applications, databases, portals and business services. The need for federated identity is thus driven by four major drivers; security, compliance, business agility and operational efficiencies. See also Fig. 4.



Centralized Identity Management
User self service
Delegated administration
Automated provisioning
Identity synchronization
Web based administration
Risk management
Operational Efficiency & Cost reduction
Multifactor authentication
Enterprise Single Sign-On (SSO)
Centralized policy management
Role based access control
Centralized biometric services
Centralised PKI & token services
Security
Business Agility
Business Agility
Vertical and horizontal scalability
Supports Web Applications, Major RBMS and LDAP Compliant directories
Supports SAML, SPML & XACML
Built around SOA standards
Compliance
Segregation of Duties
Multi factor Authentication
Authorization workflows
Governance & Audit Trails
Secure cryptographic key management

Fig. 4: Drivers for federated identity management

Federated identity is the big move forward in providing an integrated environment for the citizens, service providers and the different government agencies. While a service is delivered to a citizen online, there would be different stakeholders that would be involved in the service delivery cycle. Federated identity provides a very effective solution that obviates the need of repeated authentications and verifications each time a new stakeholder joins the service delivery cycle.

A single credible source of verification can be shared by the different entities which rely on the trust created by the source. This verified identity is then federated to different entities. This leads to uniform security policy enforcement, greater compliance to regulations related to Identification, provides better scalability and responsiveness from different stakeholders ultimately ensuring operational efficiencies and reducing operational costs.

Having said this, the next section looks at the IAM ecosystem that attempts to explain how an integrated architecture can be developed to unify siloed security technologies into a comprehensive, standards-based identity management framework.

3. IDENTITY MANAGEMENT ECOSYSTEM

Identity and access management like many other enterprise solutions cannot add value in a stand-alone mode. The overall value of identity and access management entirely depends on the level and easiness with which it integrates with other enterprise systems. Fig.5 depicts a typical identity and access management ecosystem. On one side, we have different kinds of users like employees, partners, suppliers and customers. On the other side, we have diverse kind of enterprise resources like directories, databases, servers, network resources etc.

There exists a complex relation between the users and enterprise resources in terms of identity lifecycle management and access controls. This in turn has to comply with various security standards and guidelines, enabling, at the same time, organizations to achieve their business objectives. It is desirable to have a governance and policy control framework at the heart of the ecosystem that orchestrates the way the whole ecosystem work.

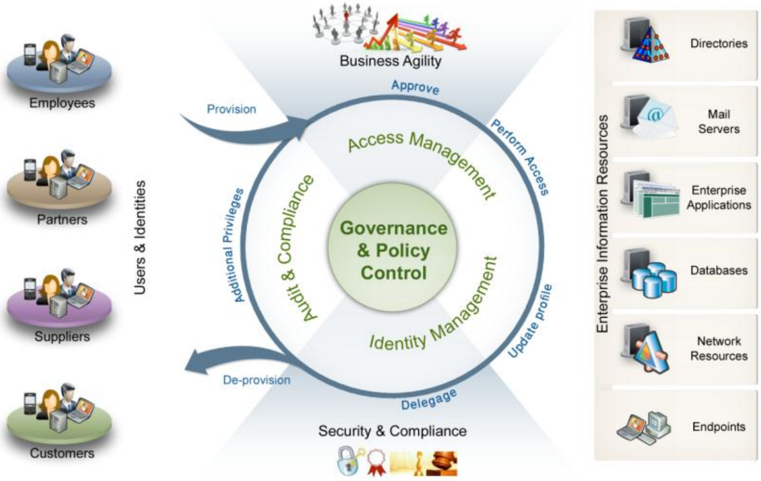


Fig.5. Identity and access management ecosystem

In a step to develop more cohesive identity and access management working models, there is a trend in the industry that is pushing for the convergence of physical and logical access systems. This is likely to enhance the ecosystem as we discuss next.

3.1 Convergence of Physical and Logical Access

Organizations have long operated, and still many do operate physical and logical access systems as two independent structures, and are typically run by completely separate departments. This is very much evident in current organization structures in the Middle East for example. This is to say that logical access to corporate ICT resources such as e-mail, database permissions, web access, intranet/internet connectivity and database applications are granted and remain the responsibility of ICT departments. The service or facilities departments are responsible to control physical access systems such building doors access, life support systems, etc.

Nonetheless, boundaries between physical access and logical access systems are melting in the current digital world due to several economical and efficiency factors. In fact, identity and access management technology is bringing in a transformation in the way the industry categorizes security and in the development of the primary capabilities of authentication, authorization and administration [24]. This transformation is expected to revolutionize e-business, allowing organizations to use digital identities to contribute real value to their business (ibid).

From one standpoint, combining logical and physical security systems gives a more comprehensive view of potential intrusions across the physical and IT environments. From another perspective, it is likely to result in significant improvement of the user experience both from administration and end-user perspectives, e.g., cost savings and improving efficiency and enforcing policies throughout the organization. This should provide multilayered security across company networks, systems, facilities, data, intellectual property and information assets.

Fig. 6 shows the convergence of some physical and logical access systems. Physical facilities like office complexes, warehouses, production facilities need to be protected from unauthorized access. Once inside the premises, a person would need access to the network resources like ERP applications, files etc that are stored on a central database. Conventionally these two systems were separate, even though the access and authorization for access were similar, if not the same.

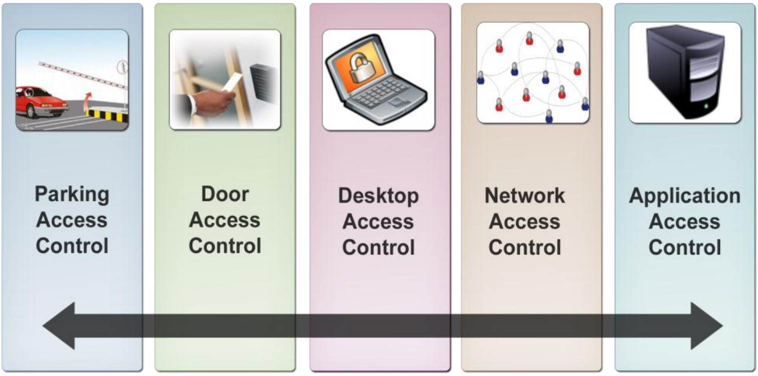


Fig. 6. Convergence of physical and logical access

It is important to refer here that traditional identity and access management architectures focus more on the user provisioning and access management. Today's identities comprise not only of human entities, but also numerous kinds of endpoints such as desktops, laptops, PDAs, smart phone etc. Hence a comprehensive credential management system capable of managing the lifecycle of credentials of these diverse types of entities is a fundamental requirement for today's world. The next subsection looks at how modern identification systems are enabling more robust identity establishment and lifecycle management.

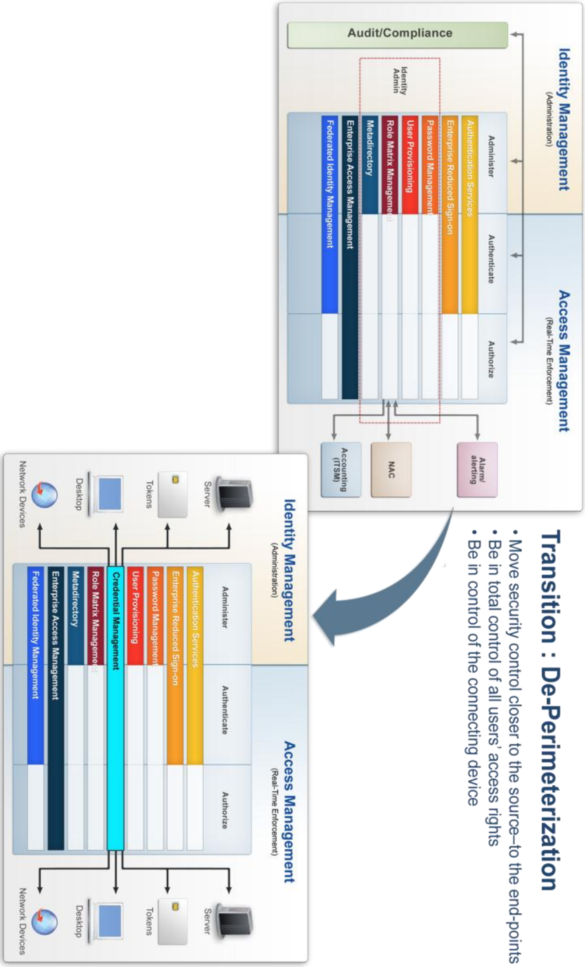
3.2 Modern digital identification systems: enablers of transformation

Critical Infrastructures have long relied on biometric verification and authentication of individuals to provide stricter access to secure locations. Only authorized personnel verified by the biometric data could gain access to secure areas. The file access and network access depends largely on provisioning of users on IT systems like

LDAP. Single factor authentication limited the verification of the authorized users by means of passwords. Stronger authentication systems based on biometrics advancements made the biometric data to be available on smart cards enabling what-so-called digital IDs. The same biometric systems that provided physical access could now be utilized for network access. This has made the identity management administration move from facilities management to IT administration.

As authentication remains the mechanism through which access is granted to any corporate resource either physical or logical, identity management systems are forming a primary building block and enabler for such convergence. In other words, modern digital identification systems are facilitating this convergence and unification of identification systems and authorization for access, as they provide identities in digital forms. Smart card technologies are considered to be a key player in this regard. Smart cards use a unique serial number and a Personal Identification Number (PIN) to identify a user, prove identity and grant network access. This 'unified access' token can provide several security-level options ranging from simple access control to complex data encryption. See also Fig. 7.

At the core of all access control is policies, roles and provisioning of users to their roles. Identity establishment is based on the digital credentials backed by strong authentication mechanisms (multi factor authentication) and secure verification of the credentials thus presented. Trust is established by the secure identification that provides assurance to the identity seeker of the genuineness of the identity. The application of identity and access management could vary from one domain to another. Hence it is important to look at the IAM in the context of different domains and their applications, as we outline next.



Transition : De-Perimeterization

- Move security control closer to the source—to the end-points
- Be in total control of all users' access rights
- Be in control of the connecting device

Fig. 7. De-perimeterization of identity and access management (Source: Jerichofurm)

3.3. Enterprise Context

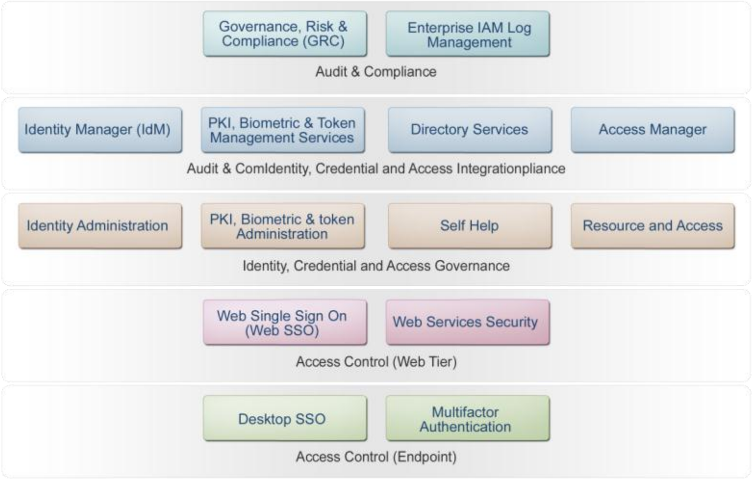

Governance, Risk & Compliance (GRC)
Enterprise IAM Log Management
Audit & Compliance
Identity Manager (IdM)
PKI, Biometric & Token Management Services
Directory Services
Access Manager
Audit & ComIdentity, Credential and Access Integrationpliance
Identity Administration
PKI, Biometric & token Administration
Self Help
Resource and Access
Identity, Credential and Access Governance
Web Single Sign On (Web SSO)
Web Services Security
Access Control (Web Tier)
Desktop SSO
Multifactor Authentication
Access Control (Endpoint)

Fig. 8: Layers of identity and access management in an enterprise context

There are typically 5 layers of identity and access management in an enterprise context as depicted in Fig. 8. Using a top-down approach, the first layer integrates business intelligence, process management, and automated controls enforcement to enable sustainable risk and compliance management. It encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.

The second layer deals with identity credentials and access integration. This layer is a result of the identity management polices and the laid down requirements for establishing and verifying an identity. This is a crucial component of the enterprise IAM. Identity can be established by providing an ID number to an individual. To strengthen the identity, digital credentials can be provided as verifiable metadata of the ID. Typically the credentials are issued in the form of a digital certificate from a PKI system and biometric minutiae. A directory service (e.g., LDAP) provides the ability to list and provision an individual's identity for access management. A policy repository with role definition and provisioning of users provides the last component of this layer; i.e., the access management system.

The third layer deals with access governance. This governs the mechanism of defining policies, administration of the identity management system, audit trails, reporting, etc. The remaining two layers are access management component and the application of identity administration and governance components. The Web Tier access management layers allows secure web single sign-on solution that connects remote users to corporate web applications and systems through a secure portal. The Web based applications can be tied together with the Web SSO enabling centralization of access control and policy enforcement.

The last layer of access control employs multiple factor authentication mechanism to grant access to enterprise systems, platforms and applications. This layer is used for according authorized access to protected resources and prompts strong authentication capabilities. Both access control layers are truly integrated. The same single password (or token) works in both layers as user credentials are managed from a centralized SSO.

Apparently, identity management architecture in enterprises is driven by security needs. There is a colossal difference when we talk about identity management in a government context, as the next subsection outlines.

3.4. Government Context

A governmental initiative for identity management is typically driven by various factors as in the enterprise context, but the drivers are slightly different. Major drivers for identity management in the government sector are:

- compliance with federal laws, regulations, standards, and governance relevant to identity management;
- facilitate e-government by streamlining access to services;
- improve security posture across the federal enterprise;
- enable trust and interoperability;
- reduce costs and increase efficiency associated with identities.

Identity management is largely citizen centric in the government context. Citizens transact with their governments in many ways - to seek information, rightful benefits, business services, legal recourse etc. The interactions of the citizens with their governments are varied and very dynamic. In a federal context,

IAM provides tremendous value in the interactions between the government, citizens and businesses. A robust identity management system seeks to make the service delivery more convenient. Consequently, for the government, the core element in providing right content and personalized services is to ensure its citizens are provided with credible and verifiable credentials.

Reliable identification and authentication of entities in an online or over the counter environment is a critical requisite [25]. Fig. 9 below depicts the typical value pyramid for the IAM in government context. Trusted entities can reliably transact in seeking and availing of services delivered remotely or over the counter. Identity needs to be established at every node – i.e., in G2G, G2B, G2C, B2B, C2C and B2C transactions.

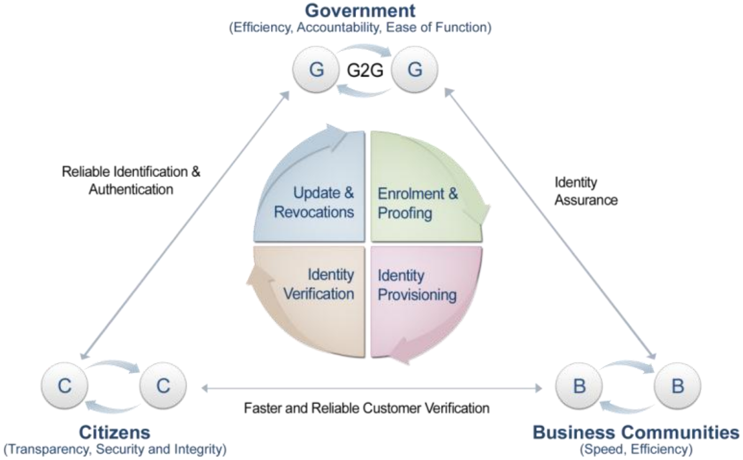


Fig. 9. IAM value pyramid in government context

The identity and access management platform here is very akin in functionality to the one in the enterprise context. The difference is in the application. Herein, the government facilitates the identity issue and provides assurance to the identity by means of strong authentication mechanisms. So at the core of the IAM value pyramid is the "identity issue system". This system allows the government to enroll its citizen and resident population and provide them with identity baselines "proof of identity" that will be used as credible credentials for identity provisioning and strong authentication.

Management of identities is carried out by means of dynamically updating the identity repository for new additions and revocations. As the provider of the identity, the government provides a third party service for reliable identity verification to the seekers of this service. To understand how this pyramid works in practice, let us look at the role of national identity cards and PKI technology in the optimisation of identity and access management systems.

4. ROLE OF NATIONAL ID CARD & PKI IN IAM OPTIMIZATION

Governments and enterprises have always been engaged in providing an Identity to their stakeholders for benefit deliveries and services. Conventionally, identity documents were all paper based (e.g. passports, birth certificate, etc.) which have very limited use in online transactions and incur cumbersome processes to verify the authenticity of these documents.

The role of optimization thus gets defined. Identity management optimization includes a re-look at the identity infrastructure, processes involved in determining the authenticity of an identity, parameters to establish the identity and processes for trust establishment and, providing assurance to the service seekers and service providers of the identity established in the process. Identity management optimization seeks to reduce the time involved in completing the processes of identity and trust establishment between two entities.

In a national context, many governments around the world are issuing national identity cards as a vehicle that carries digital identity credentials. Many of the modern national identity cards are based on smart card technology. It enables faster identification and authentication of citizens and residents. Thus we view a national identity card as an enabler and a means to optimize the identity and access processes across various organizations by eliminating redundant identity infrastructure and providing higher levels of assurance.

Smart cards are an exceptional means to store identification metadata of the card owner securely. The security accorded by the smart cards, backed by a strong and solid multi factor authentication methods allow secure communications with the card. The smart cards provide tamper proof mechanism to store identity data. Table 4 provides an overview of the features provided by smart cards.

Table 4: Smart card capabilities

<table>
<tr><th>Security</th><th>Protection</th></tr>
<tr><td>• Match on card biometric
• Support for RSA (PKI), DES and Hash algorithms
• PIN protection to access card information</td><td>• Tamper proof protection against forgery
• Self locking on brute force attacks
• Applications can be protected through SAM</td></tr>
<tr><th colspan="2">On Card Processing</th></tr>
<tr><td colspan="2">• On card cryptographic processing chip
• Protection of PKI private keys on Smartcard
• Capability to generate PKI key pairs on card
• On-card digital signing and encryption</td></tr>
</table>

These features provide an unshakeable trust in the data held in the card [26]. Therefore, any data read from such secure cards provides the means for instant verification of identity. The smart card can store biometric information that can be checked with a biometric device to match the data in the card. Further, any communication with the card itself is encrypted and is carried out only using authorized protocols. Such authorized protocols provide a control on who gets to read the data and use for verification.

In addition to the personal information that can be stored, the smart card can store securely the set of private and public keys that constitute an electronic signature of an individual. The PKI system provides the equivalent of a biometric fingerprint to individuals in the form a digital certificate which is a unique signature that is provided to individuals. This certificate can then be used as credentials from the secure store in the card to establish further trust in the transactions carried out electronically by the individuals. The following diagram provides an overview of key PKI benefits.

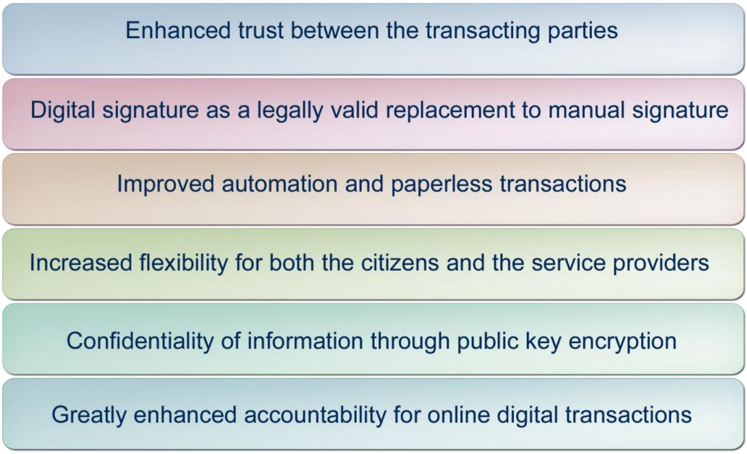

Enhanced trust between the transacting parties
Digital signature as a legally valid replacement to manual signature
Improved automation and paperless transactions
Increased flexibility for both the citizens and the service providers
Confidentiality of information through public key encryption
Greatly enhanced accountability for online digital transactions

Fig. 10. Key benefits of PKI

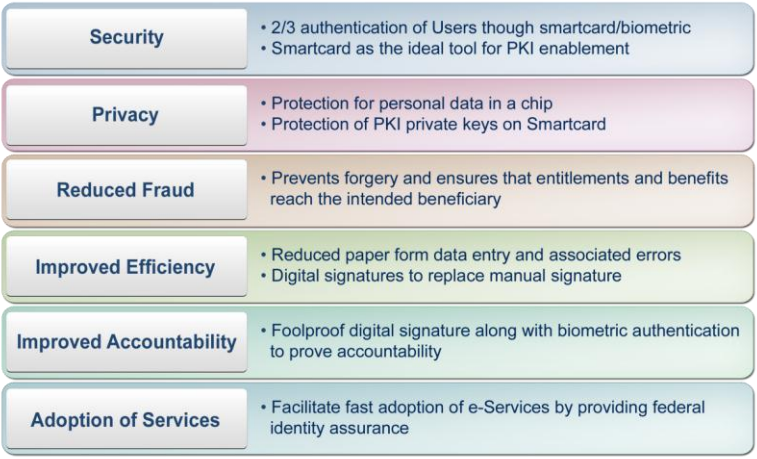
Establishing the identity of a person is not sufficient to conduct a transaction. Enhanced mutual trust is needed to be established that assures the stakeholders of the transaction that:

1. the transaction indeed did take place;
2. the stakeholders in the transaction did indeed take part in the transaction and have accepted the transaction as completed;
3. there is irrefutable evidence on the time at which the transaction has taken place;
4. confidentiality of the transaction is maintained; and
5. in case of a dispute, the transaction can be legally upheld.

PKI technology enhances the trust between the parties involved in the transaction. PKI allows digital signing, allowing transactions to be carried out electronically without geographic barriers, providing tremendous ease in the transactions across the globe. Such a transaction obviates the need of paper. And, if the PKI is provided as a service by the identity provider, it provides a third party assurances leading to enhanced accountability in the transaction.

With smart cards, multi factor authentication is possible i.e., biometric, PIN and password can be used since the card can provide such capabilities. Typically two of these three factors can be used by service providers for identity verification. The security on the card ensures strong privacy since unauthorized users cannot read any data from the card. This leads to less fraud since identity is securely established and business can then authorize the authenticated users to complete the transaction. Being digital, all the transactions, services, verification, etc are audit trailed for a back track check providing very high accountability.

No one can deny the usage of the card, if the card has been used in a transaction. Such secure features backed by the ease of implementation allow quick adoption of the card and PKI for rendering services electronically. Such identity systems provide a win-win platform for businesses to enable lower turn-around times in their go-to-market strategies. The following diagram summarizes the benefits accorded by these complementary technologies.



Security	• 2/3 authentication of Users though smartcard/biometric • Smartcard as the ideal tool for PKI enablement
Privacy	• Protection for personal data in a chip • Protection of PKI private keys on Smartcard
Reduced Fraud	• Prevents forgery and ensures that entitlements and benefits reach the intended beneficiary
Improved Efficiency	• Reduced paper form data entry and associated errors • Digital signatures to replace manual signature
Improved Accountability	• Foolproof digital signature along with biometric authentication to prove accountability
Adoption of Services	• Facilitate fast adoption of e-Services by providing federal identity assurance

Fig. 11. Smart card and PKI benefits

The next section looks at one of the pioneering government implementation programs in the Middle East to setup and provide reliable identification and verification mechanisms to enable digital identities with the aim to support e-government and e-commerce initiatives.

5. IDENTITY INITIATIVE: THE CASE OF THE UNITED ARAB EMIRATES

Globally there are a few countries that have successfully adopted digital identity systems. Belgium, France, Finland, Malaysia, South Korea, Singapore remain some of the successful examples. In the Gulf region, there are appealing initiatives in the digital identity front. United Arab Emirates, Oman, Bahrain and the Kingdom of Saudi Arabia have launched in the last five years modern identity management programs. Due to the current role of the author in the UAE program, and lack of information about other governments' practices, the discussion in this section will be limited to only the UAE project.

United Arab Emirates has taken the lead in the Middle East to implement a modern national identity management infrastructure with smart card, PKI and biometric technologies and in promoting digital identities to its citizen and resident population – estimated around 9 million people in 2011. The government established an independent federal agency named Emirates Identity Authority in 2004, to become the sole identity provider in the country. The organization introduced lately a "4E Strategy" to promote the application of digital identities. This strategy is envisaged to support and play a key role in the transformation of service delivery infrastructure and in enabling e-government and e-commerce initiatives in the country.

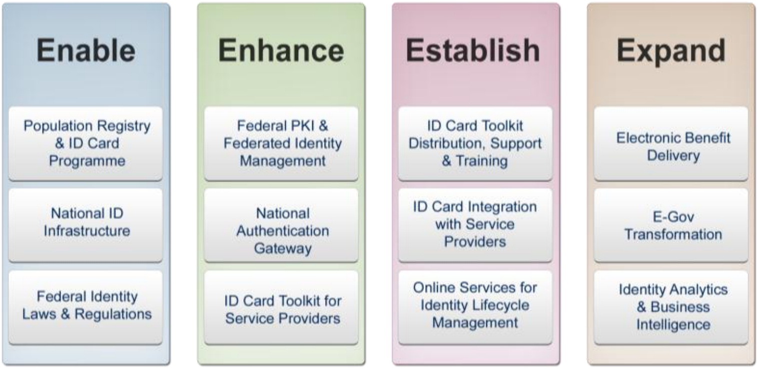

Enable
Population Registry & ID Card Programme
National ID Infrastructure
Federal Identity Laws & Regulations
Enhance
Federal PKI & Federated Identity Management
National Authentication Gateway
ID Card Toolkit for Service Providers
Establish
ID Card Toolkit Distribution, Support & Training
ID Card Integration with Service Providers
Online Services for Identity Lifecycle Management
Expand
Electronic Benefit Delivery
E-Gov Transformation
Identity Analytics & Business Intelligence

Fig. 12. UAE "4E Strategy" implementation framework

As depicted in Fig. 12, the first phase of the strategy relates to the setup of a national identity infrastructure to (enable) and empower citizen and the resident population digitally by enrolling them in a state of art and technologically sophisticated population register. The registration process includes the capturing of biographical data, personal portrait and ten rolled fingerprints.

A robust identity verification process takes place to perform biographical and biometrics checks against the population register and other forensic systems, to ensure that the person has not been enrolled previously and/or is needed by the legal authorities for criminal charges.

After passing through this stage, each individual is then assigned a unique identification number, which is linked to his or her biometrics. A smart card is issued to each individual that contains multiple credentials including unique RFID, MRZ barcode, photo ID, two best fingerprints for authentication purposes. The ten prints taken at the enrolment stage is stored in the population register database.

The UAE smart card, which is considered the highest in specification worldwide in government application to-date, is a combi-microprocessor-card, with both contact and contactless capabilities. To enable digital identities, the card also contains crypto keys and digital certificates.

The UAE government invested heavily in PKI technology to support e-government and e-commerce initiatives. PKI is seen as an important trust anchor, as it will determine compliance to defined criteria of trustworthiness of online identities. The government is working on crafting a legal framework and policy structure to provide the legal grounds and promote the adoption of digital identities in all walks of life in the country.

The government has shown particular effort to further enhance the digital identity infrastructure through the development and setting up of a federated identity management system and a national authentication gateway. The government aims to integrate multiple authentication capabilities provided by the new smart ID card and access channels to diverse resource interfaces in e-government and e-commerce environments. In an attempt to demystify the application of smart cards, a tool kit has been developed to allow service providers to seamlessly integrate the digital identification solution with their service delivery chain systems [27].

Managing the lifecycle of a digital identity presents significant business challenge i.e., the processes and technology used to create and delete accounts, manage account and entitlement changes and track policy compliance, etc. From this perspective, the government is working on establishing and providing managed identity services to both government and private sector organizations. This will provide a service level-based identity lifecycle management solution that is designed to offer authorization services only to individuals with valid ID cards. Indeed, a government based certification authority that issues and manages the lifecycle of digital identities is likely to acquire higher levels of trust.

The government is currently working to develop an integration platform to integrate the population register database with multiple government organizations involved in the identity lifecycle management related processes i.e., ministries of interior, health, justice, labour, and education who are responsible for civil incidents of the individuals related to (residency details, birth, marriage, divorce, death, education and health register). This will support organizations to better define and automate the processes and policies related to the authorization of digital identities and associated entitlements.

The integration platform and the national authentication gateway being designed and implemented are expected to completely transform the nature of business and government transactions in the country. The government expansion plans focus to provide the foundation for secure government communications and transactions and identity business intelligence for e-government transformation. This infrastructure provides a key building block to defend against security threats and identity fraud and at the same time enhancing resource utilization, improve productivity, and maximize ROI.

Expansion of the online identity services and continual improvement to the identity infrastructure is envisaged to greatly support national and individual security, as well as building the country's new digital economy [28]. So to clarify how the national identity framework adopted in the UAE government is designed and implemented, we attempt to outline in the following subsections its primary components and how they work.

5.1. UAE National Identity Framework

The national identity and access management in government context as we explained earlier differ vastly in the objectives and the expected outcomes of identity management from enterprise perspectives. Identity management in enterprises is driven by their security needs. And in this context, enterprise investment in identity management is dictated by the criticality of their internal data and the exposure they need to service their clients. At a national (government) level, identity management takes a different connotation altogether. The UAE government is assuming the role of an identity service provider to provide identity credentials to entities.

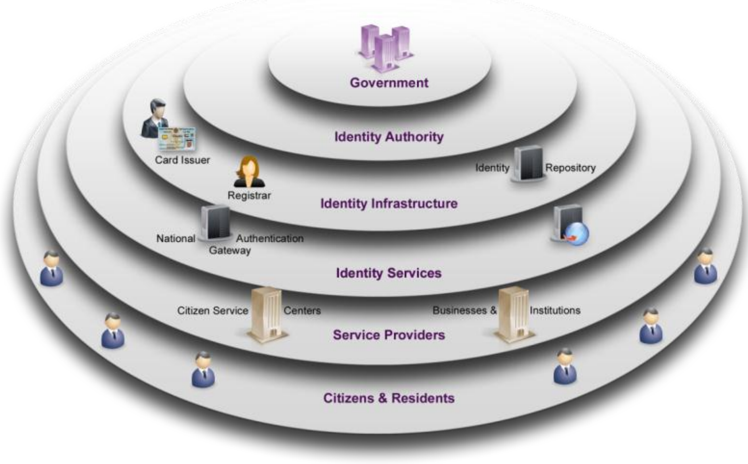


Figure 13: Government identity and management layers

As depicted in Figure 13, the adopted national identity framework in the UAE consists of many layers to enhance its reach and to improve the identity assurance levels. It assumes the role of providing the necessary credentials to provide baselines for provisioning and authenticating identities. The credentials are packaged in a secure system and delivered to the citizen. At this stage, smart cards act as the vehicle for such credentials to be delivered to the citizens.

An identity infrastructure is currently being setup in the UAE to contain various identity repositories along with the verification mechanisms to enable identity establishment and verification on demand. This then should form a credible identity service provided by the government that can be used by the different service seekers and service providers alike. Let us take few examples.

Banks and financial institutions are classic examples of service providers. Banks invest heavily in securing their financial systems. Conventionally, customers need to carry out their financial transaction with their banks by physically visiting one of the bank branches, where a teller agent verifies the customer in a "face-to-face" approach. With the increase in online banking facilities and in attempt to provide convenience, banks currently resort various identity establishment mechanisms ranging from interactive tokens with one time passwords (OTP), virtual keyboards, PIN verification and biometric verification.

Now, with the government stepping in, to securely verify the credentials and to stand to guarantee online identities, electronic banking and e-business models are expected to flourish and support the country's economy.

Let us consider another scenario where a government agency needs to deliver a service to a citizen. As part of the service delivery, the government employee needs to verify the credentials of the citizen. During the process of service delivery, the government employee needs to access different applications, databases – sometimes cutting across different departments and different government agencies. Current conventional processes depend on time consuming manual tasks that necessitate communication going back and forth to access data, verify identity, seek and get approvals and so on.

The new government federated identity architecture provides online credentials to both employees and citizens. This allows employees' identities to be established and trusted to accord access across different systems in the government. The same identity management system would ensure verification of the citizen's identity and allow the right services to be delivered to the right entities in the right time. This is expected to supporting the government's strategy to revolutionizing public services and e-government transformation. Let us see how the national identity authentication is architected in the next subsection.

5.2. National Authentication Gateway

Fig. 14 provides an overview of the national authentication architecture in the UAE and its key components. At the heart of the architecture is the identity gateway.

As the national identity provider, the UAE government relies primarily on the digital identity it issues in the form of a smart card as a vehicle for authenticating physical or virtual users. All requests for verification of an identity would have to be ported through an electronic system that acts much like a gatekeeper for the requests. Valid requests are entertained and sent to the identity verification systems managed by the identity provider. These are web based systems that provide the front end access to submit a request for identification and identity verification using defined industry standard protocols.

The requests are redirected to the gateway which in turn communicates with the identity management system. PKI systems provide the ability for transactions in real time using online certificate status protocol (OCSP).

In transaction terms, a citizen is served by a service provider remotely. The citizen tries to access the services through a secure web site. The service provider needs to identify the citizen. The citizen submits his identity card with his credentials. The service provider's application on the web reads the cards, collects the credentials from the card and refers the data with a verification request to the identity service provider.

The identity provider validates the request coming from the service provider as a valid request and allows the request to be processed. The identity provider verifies two main components of the ID data submitted by the service provider:

1. the Card itself to check the genuineness of the card; and
2. the Certificate data in the card.

Optionally, the service provider could also request for the verification of the biometrics. Secure communication is established between the card and the service provider's application. This is provided by an Active X control component running on the browser or by the authentication gateway. The architecture is designed to handle millions of identity validation requests on daily basis and is expected to scale based on requirements. Having said this, the following section summarizes and concludes the article.

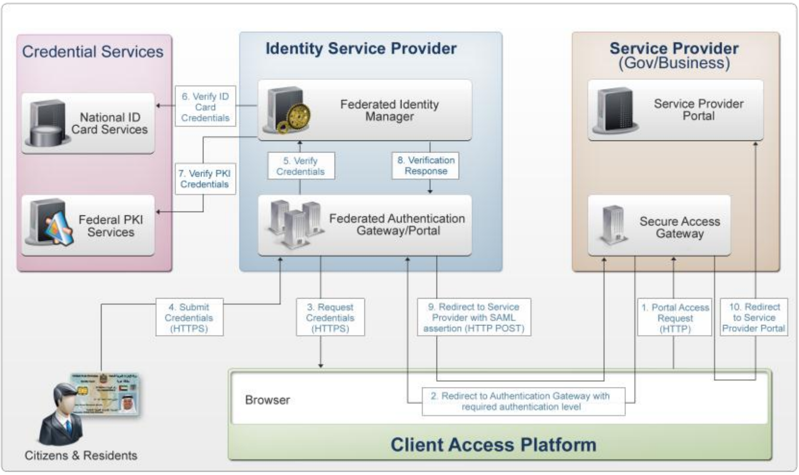

Credential Services
National ID Card Services
Federal PKI Services
Identity Service Provider
Federated Identity Manager
Federated Authentication Gateway/Portal
Service Provider (Gov/Business)
Service Provider Portal
Secure Access Gateway
6. Verify ID Card Credentials
7. Verify PKI Credentials
5. Verify Credentials
8. Verification Response
4. Submit Credentials (HTTPS)
3. Request Credentials (HTTPS)
9. Redirect to Service Provider with SAML assertion (HTTP POST)
1. Portal Access Request (HTTP)
10. Redirect to Service Provider Portal
2. Redirect to Authentication Gateway with required authentication level
Browser
Client Access Platform
Citizens & Residents

Fig. 14. National authentication gateway architecture

CONCLUSION

We presented in this article how identity and access management technology can provide a framework for (1) simplifying the management of access to services, (2) implementing policy, (3) increasing transparency, and (4) enabling scalability in operations to integrate identity management infrastructure with services provided by both central and distributed ICT systems.

We believe that the scope of identity management is becoming much larger in today's organizational context, and its application more critical. They indeed provide new levels of trust and confidence to identification systems. The role of the government is seen to play a major role in setting up a trusted identity management system and addressing the entire identity lifecycle of establishment, management and usage. The case of the UAE government is worth to be further examined and evaluated to measure its success, and most probably other cases from other countries.

It was not in the scope of this article to discuss the case of the UAE government in detail. The author just presented it for the purpose of referring to one of the very ambitious government initiatives in the field. The existing literature lacks such references from government implementations as it merely focuses on private sector and commercial cases.

In summary, the following key points discussed in this article, are likely to have a high impact on governments and public services in the near future:

- With the growing needs of Identification and rapid growth in information technology, the manner in which physical access and logical access requirements are met show a high degree of convergence. A digital identity issued to a person serves to provide access control to physical areas controlled for secure access as well as access to secure logical information.

- As the needs of remote (online) transactions grow, the identity and trust management between stakeholders becomes a key issue. Trust is accorded in identities by the assurance of the Identity provider. This makes the government, as indicated above, a key player in identity management by becoming the de-facto Identity provider to the citizens of the nation. System deployed by governments to provide identity assurance services are likely to evolve in the coming few years to address identity assurance requirements i.e., complete identity services from identity issuance, credentials management, verification services and identity assurance;

- National identity frameworks are characterized by a national authentication gateway will provide standards based, reliable identification and verification requirements of e-government service providers and businesses;

- Enterprise IAM implementations are growing towards maturity and we will see federated identity management integrating government, businesses and citizens at a national level; and

- Smart cards and PKI technologies will play a central role in optimizing the identity services, being the enablers and the vehicles of identity management.

REFERENCES

[1] Williamson, G., Yip, D., Sharoni, I., and Spaulding, K. (2009) Identity Management: A Primer. McPress.

[2] Whitman, M.E. and Mattord, H.J. (2011) Principles of Information Security (4th edition). Course Technology.

[3] Stamp, M. (2011) Information Security: Principles and Practice (2nd edition). Wiley.

[4] ABA Report (2011) Trust Framework, ABA Federated Identity Management Legal Task Force [Online]. Retrieved from: http://www.fips201.com/resources/audio/iab_0211/Draft_Trust_Framework-6.pdf. Accessed: 13 June 2011.

[5] Choi, H., Kruk, S.R., Grzonkowski, S., Stankiewicz, K., Davis, B. and Breslin, J.G. (2006) Trust Models for Community-Aware Identity Management [Online]. Retrieved from: http://www.ibiblio.org/hhalpin/irw2006/skruk.html. Accessed: 2 July 2011.

[6] Aberdeen Group (2007) Identity and Access Management Critical to Operations and Security. Communication News. Retrieved from: http://www.comnews.com/WhitePaper_Library/Managed_services/pdfs/Quest_Software_Aberdeen_IAM_Critical_to_Operations_and_Security.pdf. Accessed: 1 June 2011.

[7] Benantar, M. (2005) Access Control Systems: Security, Identity Management and Trust Models. Springer.

[8] Baker, W.H., Hutton, A., Hylender, C.D., Novak, C., Porter, C., Sartin, B., Tippett, P. Valentine, J.A. (2009) Data Breach Investigations Report - Verizon Business [Online]. Retrieved from: www.verizonbusiness.com/resources/.../reports/2009_databreach_rp.pdf. Accessed: 2 July 2011.

[9] Deloitte-NASCIO (2010) State governments at risk: A call to secure citizen data and inspire public trust. The 2010 Deloitte-NASCIO Cybersecurity Study. A publication of Deloitte and the National Association of State Chief Information Officers [Online]. Retrieved from: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_state_2010DeloitteNASCIOCybersecurityStudy_110910.pdf. Accessed: 4 August 2011.

[10] Keeney, M., Cappelli, D., Kowalski, E. and Moore, A. (2005) Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors [Online]. Retrieved from: http://www.secretservice.gov/ntac/its_report_050516.pdf. Accessed: 23 May 2011.

[11] Randazzo, M.R., Cappelli, D., Keeney, M. Moore, A. and Kowalski, E. (2004) Illicit Cyber Activity in the Banking and Finance Sector [Online]. Retrieved from: http://www.secretservice.gov/ntac/its_report_040820.pdf. Accessed: 13 June 2011.

[12] Forrester Report, "Twelve Recommendations For Your 2011 Security Strategy." Forrester Research [Online]. Retrieved from: http://www.forrester.com. Accessed 18 June 2011.

[13] Cser, A. and Penn, J. (2008) Identity Management Market Forecast: 2007 to 2014. Forrester. Retrieved from: http://www.securelyyoursllc.com/files/Identity%20Management%20Market%20Forecast%202007%20To%202014.pdf. Accessed: 1 June 2011.

[14] Trigoso, C. (2010) Thinking of the Future: Identity and Access Management. Retrieved from: http://carlos-trigoso.com/2010/12/22/thinking-of-the-future-identity-and-access-management. Accessed: 13 June 2011.

[15] FIDIS (2006) D5.2b: ID-related crime: Towards a common ground for interdisciplinary research. Retrieved from: http://www.fidis.net. Accessed: 1 June 2011.

[16] KPMG (2008) KPMG's 2008 European Identity & Access Management Survey - Status and maturity of identity and access management projects in European organizations [Online]. Retrieved from:

http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/European-identity-access-management-survey.pdf. Accessed: 23 May 2011.

[17] Aldhizer III, G., Juras, P., & Martin, D. (2008) Using Automated Identity and Access Management Controls. CPA Journal, 78(9), 66-71. Retrieved from Business Source Complete database: http://0-search.ebscohost.com.maurice.bgsu.edu/login.aspx?direct=true&db=bth&AN=35654420&loginpage=login.asp&site=ehost-live&scope=site. Accessed: 1 June 2011.

[18] Reymann, P. (2008) Aligning People, Processes, and Technology for Effective Risk Management [Online] Retrieved from: http://www.theiia.org/intAuditor/itaudit/archives/2008/january/aligning-people-processes-and-technology-for-effective-risk-management. Accessed: 13 June 2011.

[19] Rai, S., Bresz, F., Renshaw, T., Rozek, J., and White, T. (2007). Global Technology Audit Guide: Identity and Access Management. The Institute of Internal Auditors. Retrieved from infotech.aicpa.org/NR/rdonlyres/...9CE1.../GTAG9IdentAccessMgmt.pdf. Accessed: 2 July 2011.

[20] Engelbert, P. (2009) 5 Keys to a Successful Identity and Access Management Implementation [Online]. Retrieved from: http://www.ca.com/files/whitepapers/iam_services_implementation_whitepaper.pdf. Accessed: 8 April 2011.

[21] Links, C.H. (2008) IAM Success Tips: Identity And Access Management Success Strategies.

[22] IDG (2009) As hyper-extended enterprises grow, so do security risks. IDG Research [Online]. Retrieved from: http://www.rsa.com/innovation/docs/IDGResearchWhitePaper_Final_060409.pdf. Accessed: 23 May 2011.

[23] Egan, M. and Mather, T. (2004) The Executive Guide to Information Security: Threats, Challenges, and Solutions. Addison-Wesley Professional.

[24] McQuaide, B. (2003) Identity and Access Management: Transforming E-security into a Catalyst for Competitive Advantage. Information

Systems Audit and Control Association [online]. Retrieved from: http://kuainasi.ciens.ucv.ve/cisa/articles/v4-03p35-37.pdf. Accessed: 13 June 2011.

[25] Al-Khouri, A.M. (2010) Supporting e-government, Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

[26] Al-Khouri, A.M. (2007) Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics. Journal of Computer Science, Vol.3, No. 5, pp.361-367.

[27] Al-Khouri, A.M. (2011) PKI in Government Identity Management Systems, International Journal of Network Security & Its Applications, Vol.3, No.3, pp. 69-96.

[28] Emirates Identity Authority's 2010-2013 Strategy [Online]. Retrieved from: http://www.emiratesid.ae/en/eida/eida-strategy.aspx. Accessed: 1 June 2011.

Towards Federated e-Identity Management Across GCC

Solution's framework [34]

ALI M. AL-KHOURI AND MALIK BECHLAGHEM

ABSTRACT: Many governments around the world have introduced modern Identity Management systems that utilize advanced and sophisticated technologies. The electronic identity (e-identity) card which is a product of such systems is considered an imperative and binding government-issued document for online and offline identification of individuals. There is a global trend in governments to replace conventional identity cards with the e-identity cards. The new card is seen to be an ideal building block for key strategic initiatives related to developing innovative business and service models. One of the initiatives introduced recently in GCC countries is to stimulate e-identity card applications to allow citizens of the different GCC member states to travel between their countries using the new card. A major challenge facing this GCC initiative is related to the interoperability of the different GCC systems. This article is written to explore this area in more detail. It also attempted to put forward an innovative solution framework to leverage

[34] Al-Khouri, A.M. and Bachlaghem, M. (2011) "Towards Federated Identity Management Across GCC: A Solution's Framework", **Global Journal of Strategies and Governance**, Vol. 4, No. 1, pp. 30-49.

and complement existing GCC infrastructures in order to address the need for cross validation of different identity cards issued by GCC member states.

Key words: *electronic identity, federated identity management, interoperability.*

1. INTRODUCTION

FOR For the past 10 years, governments around the world have increasingly shown interest in the deployment of advanced technological systems to establish and confirm identities of their population (Duncan and Al-Khouri, 2010; Al-Khouri, 2011). Modern national identity management systems include biometrics and smart crypto cards that provide strong capabilities to link the biographical data to the personal biological characteristics e.g., fingerprints, facial, iris, etc.

The smart crypto card on the other hand, is a portable document with digitally embedded information and is considered as a token to tie and confirm a given legal identity. This is envisaged by many researchers and practitioners as a breakthrough enabler to revolutionizing public services and many other sectors (Duncan and Al-Khouri, 2010; Petrovic et al., 2003; Shaw, 2003; Shy, 2001). This is to say that electronic authentication and digital signature capabilities of such systems have the potential to contribute significantly to the effective and secure handling of identification requirements in the electronic world.

It is important to highlight here that government officials' and experts in the field have emphasized the need for a globally verifiable electronic identity systems in light of the ever increasing global migration (Noble, 2011). Global migration is considered as a key contemporary social phenomenon. Over the past 15 years, the number of people crossing borders in search of a better life has been rising steadily (BBC, 2011). At the start of the 21st Century, one in every 35 people is an international migrant. If they all lived in the same place, it would be the world's fifth-largest country. According to Research World (2008) more than 190 million people live outside their countries of birth and migrants comprise more than 15 percent of the population in over 50 countries. These numbers will grow as social, cultural, economic and demographic factors intensify (BBC, 2011; Gannon, 2001).

Figure 1 depicts an interesting global migration map with population movement patterns between countries. The green circles represent places where more people are coming in, and the orange circles show countries where more people are leaving.

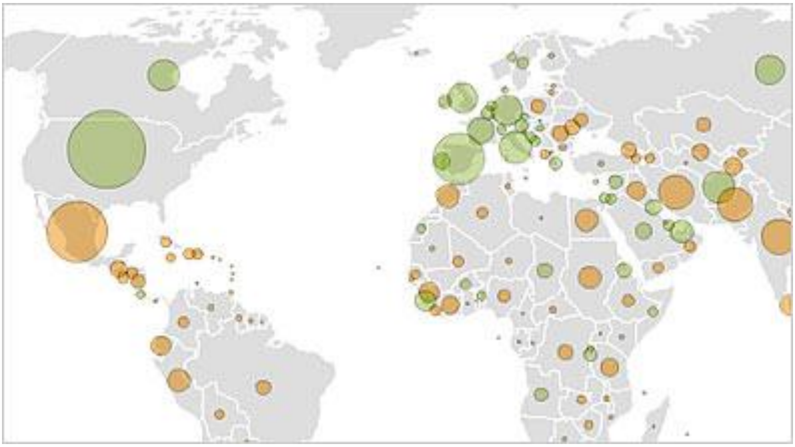


Figure 1: Global Migration
Source: http://southoftheborder.wordpress.com

There a trend in governments to develop a global system that can verify identities of migrant citizens using the same identity document issued by his or her home country. If countries were to issue work and residence permits in an e-identity format that satisfies common international standards, then it is argued that both the migrant workers and the countries themselves would benefit from improved efficiencies and security at the national and global level (Nobel, 2011).

The GCC countries in the Middle East have been among the first implementers of modern identity management systems (Al-Khouri, 2011b). Though with different readiness levels, many of the GCC countries have introduced electronic identity initiatives in public services in the form of e-government projects.

One of the recent ambitious projects underway in GCC countries is to enable GCC citizens to cross GCC borders and access local services in member states (also referred to in this article as domestic services). In practice, there is a clear need for an interoperability framework to address e-identity requirements at a GCC level. It is the intention of the article to outline the associated challenges and delineate a proposed approach for cross validation of different identity cards issued by GCC member states.

The article is structured as follows. A short introduction is provided about GCC countries. The issue of interoperability is then discussed in detail. Next, the business objectives are presented, and the solution framework is explicated. Finally, the key components of the proposed approach are summarized, and the article is concluded.

2. GCC COUNTRIES

GCC is the acronym for Gulf Cooperation Council, also referred to as the Cooperation Council for the Arab States of the Gulf (CCASG). It includes six countries namely, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. The number of GCC population is estimated to be around 40 million people (GCC Portal, 2011). GCC citizens can usually travel freely between member states without the need for visas, and can use either their passports or national identity cards for border crossings.

All GCC countries have initiated a national smart identity card programs with a state of art technologies i.e., smart cards, biometrics, PKI. Although as less as 50% of the population has been enrolled to date for the new ID card, GCC countries are putting in place more strict procedures to ensure the registration of all the remaining population (Al-Khouri, 2011b). The majority of GCC states have developed with varying levels of complexity e-identity service models including Qatar, Saudi Arabia, United Arab Emirates, Oman, and Kuwait. They have recently introduced projects to accelerate the adoption of e-identity in their local societies mainly in the context of e-government.

Among these exciting projects, GCC countries are working to develop a common e-identity infrastructure that will enable the authentication of GCC citizens by any service provider at a member state e.g., border control, public services, etc. In light of the imminent requirement to enable e-identity on the GCC level, a major challenge upraises on the interoperability of these different silo systems. The next section explores this in more detail.

3. INTEROPERABILITY

Plausibly, service providers cannot be expected to deal with the large number of different, manufacturer-dependent interfaces that are offered by smart card readers and smart card services (Vogt, 2004). Therefore, all GCC countries have developed middleware applications to enable interaction and access to their electronic identity cards. This middleware that sits "in the middle" between the user and service portal, is typically a set of multiple interacting layers of software that serve as a bridge between the card and the service providers to facilitate remote identification and authentication of the card and the cardholder (see also Mayes & Markantonakis, 2010; Rankl & Cox, 2007).

Let us consider a simple scenario to elaborate on some of the main interoperability issues. Citizen A of Member State X uses his electronic identity card to access an online public service offered by another Member State Y. In order to provide access to relevant services, the public service provider in Member State Y requires that the citizen uses his or her electronic identity card as a token for identification and authentication prior to be granted access to any particular service.

An ideal situation would be where irrespective of geographical boundaries within GCC countries, a GCC citizen can deal with any GCC online service provider using his e-identity card. Two possible application scenarios for card and cardholder validation can then be prominent in this GCC cross border scenarios:

1. The cardholder, while residing in his home country attempts to perform an e-identity transaction on a foreign (another) GCC country online service provider;

2. The cardholder is residing in a foreign (another) GCC member state and attempts to conduct an e-identity transaction to a foreign (another) online service provider.

These scenarios are envisaged to be arduous to endure as they bring about their own set of challenges as we listed them below.

- The identification process takes place typically through a unique identifier stored in the card and sometimes through a combination of attributes. The user's attributes can be stored in several files and in different formats.

- The authentication of the card and the cardholder requires that the domestic public service provider can interact with the backend infrastructure of the card issuer.

- Interacting with electronic identity cards requires the development of specific security modules to interact with the card on the client computer stations e.g., biometric verification, access to private key, etc.

- For the cardholder to perform an electronic transaction in a foreign (another) country, he oor she requires a client computer station equipped with all required pre-requisites of software and hardware.

4. ABSENCE OF A GENERIC MIDDLEWARE

Smart card middleware is a software connecting smart cards in readers to applications via standardized or proprietary interfaces. In practice, where a public service provider attempts to communicate with a foreign (another) card, communication would not be possible if there is no common interface through which communication can take place between the foreign card and the domestic (local) public service provider.

While all GCC e-identity cards are ISO 7816 standard compliant, certain characteristics of the GCC cards are issuer or vendor specific. In particular, GCC cards have tailor developed and most of the times proprietary applications (i.e., applets). These applications have their own file layouts and formats that expose a dedicated set of APDUs (Application Protocol Data Units). In the context of smart cards, an application protocol data unit (APDU) is the communication unit between a smart card reader and a smart card itself.

Obviously, the first major issue facing the domestic public service providers is related to the absence of a middleware which can recognize a foreign card and interact with it. Standardization efforts would suffer from their high cost and the rapid change of market needs, and practically interoperability would heavily depend on the environment they are used in (Kehr et al., 2001).

4.1 Complexity of backend validations

Another major challenge faced by the domestic public service providers is related to "backend validations" required to complete the electronic transaction. Depending on the business service model defined by the domestic service provider, card or cardholder validation may involve different levels of technical integration. Let us look at each scenario individually.

- If card validation is required, a communication with the card issuer system is required in order to establish that an electronic identity is authentic and valid. Such a validation system has typically a proprietary web interface and requires the public domestic service provider to authenticate itself prior to providing access to the required validation service.

- If cardholder validation is required, a complete revocation path shall be built and validated including the extraction of various CRLs (Certificate Revocation List). While dealing with CRLs may be trivial nowadays, however validating a certification path requires trusting various CAs (Certification Authority) from foreign countries. Establishing such trust relationships may not be as easy to achieve and to manage for a domestic online service provider standpoint.

Each card issuer would normally define a set of online validation services that will be offered to service providers. Some of the validation services would be insignificant from an integration viewpoint and would for example only require access to an LDAP to retrieve CRLs. Other validation services may require advanced and complex set ups and operations. To deal with a foreign card, domestic service provides need to set up and operate separate system to deal with card issuing authority in each country for which an electronic identity are to be supported. The interoperability of systems here could potentially be a stopper point considering the number of potential proprietary backend validations.

4.2 Dealing with on-card required secure messaging

In order to be resilient to sophisticated threat scenarios, electronic identity card issuers in GCC countries have invested heavily in state of the art security mechanisms to guarantee the security of their systems. In some GCC cards, even reading public data files require the initialization of a secure channel communication with the medium. See also Table 1. Setting such secure channels involves specific cryptographic protocols to secure the messaging as well as having shared cryptographic keys between the domestic service provider, foreign card issuer, and the card itself e.g., PIN verification process as part of a PKI authentication.

From an outset viewpoint, such string-based-security models may well enforce the overall security of the electronic identity systems and may show strong cases for proven resiliency to sophisticated threat scenarios. However, such complex security and trust models may induce fundamental developments and set up requirements on both the infrastructure and on the client side.

Since secure messaging is fundamental prerequisite to perform trusted operations with the card, particular hardware is normally required on client stations. Such hardware is typically referred to as Security Access Module (SAM). SAM is designed to act as a general cryptogram computation module or as a security authentication module for smart cards. It is used to interact securely with the electronic identity cards mainly to perform a mutual authentication to guarantee the authenticity of the terminal and the client card.

For a domestic service provider to offer its service to a foreign card, it may have to consider the deployment of SAM devices that can support secure messaging with different interfaces. The alternative to using SAM devices is to hardcode the electronic identity issuer attributes in the software which is an option that may be appropriate within a domestic scheme. However within a GCC interoperability framework, relying on keys in software may go against the interests of some political and technical policies.

Table 1: Security Enforcement on GCC ID cards

	What's in the chip?	How is security enforced?
Data containers	Public data including: • Cardholder data (name, unique identifgier, address, sponsor, ...etc) • Card data (card nuber, etc)	• Typically 100 % accurate information contained in files digitally signed by the eID issuer • Organizations can read the data and then validate the signature on to establish that the data is accurate. • In some cases, secure messaging with the eID is required in order to read public data files.
	• Private data containers some owned by the eID issuer and some by other organizations, for example: • Family book, eHealth	• Secure messaging with the eID card si required in order for an external entity to conduct operations on the contaimer
Authentication	• PKI credentials typically contaimed within a PKI applet on the eID card: • Authentication key pair • Authentication digital certificate	• PIN code protection where the cardholder introduces his PIN in order to authorize the usage of his ID card for authentication • In some eID cases, conducting a secure messaging with the eID is a pre-requisite to perform PIN verification by th eeID • The service provider shall validate the authentication certificate prior to completing the authentication process with the cardholder
	• Biometric application enabling the verification of holders with biometrics (fingerprints)	• In most of the known cases, conducting secure messaging with the eID card is a pre-requisite to conducting biometric verification

4.3 Too many client dependencies

Another important challenge relates to the dependencies required on the client computer station in order for a cardholder to be able to use his e-identity card to access a foreign online public service. The middleware may not support the OS platform or browser available on the client station.

In addition to that, the actual middleware itself or some of its software components may require to be pre-installed on the client computer station prior to any e-identity transaction to occur. Last but not least, our experience in GCC countries shows latency and slowness in enabling the download of web components (ActiveX, applet) of the e-identity middleware as part of service provider portal pages.

5. VISION AND BUSINESS OBJECTIVES

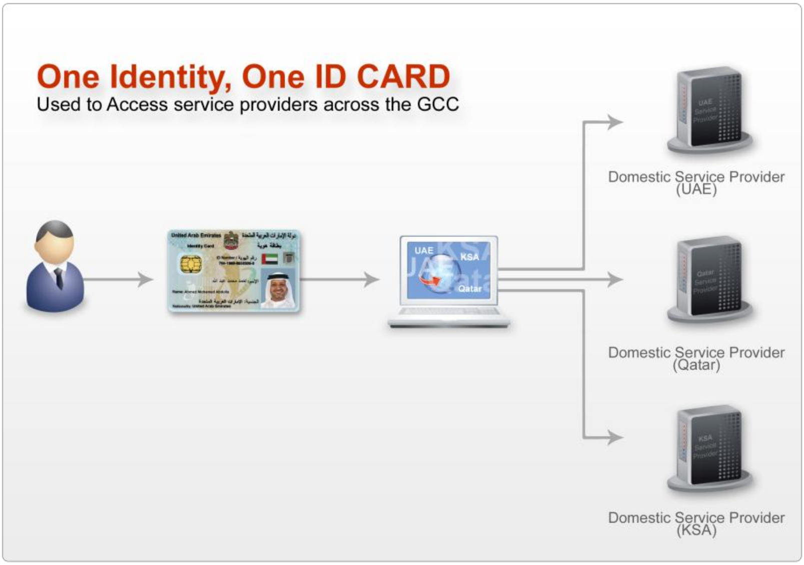

One Identity, One ID CARD
Used to Access service providers across the GCC
UAE
KSA
Qatar
Domestic Service Provider (UAE)
Domestic Service Provider (Qatar)
Domestic Service Provider (KSA)

Figure 2: One Identity, one e-identity concept across GCC countries

Having clarified the problem areas, a number of assumptions were laid down to guide the development of the proposed framework and to define its direction. Figure 2 illustrates a graphical representation of the desired project outcome. The following elements were seen as key strategic objectives to implement the common e-identity infrastructure:

- Primarily, and in order for a GCC member state to engage in a common e-identity infrastructure initiative, it needs to have already invested in some form of e-identity validation and authentication services;

- Domestic (local) online services need to be accessible to mobile GCC citizens;

- Building a more citizen inclusive GCC community and enhancing the sense of GCC citizenship through supporting different domestic business service models;

- Improving and combating ID fraud and ID theft across GCC countries;

- Improving the effort related to preventing illegal work, illegal immigration and organized crime.

The proposed development framework is presented and discussed next.

6. THE SOLUTION FRAMEWORK – FEDERATED eID MANAGEMENT

6.1 Federated e-identity management - Conceptual view

It was envisaged that an interoperable solution would meet public and authorities' acceptance across GCC countries only if it meets some basic requirements as listed below:

- The solution framework shall take into consideration existing GCC members' independent e-identity schemes deployments and technical implementation rather than trying to replace them. GCC states have already invested heavily in building their e-identity infrastructures and it would be impractical to suggest an approach that induces fundamental changes on existing infrastructures.

- The solution framework shall not disturb domestic online service providers dealing with foreign e-identity cards. The best solution framework shifts the entire card transaction from the domestic service provider to the issuer of the foreign e-identity card. The domestic service provider would only need to redirect the cardholder to relevant online services offered by the e-identity issuer where card interaction is going to take place. At the end of an e-identity card transaction, the domestic online service provider receives an assertion from the eID issuer on the result of the card/cardholder transactions.

- Any proposed solution framework shall be user centric. While the user would be conducting transactions with a foreign service provider, the user should still have the perception that he or she is being validated by his own e-identity issuer. He would as such still be in control of the information that is revealed to the foreign online service provider. In addition to this, the solution framework shall guarantee user mobility by enabling e-identity card transactions with minimum dependencies on the client computer stations. The best solution framework shall guarantee that e-identity transactions on a client computer station have no dependencies apart from the availability of a smartcard reader.

- An interoperable solution framework shall support at minimum PKI authentication where the cardholder can be authenticated within any GCC member state using his e-identity card PKI capabilities. In addition, the solution framework shall offer the means for online public service providers to identify the cardholder via proper identifiers.

Looking at the above requirements, a Service Provider (or Identity Provider) implementation model is recommended where every e-identity scheme owner would make available e-identity validation services for online service provider within GCC countries. From a conceptual standpoint, this would enable the implementation of a federated e-identity infrastructure across the GCC countries where a domestic online service provider would redirect a cardholder to the e-identity validation services of the e-identity scheme owner as depicted in Figure 3.

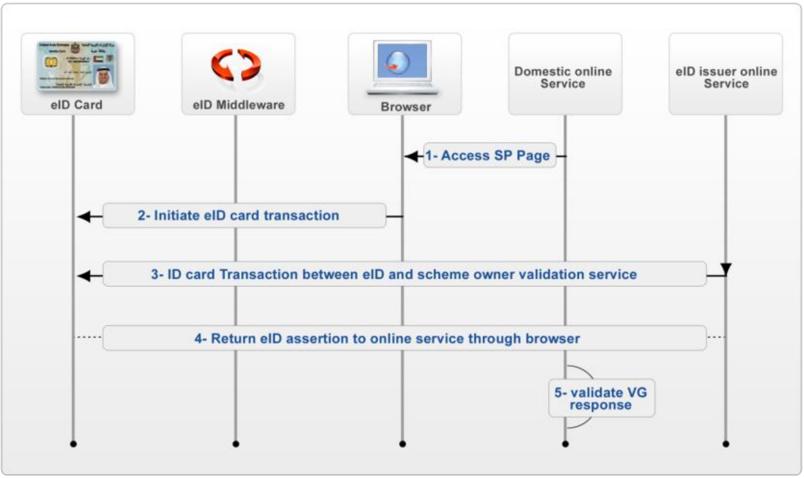

eID Card
eID Middleware
Browser
Domestic online Service
eID issuer online Service
1- Access SP Page
2- Initiate eID card transaction
3- ID card Transaction between eID and scheme owner validation service
4- Return eID assertion to online service through browser
5- validate VG response

Figure 3: Federated e-identity management concept

The overall flow of an e-identity transaction in the proposed model is as follows:

1. The e-identity cardholder visits the website of the domestic online service provider. This would require the e-identity issuer middleware to be loaded on the end user browser.

2. The e-identity transaction is triggered from the browser using one of the middleware functions.

3. An end-to-end card transaction occurs between the e-identity card and the backend validation services of the e-identity scheme owner. This communication happens through the middleware and the service provider is not involved at this stage.

4. A validation response is returned to the browser. This response would be an assertion from the e-identity scheme owner validation service to confirm or reject the transaction. It

indicates the status of the validation (success/failure) as well as relevant attributes such as cardholder unique identifier and card number. This request is typically signed and timestamped. The browser returns the response to the domestic online service provider.

5. The online service provider validates the response and provides or denies the access to the service accordingly.

The above approach allows implementing the concept of federated e-identity management between e-identity scheme owners within the GCC countries. The e-identity scheme owner acts as an identity provider exposing e-identity validation services that deal with all backend interactions such as interacting with the CA to perform certificate validation, accessing backend directory/database services for card/cardholder validations, etc.

Such approach enables each e-identity scheme owner to keep control of their existing backend infrastructure with minimum disturbance. On the other hand it guarantees minimum integration requirements on domestic online service providers as illustrated in the above figure where the actual card interaction is completely shifted from the service provider to the e-identity scheme owner. Last but not least, the desired level of security is met assuming that all e-identity cards and schemes offer at minimum two-factor authentication of the cardholder with PKI.

6.2 Federated eID management – Common eID interfaces

The concept of cross GCC e-identity federation services presented above addresses some important interoperability requirements. It guarantees minimum impact on e-identity scheme owners' backend infrastructure as well as low integration requirements for domestic online services providers.

In order to ensure a full interoperable solution, adequate formats must be agreed between e-identity scheme providers that would allow domestic service providers to support multiple e-identity schemes each having its own client middleware. At minimum e-identity scheme owners shall agree on a common e-identity client middleware as well as on common e-identity validation (assertion) mechanisms.

6.2.1 Common e-identity client middleware interface

While each e-identity scheme would have its own client middleware, a common interface shall be agreed between the e-identity scheme owners. Each e-identity scheme owner would provide an implementation of such interface so that a service provider would use the same interface regardless to which e-identity card is used.

The common middleware interface would specify a set of business functions such as:

- PKI Authenticate: functions that perform cardholder verification with PKI.
- Certificate validation: functions that perform the online validation of the cardholder certificate using standard protocols such as OCSP (Online Certificate Status Protocol).

- Card Status: a function that performs card status validation. It indicates whether the e-identity card is genuine and returns its status (revoked/active).

- Biometric verification: a function that performs cardholder verification with fingerprint validation. Match-Off-Card or Match-On-Card could be implemented by the e-identity scheme owner depending on the e-identity capabilities and technical constraints.

It would be at the discretion of the e-identity scheme owner to implement a subset or all of the interface functions. However, the minimum requirements for the e-identity scheme owner would be to offer an implementation of the cardholder verification with PKI as well as the card status validation. The following Figure 4 illustrates the components of the common e-identity middleware interface and how it could be used.

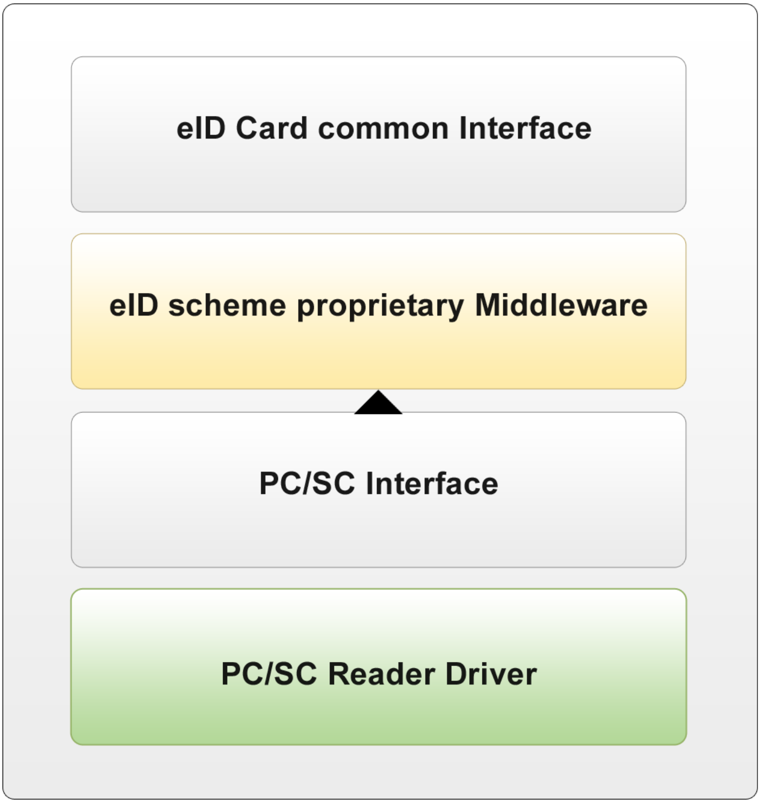


Figure 4: Common e-identity interface

6.2.2 Common eID validation assertion

The federated e-identity management concept relies on an e-identity validation assertion that is returned by the e-identity scheme owner validation server. An adequate format for the validation assertion shall be agreed by GCC e-identity scheme owners. It shall incorporate the minimum card and cardholder attributes in a manner that is clear and understandable by domestic online public service providers. The minimum attributes to be returned in the validation assertion should be as follows:

- Cardholder unique identifier: an identifier uniquely identifying the cardholder as read from the e-identity card;

- Card number: indicating the unique identifier of the e-identity being processed;

- Validation request type: indicating the type of request processed by the e-identity scheme owner validation service (card validation/cardholder verification with PKI, etc.);

- Validation status: indicating whether the validation succeeded of failed;

- Validation time: timestamp indicating the time at which the validation service performed the validation and created the validation assertion; and

- Validation period: duration (in seconds) of validation of the assertion.

The agreement on a common validation assertion format is considered to be a breakthrough capability for e-identity interoperability across the GCC countries. It guarantees a common format for the domestic online service providers for all GCC e-identity schemes.

6.3 Federated e-identity management – Formats and standards

6.3.1 Common e-identity client middleware interface

The common e-identity interface as described earlier in this article is implemented by the e-identity scheme owner on top of the proprietary/legacy e-identity middleware. It is assumed that the existing e-identity middleware covers online web scenarios and as such it integrates web components in the form of an ActiveX or Applet or both. Within a domestic scenario, these web components are used by domestic online service providers and embedded within its web/portal pages. Typically, functions of the web component (Activex/applet) are triggered through Javascript code that may be produced by the online web service provider.

An important principle of the federated e-identity management solution framework is that it takes into consideration existing e-identity schemes infrastructure and should induce as minimum impacts on these as possible. Therefore, an interesting approach to implement the e-identity common interface would be to use a common Javascript specification on top of the existing e-identity schemes web components (Activex/applet). This would mean that each e-identity scheme owner would provide a set of Javascript functions for the e-identity business function it exposes.

A simple scenario is presented to elaborate further the suggested e-identity middleware common interface. The e-identity scheme owner of GCC member state X has an Applet part of his existing e-identity middleware. The Applet exposes a PKI authentication function called "PKI authentication()".

On the other hand, the eID scheme owner of another GCC member state Y has an Applet part of his existing e-identity middleware that exposes a PKI authentication function called "CardholderAuthenticate()". In order to illustrate the common e-identity interface concept, a domestic online service provider from a GCC member state Z is introduced. The e-identity common interface would include a set of Javascript functions to be implemented by each member state. For example, the PKI authentication Javascript function would be referred to as "PKI Authenticate". E-identity scheme owners from member X and Y would provide an implementation of this Javascript function "PKI Authenticate" that would be used by the domestic online service provider depending whether he or she is dealing with an e-identity from state X or Y. Figure 5 below illustrates this simple scenario.

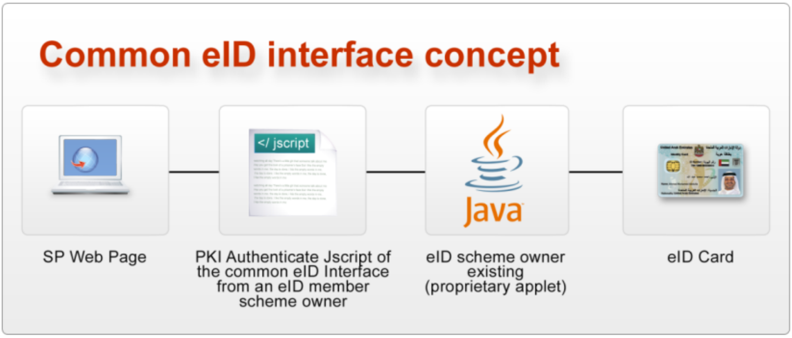

Common eID interface concept
</ jscript
Java
SP Web Page
PKI Authenticate Jscript of the common eID Interface from an eID member scheme owner
eID scheme owner existing (proprietary applet)
eID Card

Figure 5: Common e-identity middleware interface implementation concept

It is noted that other options to implement a common e-identity middleware interface are possible and discussing them is not part of the scope of this article. It seems however that the approach suggested is quiet innovative and induce minor impacts on e-identity scheme owners existing investments in their e-identity front-end (client) and backend interfaces.

6.3.2 Common e-identity validation assertion

The federated e-identity management concept relies on an e-identity validation assertion that is returned by the e-identity scheme owner validation server to the domestic online service provider. The online service provider validates the assertion and completes the e-identity transaction.

The first observation here is that the assertion shall be of a common format and that there shall be means for the online service provider to validate the assertion that originates from a trusted e-identity scheme and that it has not been tampered with during its transport over the network. It is therefore suggested that the common e-identity validation assertion is a signed XML document that incorporates three types of data as follows:

- Data identifying the e-identity scheme member;
- Data identifying the e-identity card including cardholder unique identifier and e-identity card number;
- Data identifying the transaction status including validation status, validation timestamp and assertion validation period.

The federated e-identity management concept is recommended to implement a Service Provider – Identity Provider (SP – IdP) model based on SAML standard (Security Security Assertion Markup Language). This is considered to be a contemporary practice in the field of Identity Management. SAML is an XML-based open standard for exchanging authentication and authorization data between entities from different security domains. In particular, SAML is well suited for Service Provider (SP) that decides to offload the whole authentication process to a trusted Identity Provider (IdP) which is also referred to as SP-IdP model.

Looking at the federated e-identity management concept, the domestic online service provider acts as a Service Provider (SP) relying on an e-identity scheme owner to validate an e-identity card transaction and that is therefore acting as an IdP. Therefore, SAML appears to be an obvious option for the common e-identity validation assertion format. SAML assertion may allow the minimum data attributes for the e-identity validation assertion listed above.

As a conclusion, the e-identity validation assertion format should at least comply with SAML format. As a means to support service providers that have not invested in a SAML infrastructure, a dedicated XML schema (format) for the common e-identity validation assertion across GCC should be specified and used. Depending on the transaction context, the e-identity scheme owner validation service will return an e-identity validation assertion in either SAML or any other specified GCC format.

6.4 Federated eID management –eID scheme discovery in a mobile GCC environment

The discussion so far on the federated e-identity model can be summarized as follows:

- A common e-identity middleware is used by the domestic service provider to interact with a foreign e-identity card. This middleware is used as a bridge between the e-identity card and the target e-identity scheme owner validation services.

- The e-identity scheme owner validation services execute an end-to-end transaction with the e-identity card through the common e-identity middleware software components. It then responds with a proper e-identity validation assertion that can be conveyed to the service provider who will validate it.

The fundamental issue that is remaining is how the domestic service provider would recognize the e-identity card as coming from a specific GCC country member so that it can then call and use the proper e-identity middleware for that target e-identity scheme owner. There are three possible options to circumvent this challenge. All options assume that the e-identity card scheme can be identified using the e-identity ATR (Answer To Reset) that can be read from the e-identity. The possible options are discussed below.

1. In the 1st option, all the different common middlewares implementations from various Member States are put together as one module that can be installed on the service provider site. This can then be downloaded as part of the initial steps of the e-identity card transaction. Once the service provider page recognizes the origin of the e-identity card (i.e. its ATR), it can then invoke the proper e-identity common interface for the target eID scheme owner.

2. In the 2nd option, each e-identity scheme owner may build the support in its e-identity middleware for foreign GCC e-identity cards. This would result in a large e-identity

middleware to be distributed by the e-identity scheme owner to online service providers within the same country. Once the service provider page recognizes the origin of the e-identity card (i.e. its ATR), it can then invoke the proper e-identity function calls from the e-identity middleware augmented with the support of all e-identity schemes.

3. In the 3rd option, the domestic service provider relies on a discovery service that is part of the overall federated e-identity management solution. The discovery service is used to discover where the e-identity card is originating. It then has the capability to download in real time the e-identity middleware of the target e-identity scheme. Once loaded on the browser, the target scheme e-identity middleware is used to initiate the relevant e-identity transaction with the e-identity scheme owner validation services.

Options 1 and 2 seem to be impractical to implement. They go against one of the main objectives of GCC interoperability which is ensuring minimal impacts on existing e-identity schemes. Moreover, they would involve large e-identity middleware components that impact end user experience and the overall e-identity transaction performance.

The 3rd option involves a new building block for the federated e-identity management solution framework which is the e-identity discovery service. This option copes with all interoperability requirements and is therefore the option recommended to be part of the federated e-identity management solution framework. Figure 6 illustrates how the discovery service is used.

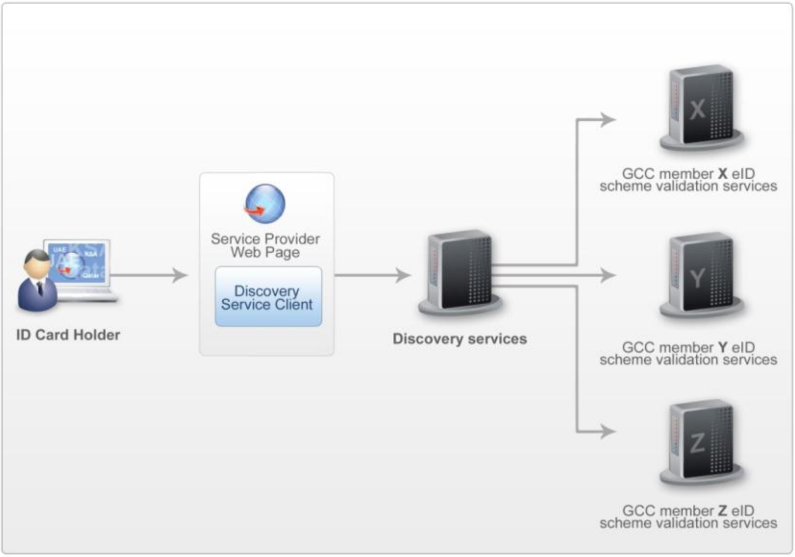

ID Card Holder
Service Provider Web Page
Discovery Service Client
Discovery services
X
GCC member X eID scheme validation services
Y
GCC member Y eID scheme validation services
Z
GCC member Z eID scheme validation services

Figure 6: e-identity discovery service

The discovery service would provide a lightweight web component (Applet/active X) that is loaded with the domestic service provider page visited by the e-identity cardholder. This web component will then read the card ATR through a standard APDU command.

The discovery service web component will then query its discovery service that is configured with details of each GCC member state e-identity scheme owner. The discovery service will query a dedicated service from the target e-identity scheme owner validation services that will return data to be used by the discovery web component to load the e-identity middleware. This data consist mostly in HTML tags and file paths that would enable the discovery service web component to download the target e-identity scheme owner e-identity middleware.

The discovery service web component loads the target e-identity scheme middleware that will then take control of the card transaction. Figure 7 below illustrates the discovery service web component and e-identity scheme owner middleware.

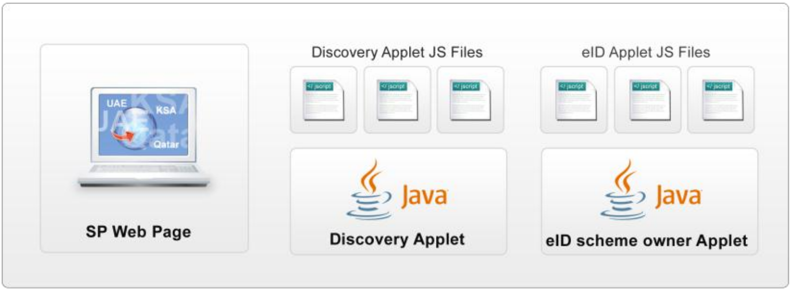


Figure 7:Discovery service and eID scheme owner middleware

Depending on the agreements between GCC member states, there could be one discovery service across GCC with its mirror site. These would be used by service providers from all GCC countries. Another approach would be to have one discovery service within each GCC country that could be hosted within the domestic e-identity scheme owner infrastructure. Opting for one of the options would be dependent on the logistical and political reasons but implementing either option is equally possible.

6. SOLUTION'S BUILDING BLOCKS AND FUNCTIONAL SUMMARY

The earlier sections of this article attempted to present the proposed federated e-identity management framework, its guiding principles and an overview of the building blocks of the approach. The following components were introduced as important building blocks and their role and potential implementation were discussed:

1. e-Identity Validation Gateway (VG): a Server exposing the e-identity scheme owner card validation services as web services available over the cloud. At minimum, the VG shall expose a reliable cardholder authentication method using his or her e-identity. The recommended minimum services to expose on the e-identity VG are as follows:

    - PKI Authentication: a service that interacts with the e-identity card and performs an end-to-end PKI authentication protocol. This involves PIN verification, challenge-response protocol certificate validation using CRLs or OCSP depending on the local scheme PKI infrastructure.

    - Verify Card Status: a service that interacts with the e-identity card and performs card validation. It indicates whether the card is genuine and returns its status (revoked/active).

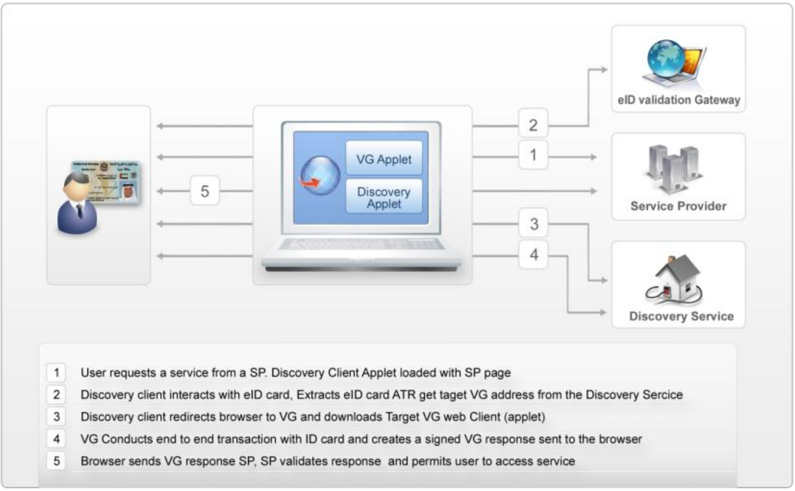
    - Biometric verification: a function that conducts cardholder verification with 1-to-1 fingerprint matching to relevant ISO/IEC 7816 biometric standards.

2. e-identity discovery service: a server dedicated to discovering the target e-identity VG to query the client terminal in order to execute a specific card transaction.

3. e-identity common middleware: set of software libraries exposing the e-identity card business functions to service

providers. In a web environment, the e-identity common middleware consists in the e-identity VG applet which interacts with the VG in order to conduct an end to end e-identity card transaction.

Figure 8 illustrates the above three components that are jointly involved in an eID card transaction.



1 User requests a service from a SP. Discovery Client Applet loaded with SP page

2 Discovery client interacts with eID card, Extracts eID card ATR get taget VG address from the Discovery Sercice

3 Discovery client redirects browser to VG and downloads Target VG web Client (applet)

4 VG Conducts end to end transaction with ID card and creates a signed VG response sent to the browser

5 Browser sends VG response SP, SP validates response and permits user to access service

Figure 8: Federated eID management solution framework summary

CONCLUSION

Electronic Identity (e-identity) cards are being issued across the world. These are seen as enablers for secure online services in general and in particular as the enabler of smart societies where the citizen is closer to his or her local authorities. Electronic identity cards are also seen to be the ideal tool to build a more inclusive and secure communities.

GCC countries have initiated multiple projects related to advanced applications development of their e-identity schemes. GCC countries are currently working on developing a unified e-identity infrastructure to enable identification and authentication of GCC citizens at any of the GCC member states. This raises serious interoperability issues due to the different and complex infrastructure setups at each member state and would likely challenge such a project.

This article attempted to outline the challenges related to offering cross GCC e-identity transactions. An innovative solution framework has been presented that leverages and complements existing investments in e-identity schemes and infrastructure. The framework referred to in this article as the federated e-identity management relies primarily on three key enablers: (1) domestic Validation Gateway (VG) put in place by domestic eID scheme owners; (2) Discovery Service that enables real time discovery of a target eID scheme owner by a domestic online service provider, and (3) a common Middleware to enable interaction with the VG and end-to-end transaction.

We do note that other options to implement a common e-identity middleware interface were possible however, discussing these were not part of the scope of this article. Nonetheless, the suggested overall approach is believed to be quiet innovative and induce minor impacts on e-identity scheme owners existing investments in their e-identity front-end (client) and backend interfaces.

The proposed framework supports the concept of coherent distributed and interoperable architectures development, which in turn should enable and simplify complex distributed applications. The approach should enable service providers to securely verify, certify and manage identification and access of citizens seeking physical or logical access.

The proposed approach was at the discussion stage between the GCC member states at the time of writing this article. Once agreed on the underlying guiding principles a better understanding will evolve of the roadmap to implement the solution across GCC. The next steps should include detailed GCC e-identity schemes survey, development of Validation Gateway and Discovery Service Specifications, and the launch of a pilot implementation.

REFERENCES

[1] Al-Khouri, A.M. (2010) "Supporting e-Government," Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

[2] Al-Khouri, A.M. (2011) "PKI in Government Identity Management Systems," International Journal of Network Security & Its Applications, Vol.3, No.3, pp. 69-96.

[3] Al-Khouri, A.M. (2011b) Rethinking Enrolment in Identity Schemes, International Journal of Engineering Science and Technology, Vol. 3, No. 2, pp. 912-925.

[4] BBC (2011) Migration Boom [Online]. Available from: http://news.bbc.co.uk/2/shared/spl/hi/world/04/migration/html/migration_boom.stm

[5] Gannon, J.C.(2001) 2001 Growing Global Migration and Its Implications for the United States.

[6] GCC Portal: http://www.gcc-sg.org/eng/index.html)

[7] Kehr, R., Rohs, M. and Vogt, H. (2000) "Issues in Smartcard Middleware." In: Attali, I. and Jensen, T. (Eds.): Java on Smart Cards: Programming and Security. LNCS, Vol. 2041, Springer-Verlag, pp. 90-97.

[8] Mayes, K. and Markantonakis, K. (Eds.) (2010) Smart Cards, Tokens, Security and Applications. Springer.

[9] Noble, R.K. (2011) Interpol chief calls for global electronic identity card system. Available from: http://www.net-security.org/secworld.php?id=10860.

[10] Petrovic, O., Ksela, M., Fallenbock, M., & Kittl, C. (2003) Trust in network economy. New York: Springer.

[11] Rankl, W. and Cox, K. (2007) Smart Card Applications: Design models for using and programming smart cards. Wiley.

[12] Research World (2008) More than 190 million people live outside their country of birth. [Online]. Available from: www.esomar.org/uploads/pdf/.../RW0807_MakeYourselfAtHome.pdf

[13] Shaw, M. (2006) Commerce and the digital economy. Armonk, NY: Sharpe.

[14] Shy, O. (2001) The economics of network industries. New York: Cambridge University Press.

[15] Vogt, H., Rohs, M. and Kilian-Kehr, R. (2004) Middleware for Communications. John Wiley & Sons.

Contemporary Identity Systems Implementation

Re-thinking Enrolment in Identity Card Schemes[35]

DR. ALI M. AL-KHOURI

ABSTRACT: Many countries around the world have initiated national ID card programs in the last decade. These programs are considered of strategic value to governments due to its contribution in enhancing existing identity management systems. Considering the total cost of such programs which goes up to billions of dollars, the success in attaining their objectives is a crucial element in the agendas of political systems in countries worldwide. Our experience in the field shows that many of such projects have been challenged to deliver their primary objectives of population enrolment, and therefore resulted in failing to meet deadlines and keeping up with budgetary constraints.

The purpose of this paper is to explain the finding of a case study action research aimed to introduce a new approach to how population are enrolled in national ID programs. This is achieved through presenting a case study of a business process reengineering initiative undertaken in the UAE national ID program. The scope of

[35] Al-Khouri, A.M. (2011) "Re-Thinking Enrolment in Identity Schemes", International Journal of Engineering Science and Technology, Vol. 3, No. 2, pp. 912-925.

this research is limited to the enrolment process within the program. This article also intends to explore the possibilities of significant results with the new proposed enrolment approach with the application of BPR. An overview of the ROI study has been developed to illustrate such efficiencies.

Key words: *National ID; BPR; ROI.*

1. INTRODUCTION

IN today's dynamic global business environments, organisations both in public and private sectors are finding themselves under extreme pressure to be more flexible and adaptive to such change. Over the past two decades, organizations adopted business process reengineering (BPR) to respond to such business agility requirements.

This is based on the belief that process is what drives the creation and delivery of an organization's products and services (Evans, 2008). The literature demonstrates that BPR can yield profound and dramatic effects on lowering costs, quality of service delivery and customer satisfaction (Hammer and Champy, 2003; Jeston and Nelis, 2008; Madison, 2005). Thus, it considers it as an important approach to transform operations, and to achieve higher levels of efficiency and effectiveness. In short, BPR is more of a holistic approach to change with a comprehensive attention to process transformation in light of social issues, business strategy, people performance, and enabling technologies.

Many governments around the world have initiated national ID card programs with allocated budgets exceeding multi-billions of dollars. Many of such programs worldwide have been challenged to achieve their core objective of population enrolment (Al-Khouri, 2010). Taking into consideration the strategic objectives of such programs and high budgets, it is deemed necessary that learnings from various implementations are shared between practitioners in the field to address common challenges and learn from best practices. It is the purpose of this paper to contribute to the current body of knowledge and present an action based case study research in one of the most progressive countries in the Middle East. It attempts to present a case study of a process re-engineering project that was implemented in the United Arab Emirates (UAE) national ID program. It also sheds light on the staggering results gained from such an exercise.

This paper is structured as follows. First, a short literature review of the BPR concept is provided. Some background information about the project and the triggering needs for process improvement are discussed next. Some reflections and management consideration areas are discussed afterwards, and it ends with some concluding remarks and possible future research areas related to this topic.

2. LITERATURE REVIEW: BUSINESS PROCESS REENGINEERING AND NPM

Process reengineering has long history and application as it evolved overtime in various forms to represent a range of activities concerned with the improvement of processes. The reengineering concept goes back in its origins to management theories developed as early as the late eighteenth century, when Frederick Taylor in 1880's proposed process re-engineering to optimize productivity and improve performance. 30 years later, Henri Fayol, instigated the reengineering concept seeking to derive optimum results from available technology resources in a manufacturing environment (Lloyd, 1994).

Some revolutionary thinking was added to the field in the past two decades. For instance, Davenport and Short (1990) presented process re-engineering as the analysis and design of work flows and processes within and between organizations. Extending the work of Porter (1980, 1985, 1990) on competitive advantage,

Hammer and Champy (1993) promoted the concept of business process reengineering as a fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in key performance measures e.g., cost, quality, service, and speed (see also Lowenthal, 1994; Talwar, 1993).

The reengineering concept has evolved in the recent years to reconcile with more incremental process management methods such as Total Quality Management; often referred to as TQM (Davenport and Beers, 1995; see also Caron et. Al, 1994; Earl and Khan, 1994). Other researchers have integrated reengineering with other modern management concepts such as knowledge management, empowerment, organization theory, organization control, strategy, and MIS (Earl et al., 1995; Kettinger & Grover, 1995).

Reengineering, in general, questions all assumptions about the way organisations do business and focuses on the how and why of a business process to introduce major changes to how work is accomplished. In fact, it moves far beyond mere cost cutting or automating a process to make marginal improvements (Cash et al., 1994). According to Davidson (1993), successful reengineering efforts ultimately lead to business transformation. New products, services and customer services appear in the form of improved information flows (ibid).

Several studies pointed out that while the potential payback of reengineering is high, so is its risk of failure and level of disruption to the organizational environment. Introducing radical changes to business processes in an attempt to dramatically improving efficiency and effectiveness is not an easy chore. While many organisations have reported impressive augmentation and accomplishments, many others have failed to achieve their objectives (Davenport, 1993; Keen, 1991).

Reengineering in whatever form or name it appears in, seeks to improve the strategic capabilities of an organisation and add value to its stakeholders in some idiosyncratic ways. Strategic capabilities are the means and processes through which value is added, as distinct from the products and services perspectives and their competitive positioning in the marketplace.

In government context, process reengineering has been associated with Public Administration Reform often referred to as New Public Management (NPM), a term used to transform and modernize the public sector. NPM seeks to enhance efficiency of the public sector and the control framework with the hypothesis that more market orientation in the public sector will lead to greater cost-efficiency for governments, without having negative side effects on other objectives and considerations. Dunleavy et al., (2006) defines NPM as a combination of splitting large bureaucracies into smaller, more fragmented ones, competition between different public agencies, and between public agencies and private firms and incentivization on more economic lines (Dunleavy et al., 2006).

It is such concepts that are pushing public sector organizations nowadays to act similar to those in the private sector. Therefore, governments around the world are transforming their mindsets of how they view their citizens and treat them as customers, with much emphasis on leveraging technology to building long-term relationships with their citizens. This has raised expectations of customers' relentless demands in quality and service in this sector.

The new power and freedom of the customer has destroyed many of the organisational assumptions of the early role of government, and placed them as a new powerful stakeholder. So process reengineering in this context is concerned more with facilitating the match between customer needs and organisational capabilities in light of the government roles and responsibilities. Many governments have initiated process re-engineering projects to develop citizen-focused, service oriented government architectures, around the need of the citizens, not those of the government agencies.

By and large, governments nowadays are put under tremendous pressure to strive for operational and financial efficiencies, while building an environment that encourages innovation within the government, in light of population growth, demographic changes, technological and knowledge 'explosions', and increased citizen expectations (Gordon and Milakovich, 2009). The following section outlines the research methodology and it contribution the body of knowledge.

3. RESEARCH METHODOLOGY

The research methodology adopted in this study was a mixed approach of action and case study research. The phenomenon measured in this study was considered to be too complex, and needed to be constructed and measured experimentally, and particular attention was paid to the organisational (and local) idiosyncrasies that permeate all true natural settings.

Action research is defined as "a type of research that focuses on finding a solution to a local problem in a local setting" (Leedy & Ormrod, 2005, p. 114). Action research is a form of applied research where the researcher attempts to develop results or a solution that is of practical value to the people with whom the research is working, and at the same time developing theoretical knowledge. Through direct intervention in problems, the researcher aims to create practical, often emancipatory, outcomes while also aiming to reinform existing theory in the domain studied.

Case study research, on the other hand, is a common qualitative method (Orlikowski & Baroudi, 1991; Alavi & Carlson, 1992). Although there are numerous definitions, Yin (2002) defines the scope of a case study as an empirical inquiry that (1) investigates a contemporary phenomenon within its real-life context, especially when, (2) the boundaries between phenomenon and context are not clearly evident (Yin, 2002).

Action research was found particularly appropriate to investigate and describe the situation, the issues at hand and its context to effect positive change in the situation. Clearly, the case study research method is particularly well-suited to this research, since the objective of our study is the systems in the organization, and our "interest has shifted to organizational rather than technical issues" (Benbasat et al. 1987).

The study development was primarily facilitated by the senior role of the researcher in the examined organization. The study was based on both primary and secondary data. Data were gathered from business documents, technical specifications, annual reports, observation, and both formal and informal discussions with key stakeholders in the organization.

3.1 Study Contributions: National Identity Management Systems

Many governments around the world have initiated national Identity management systems. The nature and operating model of these systems make it extremely vulnerable to considerable challenges. The customer base for such programs is basically all resident population in a country setting, and such programs require the physical presence of people to complete the registration process i.e., require the capturing of biometrics.

There are more than 130 countries that have already implemented such systems and many other countries are seriously considering the implementation of such programs. The huge amount of program cost and the complexity of its infrastructure technologies further contribute to it being challenged.

Our previous studies in the field (Al-Khouri, 2010; Al-Khouri, 2007) presented to us that these programs are challenged to meet their primary objective of population enrolment. This would in turn have a serious impact on the original implementation time frames and the allocated budgets set by governments. It is also noted that existing literature include very little data about practices about this important and critical field.

In fact what makes this study of high contribution is related to the fact that we are not aware of any previous research in this area, which points out the significance of this study. It is our attempt therefore to contribute to the existing body of knowledge and share experiences of such implementations and associated critical insights. This should serve as guidelines for framing their practices in the implementation of similar projects world over.

3.2 Research Limitation

It is comprehended that case studies and action research are usually restricted to a single organisation making it difficult to generalise findings, while different researchers may interpret events differently. The research in this study restricted to a single organisation, thus a major limitation of this research is the sample size that limits generalizability.

Having said that, the next section provides an overview of the case study organisation and high level results achieved through business process reengineering of core functions.

4. EMIRATES IDENTITY AUTHORITY

The Emirates Identity Authority (Emirates ID) is a federal government authority established in 2004 to develop and manage the implementation of a national identity management infrastructure in the United Arab Emirates. The organization began to rollout the program in mid 2005 and managed to enrol a population of 1.1 million over a 4 years period. The registration process was widely criticized by the population for being "hectic" and gained the organization with some negative reputation in the media. Long waiting times, complex registration procedures, high turnover rates, increasing costs; all indicated performance setbacks. The organization was in a real dilemma and a change from status was needed.

In late 2009, the Vice Chairman of the Board of Directors at Emirates ID articulated the need for a radical change program to examine lagging performance results. The new appointed Head of Executive Board Committee and the Director General established ambitious goals for drastic improvements throughout the organization, and they paid attention in particular to selected business areas related to the intake and the production cycle capacities at registration centres; where criticism was most. Specific goals included reducing applicant registration and waiting times by at least 50 per cent. The new management team decided to take a system-wide view of the organization and perceive its business as a factory with production lines environment that harnesses the potential of teams.

The workforce at production line processes were evaluated and rewarded based on their performance. In a little over one year, the organization achieved monstrous results; increased intake capacity by 300%, reduced registration time by 80%, reduced applicants waiting time by 1000%, reduced staff turnover by 60%, lifted customer satisfaction by over 52%, increased revenues by 400%, and cutting 300% of overheads. Due to the substantial size and details of the work conducted in the organisation, the discussion in this article was limited to the process re-engineering project performed part of the overall change program, as the next section details.

5. THE PROCESS RE-ENGINEERING PROJECT

As explained earlier that biggest motive for business process reengineering stemming from key challenges faced by the organization in achieving its objective of enrolling all citizens and residents into the UAE Federal government's "Population Register" program. Key drivers for these challenges were limited daily intake capacity, complex enrollment processes and lack of robust mechanisms to ensure a regular flow of enrollment applications. Hence and once leadership decided that a radical change was needed, it was clear that an enrollment process re-engineering was required. Prior to kicking off the re-engineering project, the team leading the project reviewed leaderships guiding principles for deploying the change process. The four guiding principles mandated by leadership were:

1. Increased efficiency,
2. Cost optimization,
3. Incremental capacity, and
4. Enhanced customer experience.

These guiding principles thus become the pillars on which the future population enrollment strategy needed to be built on. So, in order to deliver upon each of these guiding principles, the management team studied various options and revamped the end-to-end enrollment process with a specific focus on elimination of bottlenecks and redundant processes. The following subsections will outline key changes implemented addressing each of the guiding principles.

5.1 Increased efficiency

The registration process was the obvious reengineering opportunity. Much time was devoted to assessing risks and benefits of various design alternatives. The most important consideration was that the new system needed to be customer centric and driven by customer needs of faster and more convenient registration process. Common complaints from people previously were that of going through long, cumbersome and highly time consuming procedures at registration centres. Accordingly, the new redesigned process yielded the following outcomes:

- Reduction of enrollment processes from a 6 step to a 4 step process, and

- Standardization of biometrics capture technology from maximum of 3 unit workstations to a standard 1 unit workstation (See also Fig. 1).

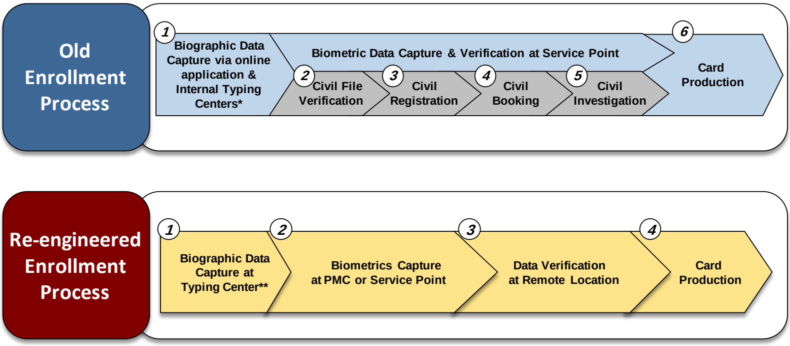

Old Enrollment Process
1
Biographic Data Capture via online application & Internal Typing Centers*
Biometric Data Capture & Verification at Service Point
2
Civil File Verification
3
Civil Registration
4
Civil Booking
5
Civil Investigation
6
Card Production
Re-engineered Enrollment Process
1
Biographic Data Capture at Typing Center**
2
Biometrics Capture at PMC or Service Point
3
Data Verification at Remote Location
4
Card Production

Fig. 1. Old registration process vs new process.

As a result of the above change, the average theoretical time for enrolling each applicant was reduced by 23 minutes per application. Key drivers for this change were a 10 minute reduction in average time to fill-out an ID card application and a 13 minute reduction in average time for biometrics capture and data verification.

A key consideration in making the time comparison between old versus new process was that in the past applicants completed their ID card applications online and in the new design, they would pay to have an application completed for them by an authorized typing center.

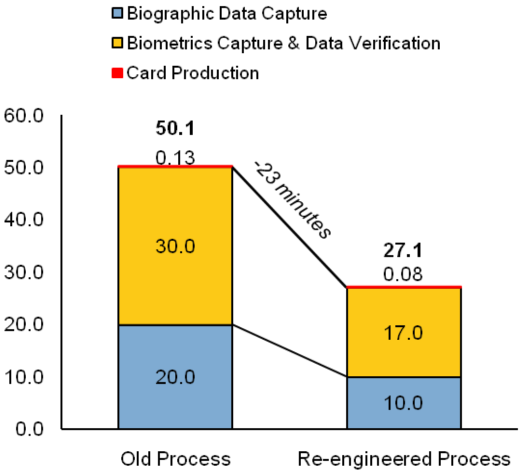


Fig. 2. Time savings in new process.

5.2 Cost Optimization

- Shorter processing time per application leading to higher utilization rate and hence increased productivity of enrollment workstation operators.

As a result of the above change, average theoretical overhead (labour) for biometrics capture and data verification was reduced by 30 AED per application. Key drivers for this change was the hypothesis that existing staff would be utilized for biometrics capture and data verification processes. The implications of the above hypothesis was that the average labour cost associated with each workstation operators would remain unchanged at an average cost of 22,000 per month; however each employee would be able to process a greater numbers of applications per day given the 23 minute reduction in lead time. In addition typing centers and outsourcing costs were excluded in order to produce an assessment purely focused on process re-engineering.

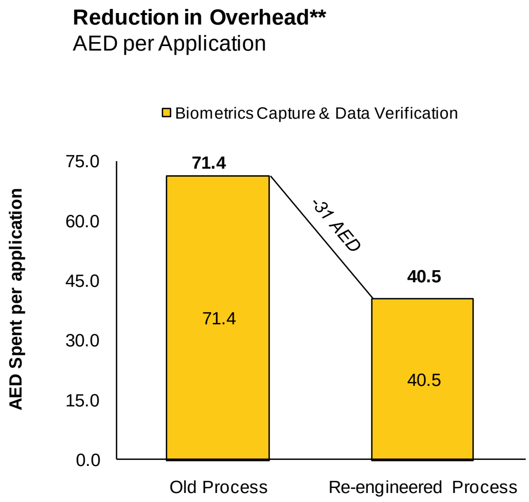


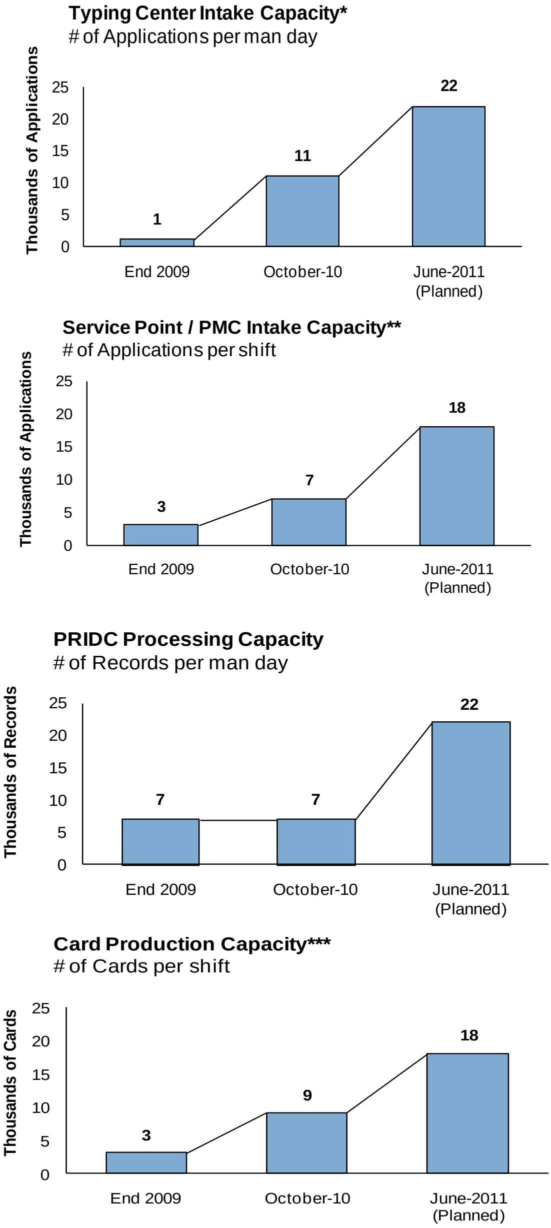
Fig. 3. Cost savings with reengineering.

5.3 Incremental Capacity

- Achievement of incremental capacity in biographic capture, biometrics capture and card production processes as of Q3 2010, and

- Additional increases in biographic capture, biometrics capture. Population register processing capabilities and card production processes planned by Q3 2011.

As a result of deploying increased capacity across sub steps of the enrollment process, Emirates ID had the potential of raising end to end daily enrollment throughput to approximately 22,000 applications per day by Q3, 2011.



Typing Center Intake Capacity*
# of Applications per man day

Service Point / PMC Intake Capacity**
# of Applications per shift

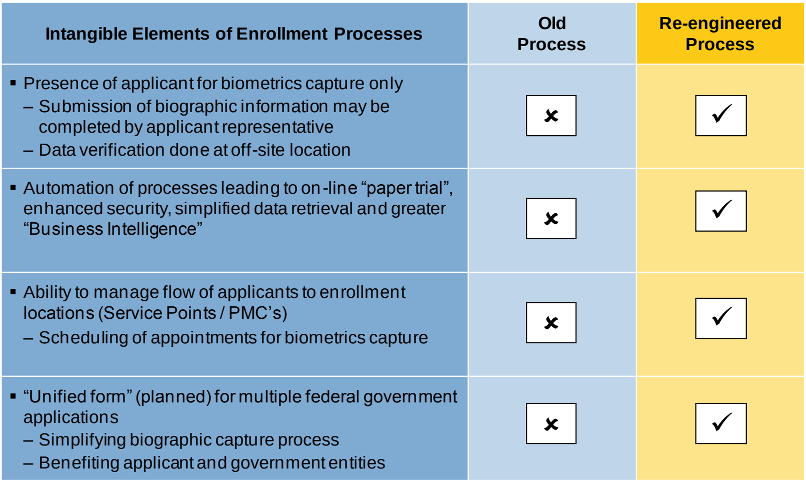
PRIDC Processing Capacity
# of Records per man day

Card Production Capacity***
# of Cards per shift

Fig. 4. Capacity development.

5.4 Enhanced Customer Experience

In addition to the tangible elements quantified in earlier sections, there were also a number of intangible enhancements that greatly benefit both Emirates ID and its customers. Some of these are mentioned in the diagram below:

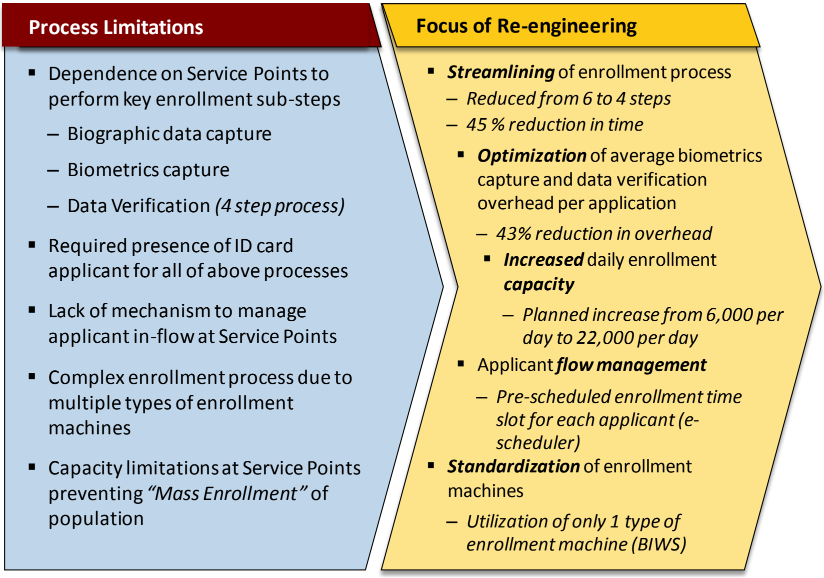


Intangible Elements of Enrollment Processes	Old Process	Re-engineered Process
▪ Presence of applicant for biometrics capture only – Submission of biographic information may be completed by applicant representative – Data verification done at off-site location	☒	☑
▪ Automation of processes leading to on-line "paper trial", enhanced security, simplified data retrieval and greater "Business Intelligence"	☒	☑
▪ Ability to manage flow of applicants to enrollment locations (Service Points / PMC's) – Scheduling of appointments for biometrics capture	☒	☑
▪ "Unified form" (planned) for multiple federal government applications – Simplifying biographic capture process – Benefiting applicant and government entities	☒	☑

Fig. 5. Customer service enhancement areas.

6. KEY RESULTS FROM PROCESS REENGINEERING

Once the entire process re-engineering program was completed, Emirates ID was expected to deliver on each of the four guiding principles outlined by leadership listed earlier.



Process Limitations

- Dependence on Service Points to perform key enrollment sub-steps
  - Biographic data capture
  - Biometrics capture
  - Data Verification *(4 step process)*
- Required presence of ID card applicant for all of above processes
- Lack of mechanism to manage applicant in-flow at Service Points
- Complex enrollment process due to multiple types of enrollment machines
- Capacity limitations at Service Points preventing *"Mass Enrollment"* of population

Focus of Re-engineering

- ***Streamlining*** of enrollment process
  - *Reduced from 6 to 4 steps*
  - *45 % reduction in time*
- ***Optimization*** of average biometrics capture and data verification overhead per application
  - *43% reduction in overhead*
- ***Increased*** daily enrollment ***capacity***
  - *Planned increase from 6,000 per day to 22,000 per day*
- Applicant ***flow management***
  - *Pre-scheduled enrollment time slot for each applicant (e-scheduler)*
- ***Standardization*** of enrollment machines
  - *Utilization of only 1 type of enrollment machine (BIWS)*

** Does not account for cost of 3rd party contracts which were not part of original re-engineering project*

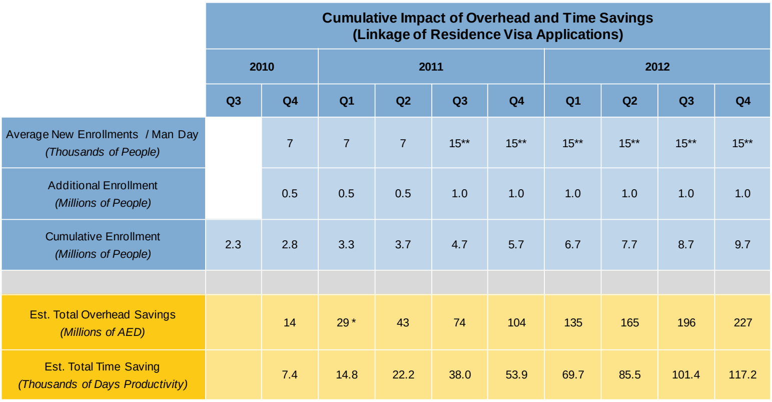
*** based on deployment of ~400 BIWS machines currently in inventory (including converted machines)*

Fig. 6. Key results from reengineering.

Having done so, not only Emirates ID was prepared to deploy its Mass Enrollment strategy, it was also able to reap the benefits of cost and time savings per applicant enrolled. A high level study of cost and time savings based on potential future scenarios led to the following results.

6.1 Scenario 1: Linkage of Residence Visa Applications

The first scenario extrapolated cost and time savings based on linkage of all residence visa applications to the Emirates ID card. If such a linkage were activated across the UAE at the beginning of Q3 2011, Emirates ID was expected to have a constant flow of 15,000 applications per day. Extrapolating this enrolment forecast through the end of 2012 reveals that at that point in time, Emirates ID would have enrolled over 9 million people in its Population Register, and in doing so would save approximately 227 million AED in labour cost and over 117,000 man hours.



	Cumulative Impact of Overhead and Time Savings (Linkage of Residence Visa Applications)									
	2010		2011				2012			
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Average New Enrollments / Man Day *(Thousands of People)*		7	7	7	15**	15**	15**	15**	15**	15**
Additional Enrollment *(Millions of People)*		0.5	0.5	0.5	1.0	1.0	1.0	1.0	1.0	1.0
Cumulative Enrollment *(Millions of People)*	2.3	2.8	3.3	3.7	4.7	5.7	6.7	7.7	8.7	9.7
Est. Total Overhead Savings *(Millions of AED)*		14	29 *	43	74	104	135	165	196	227
Est. Total Time Saving *(Thousands of Days Productivity)*		7.4	14.8	22.2	38.0	53.9	69.7	85.5	101.4	117.2

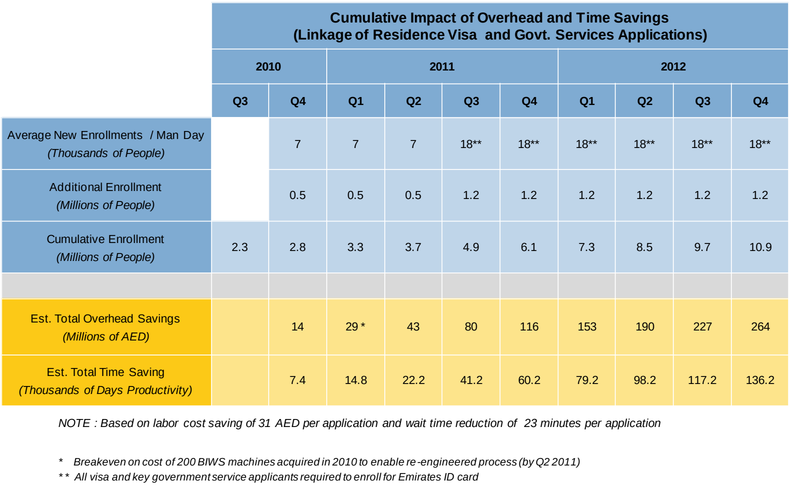
NOTE : Based on labor cost saving of 31 AED per application and wait time reduction of 23 minutes per application

* *Breakeven on cost of 200 BIWS machines acquired in 2010 to enable re-engineered process (by Q2 2011)*
** *All visa applicants required to enroll for Emirates ID card*

Fig. 7. ROI scenario 1.

6.2 Scenario 2: Linkage of Residence Visa Applications & Key Govt. Services

The second scenario extrapolated cost and time savings based on linkage of all residence visa applications plus key government services (e.g. driver's license, vehicle registrations, etc.) to the Emirates ID card. If such a linkage were activated across the UAE at the beginning of Q3 2011, Emirates ID was expected to have a constant flow of 18,000 applications / day. Extrapolating this enrolment forecast through the end of 2012 reveals that at that point in time Emirates ID would have enrolled over 10 million people in its Population Register, and in doing so would save approximately 265 million AED in labour cost and over 136,000 man hours.



	Cumulative Impact of Overhead and Time Savings (Linkage of Residence Visa and Govt. Services Applications)									
	2010		2011				2012			
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Average New Enrollments / Man Day *(Thousands of People)*		7	7	7	18**	18**	18**	18**	18**	18**
Additional Enrollment *(Millions of People)*		0.5	0.5	0.5	1.2	1.2	1.2	1.2	1.2	1.2
Cumulative Enrollment *(Millions of People)*	2.3	2.8	3.3	3.7	4.9	6.1	7.3	8.5	9.7	10.9
Est. Total Overhead Savings *(Millions of AED)*		14	29 *	43	80	116	153	190	227	264
Est. Total Time Saving *(Thousands of Days Productivity)*		7.4	14.8	22.2	41.2	60.2	79.2	98.2	117.2	136.2

NOTE : Based on labor cost saving of 31 AED per application and wait time reduction of 23 minutes per application

* *Breakeven on cost of 200 BIWS machines acquired in 2010 to enable re-engineered process (by Q2 2011)*
** *All visa and key government service applicants required to enroll for Emirates ID card*

Fig. 7: ROI scenario 2

7. LESSONS LEARNED

This section presents some of the most prominent lessons learned and consideration areas that played key roles in facilitating the overall project management.

7.1 Leadership and Commitment

The literature has recognized the critical role of leadership in BPR initiatives. Hammer and Champy (1993; 2003) state that most reengineering failures stem from the "breakdowns in leadership". Leadership role is seen to create a sense of mission among organizational members (Carr & Johansson, 1995; Hammer & Champy, 1993). Caron et al. (1994, p. 247) have also observed that for successful radical change, members of the senior management must be committed to the initiative, and must demonstrate their commitment "by being visibly involved with the project". See also (Gadd and Oakland, 1996; Barrett, 1994; O'Neill & Sohal, 1998).

The significant outcomes of the reengineering initiative at Emirates ID were the results of strong commitment from the Vice-Chairman, and persistent result focused top management. Business process improvement must be aligned with business objectives and clear set of outcomes. Successful implementation of change programs comes with a vision and a plan and an aggressive execution of that plan. Delegation and empowerment of teams is necessary to crease sense of responsibility of the work to be completed in such plans. This should facilitate the creation of the culture for ownership and accountability.

Cyert and March (1992), among others, point out that conflict is often a driving force in organizational behaviour. BPR claims to stress teamwork, yet paradoxically, it must be "driven" by a leader who is prepared to be ruthless. This is why top management macro and micro involvement during the execution is essential to guide and re-unite individuals and departments as conflicts would normally arise.

7.2 Information Technology is not a target on its own

Despite the findings of hundreds of studies which indicated it as one of the major failure reasons of initiatives, some management teams have the tendency to focus on Information Technology as a primary enabler to business needs and requirements. Top management focus to this area is crucial, as they would need to intervene at different stages to re-communicate objectives and get everybody on the same page and ensure compliance with business objectives.

Hammer and Champy (1993) suggest that organizations think 'inductively' about information technology. Induction is the process of reasoning from the specific to the general which means that manager must 'learn' the power of new technologies and 'think' of innovative ways to alter the way work is done. This is contrary to deductive thinking where problems are first identified and solutions are then formulated. A practical approach in this area is to systematically benchmark and evaluate best practices, using relevant organizations, and consider the extent to which the processes need redesigning.

7.3 Getting everybody on the same page

It was difficult times to push both second and third line management teams to shift from their comfort zones and the traditional way of doing work, to think of their departments and units as components of a larger production line where performance evaluation would be based on how the entire product line is performed. There was great tendency by them to focus on their own business functions in silo environments.

The radical process reengineering introduced in the organisation required the breaking down of functional and individual job boundaries as the new processes did not have to coincide with the existing departmental structure. Internal departments were expected to be more supportive of each other and share information and best practices.

Through lots of trial and error management approaches to improve teams performance, management teams and thereafter all other employees began to realize and feel the need for change and adaptation to the new status quo. The higher management team in the organisation was needed to adopt a culture of empowerment and learning.

We map this to the story of the five blind men who attempted to define an elephant as depicted in Fig. 8. One man grabbed an ear, another the trunk, a third the tail, the fourth a leg, and the last touched the side. The man who touches the leg concludes that an elephant is thick and round and much like a column or pillar.

Another man puts his hand on the trunk and concludes that an elephant is slender and flexible and must be something like a snake. The last man pushes on the elephant's side and determines that it is broad and unmovable like a large wall.

Obviously what the diagram is showing here that there is no shortage of perspectives one could develop. The moral of the story is that everything is relative. Each of the blind men told the truth based on their experience with the elephant, but no one man's truth could exclude another's. No truth took precedence, even in the face of completely opposite claims.

Fig. 8. Blind men and an Elephant.

This lesson is critically important for management to comprehend when introducing change in their orgnaisations. Individuals at many instances were found to work and focus on their own work within a functional area of the organization.

Unless they see and comprehend that their work is part of a larger system, it would be very much challenging to get and keep everybody on the same page. For business process reengineering to succeed, lots of training and on job coaching was required to psychologically shift their mindset to the new status quo.

One improvement that helped teams to work more homogeneously was the change of work environments where all support departments were moved to a single and larger facility that facilitated improved communication between them. The second improvement was the result of the new reengineered layouts of the registration centers. The layout was radically redesigned to better suit the new registration process flow and enabled more transparency due to the glass-partition-walls of management offices and the open space layout. This also contributed to improving customer service and satisfaction.

7.4 People and Performance Management

Perhaps one of the most important success factors for any change program is the people element. It is important that top management make tuning decisions to create the space for change. If an organization wishes to change the way it operates, it must turn to its people to make it happen. People are the agents of change. Creating business plans and strategies are important, but they are only tools to guide the actions of people.

This should pave the way for the implementation of performance-based evaluation. The shift to performance based evaluation, management empowerment, reward for creativity, and a system-view; all helped Emirates ID to enormously improve its quality and performance for its customers. The adoption of continuous improvement philosophy led to the development of a solid proactive work environment that puts customer satisfaction and operational effectiveness and efficiency at the top of the organizational priorities.

It is important for an organisation operating in the public sector to continuously revisit its defined vision and mission to revive organisational mindset of where the organization is going, and to provide a clear picture of the desired future position. Producing key performance measures to track progress should be based on that.

Management need to develop a culture for constant improvement and Identification of initiatives that will recuperate performance. Such performance management activities need to be placed in a feedback loop, complete with measurements and planning linked in Deming cycle of "Plan - Do - Check - Act", also known as the Control Circle, or PDCA. See also Fig. 9.

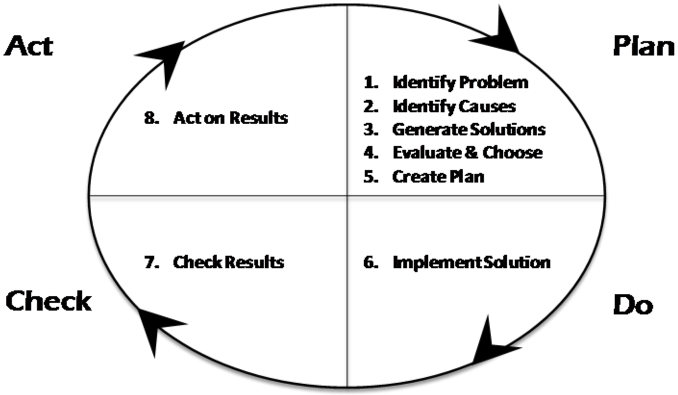


Fig 9. Deming control cycle.

7.5 BPR and TQM: A State of Confusion in Practice

In practice we observe organisations to have mixed or improper definitions for the application of BPR and TQM. TQM as defined in the literature is a strategic approach that is based on the premise of continuous improvement which puts emphasis on the identification of methods to continuously improve customer satisfaction, product quality, or customer service (Evans, 2004; George, 1998; Kemp, 2005).

BPR on the other hand is concerned with the reorganization of the complete process cycle in major parts of the organization to eliminate unnecessary procedures, achieve synergies between previously separated processes, and become more responsive to future changes (Coulson-Thomas, 1993; Davenport, 1993). Both TQM and BPR assume that in order to provide better products and services, organizations must improve business processes.

TQM is more of a systematic approach to improving business processes through a philosophy of continuous improvement resulting in an upward sloping line of linear process improvements. BPR is not about tweaking existing processes but rather combines a strategy of promoting business innovation with radical change in business processes to achieve breakthrough improvements in products and services. See also Fig. 10 below.

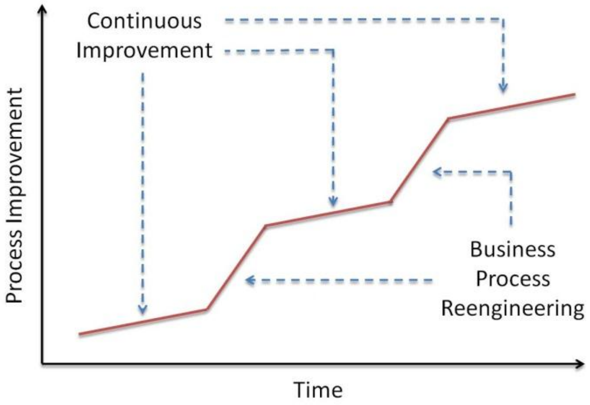


Fig. 10. TQM vs BPR. Adopted from: Hoffer et al. (2011)

It was needed that management teams to distinguish between these approaches. Unlike TQM, for instance, that aims on smoothly and incremental improvements, BPR aims on dramatic and rapid results and is suited for organisations facing gargantuan challenges to optimize the workflow and productivity. TQM targets to improve the existing systems. BPR on the other hand takes an opposite assumption as it is concerned with frame-braking change that attempts to create new systems rather than repairing old systems. BPR puts much emphasis on the enabling role of information technology and pays less attention to documentation. Table 1 provides further details about the differences between each of the two approaches.

Table 1: Comparison BPR and TQM

	BPR	TQM
Description:	Particular approach concerned with rethinking current systems and processes.	Concerned with improving work processes and methods in order to maximise the quality of goods and services.
Type of Change:	Planned, frame-braking	Planned, continuous
Aim:	To redefine existing work methods and processes to improve efficiency.	Keep existing customers by meeting or exceeding their expectations concerning products and services.
Key Driver:	Competitive pressures and intense need to cut costs.	Increasingly competitive market and the need to compete for specific customer demands. May also be driven by specific problems such as high costs or poor quality.
Change Agent:	External consultant	External or internal
Learning process:	Double loop	Single or double loop
Nature of culture change:	Values objectivity, control, consistency and hierarchy	Customer focused values
Change to team based work:	Yes. Requires a shift to team based work because the work is process based rather than task based.	Often requires a shift to team based work

Source: Millett & Harvey, 1999

7.6 Creating Sense of Agility

Agility in public sector context is the ability of an organization to be dynamic in rapidly changing and continually fragmenting operating environments for high quality, high performance, and customer configured service models. Organisations in such environments are needed to develop information capabilities to treat masses of population as individuals and services that are perceived as solutions to their individual needs and requirements.

This should help addressing the requirements of different and constantly changing customer opportunities. Goldsmith & Eggers (2004) indicate that the traditional, hierarchical model of governments simply does not meet the demands of the complex, rapidly changing era we live in, and suggests that the public sector requires agility in its systems, structures and processes. Fig. 11 depicts some pressuring elements pushing public sector organisations to adopt more agile approaches to address such requirements.

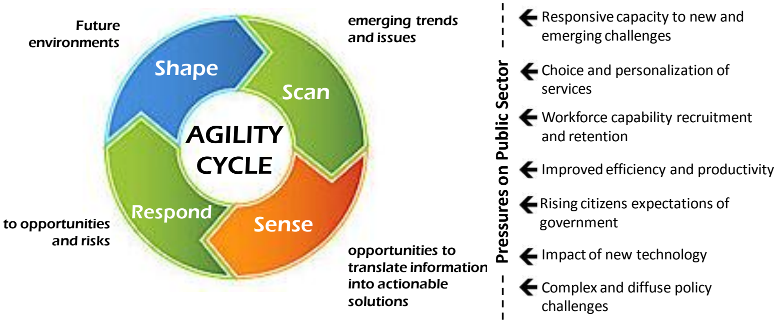

Future environments
emerging trends and issues
Shape
Scan
AGILITY CYCLE
Respond
Sense
to opportunities and risks
opportunities to translate information into actionable solutions
Pressures on Public Sector
Responsive capacity to new and emerging challenges
Choice and personalization of services
Workforce capability recruitment and retention
Improved efficiency and productivity
Rising citizens expectations of government
Impact of new technology
Complex and diffuse policy challenges

Fig. 11. Need for agility in public sector organizations.

In simple terms, we relate agility in organisations to adaptability and speed. During the BPR project, it was important to develop deep management understanding of various priority elements critical to the success of the overall project such as the organisational structure, jobs definitions, and evaluation and reward systems.

This needed to be followed by an understanding of the organisation's talent and capabilities, and creating an organisational culture that supports redeployments and re-skilling. With strong and visible leadership, the organisations needed to focus on building a unified organisation that defeats silos, and developing capabilities to manage internal change well. The work presented herein attempted to add to the limited body of knowledge of practices in the field and an experience to share and build upon.

CONCLUSION

National Identity programs around the world have been going through a number of challenges. The most obvious challenge these programs face is seen to be with the quality of the enrolment process in terms of its effectiveness and efficiency of adopted processes. This study recognises the importance of this critical field, and aimed to improve overall understanding and addressing government needs for higher quality and more citizen-focused services in national ID programs.

By implementing and examining the BPR project at Emirates ID, this study provides guidelines for BPR projects in national identity initiatives with a similar context. The business process reengineering at Emirates ID resulted in substantial business benefits and contributed to the simplification of the work of the employees at front lines, increasing the degree of transparency and accuracy in functioning of the enrolment process at registration centers, and most importantly improved overall customer experience and satisfaction.

While there are similarities in how governments may approach reengineering, each government should tailor its BPR efforts to satisfy its unique conditions and operating environment (Kettinger et al., 1997). We reiterate that managing a reengineering initiative is extremely complex and difficult, and there is (and can be) no guaranteed path to success (Sauer et al., 1997; Galliers & Baets, 1998).

Although the major limitation of this research is the sample size that limits generalisability, the study is rated high on its data richness, and appropriateness for such dynamic area of practice. National Identity schemes all over the world require going through almost the same procedures with only differences related to the choice of biometric technologies adopted in each country. The lessons learned documented in this article provide practical considerations for management in the field. They are considered important building blocks for the BPR exercise to succeed.

REFERENCES

[1] Alavi, M. and Carlson, P. "A review of MIS research and disciplinary development," Journal of Management Information Systems (8:4), 1992, pp. 45-62.

[2] Alkhouri, A.M. (2007). UAE National ID Program Case Study. International Journal Of Social Sciences, Vol. 1, No. 2, pp.62-69.

[3] Alkhouri, A.M. (2010) Facing the Challenge of Enrolment in ID Card Programs. 'The Biometric Landscape in Europe', Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, BIOSIG 2010, Darmstadt, Germany, September 09 -10, 2010.

[4] Barrett, J.L., 1994. Process visualization: Getting the vision right is the key. Information Systems Management 11 (2), 14–23.

[5] Benbasat, I., Goldstein, D.K. and Mead, M. "The Case Research Strategy in Studies of Information Systems," MIS Quarterly (11:3) 1987, pp. 369-386.

[6] Caron, M., Jarvenpaa, S.L. & Stoddard, D.B. (1994, September). "Business Reengineering at CIGNA Corporation: Experiences and Lessons Learned From the First Five Years,"MIS Quarterly, pp. 233-250.

[7] Carr, D., Johansson, H., 1995. Best Practices in Reengineering. McGraw-Hill, New York.

[8] Coulson-Thomas, C.J., 1993. Corporate transformation and business process engineering. Executive Development 6 (1), 14–20.

[9] Cyert, R. M. and J. G. March (1992), A Behavioral Theory of the Firm, Oxford: Blackwell.

[10] Davenport, T.H. & Beers, M.C. (1995). "Managing Information About Processes," Journal of Management Information Systems, 12(1), pp. 57-80.

[11] Davenport, T.H. & Short, J.E. (1990 Summer). "The New Industrial Engineering: Information Technology and Business Process Redesign," Sloan Management Review, pp. 11-27.

[12] Davenport, T.H. Process Innovation: Reengineering work through Information Technology. Boston: Harvard Business School Press, 1993.

[13] Davidson, W. (1993), ``Beyond re-engineering: the three phases of business transformation'', IBM Systems Journal, Vol. 32 No. 1, Winter, pp. 65-79.

[14] Dunleavy, P., Margetts, H., Bastow, S. and Tinkler, J. (2006) New Public Management Is Dead--Long Live Digital-Era Governance. Journal of Public Administration Research and Theory 16 (3) 467-494.

[15] Earl, M., Khan, B., 1994. How new is business process redesign. European Management Journal 12 (1), 20–30.

[16] Earl, M.J., Sampler, J.L. & Short, J.E. (1995). "Strategies for Business Process Reengineering: Evidence from Field Studies," Journal of Management Information Systems, 12(1), pp. 31-56.

[17] Evans, J.R. (2004) Total Quality: Management, Organization and Strategy. South-Western College Pub.

[18] Gadd, K., Oakland, J., 1996. Chimera or culture? Business process re-engineering for total quality management. Quality Management Journal 3 (3), 20–38.

[19] Galliers, R.D., Baets, W.R.J., 1998. Information Technology and Organizational Transformation. Innovation for the 21st Century Organization. Wiley, New York.

[20] George, S. (1998) Total Quality Management: Strategies and Techniques Proven at Today's Most Successful Companies. Wiley.

[21] Goldsmith, S. & Eggers, W.D. (2004) Governing by Network: The New Shape of the Public Sector. Washington DC: Brookings Institution Press.

[22] Gordon, G.J. and Milakovich, M.E. (2009) Public Administration in America, 10 edition. Wadsworth Cengage Learning, USA.

[23] Hammer, M. and Champy, J. (1993) Reengineering the Corporation: A Manifesto for Business Revolution. New York: HarperCollins.

[24] Hammer, M. and Champy, J. (2003) Reengineering the Corporation: A Manifesto for Business Revolution. HarperCollins Publishers, NY.

[25] Hoffer J.A, George J.F, Valacich J.S (2011) Modern Systems Analysis and Design. Sixth Edition. Prentice Hall: New Jersy.

[26] Jeston, J. and Nelis, J. (2008) Business Process Management: Practical Guidelines to Successful Implementations. Second Edition. UK: Butterworth-Heinemann.

[27] Keen, P.G.W. Shaping the Future: Business Design through Information Techology. Boston: Harvard Business School Press, 1991.

[28] Kemp, S. (2005) Quality Management Demystified. McGraw-Hill Professional.

[29] Kettinger, W.J. & Grover, V. (1995). "Special Section: Toward a Theory of Business Process Change Management," Journal of Management Information Systems, 12(1), pp. 9-30.

[30] Kettinger, W.J. & Grover, V. (1995). "Special Section: Toward a Theory of Business Process Change Management," Journal of Management Information Systems, 12(1), pp. 9-30.

[31] Leedy, P. D., & Ormrod, J. E. (2005). Practical research: Planning and design (8th ed.). Upper Saddle River, NJ: Prentice Hall.

[32] Lloyd, Tom, Giant with Feet of Clay/ Tom Lloyd Offers a Contrasting View of Business Process Reengineering, Financial Times, December 5, 1994; Pg. 8.

[33] Lowenthal, J.N., 1994. Reengineering the Organization; A Step-By-Step Approach to Corporate Revitalization. ASQC Quality Press,Milwaukee, USA.

[34] Madison, D. (2005) Process Mapping, Process Improvement and Process Management. Paton Press.

[35] Millett, B. and Harvey, S. (1999) OD, TQM AND BPR: A COMPARATIVE APPROACH. Australian Journal of Management & Organisational Behaviour, 2(3), 30-42.

[36] O’Neill, P., Sohal, A., 1998. Business process reengineering: application and success—an Australian study. International Journal of Operations and Production Management 18 (9–10), 832–864.

[37] Orlikowski, W.J. & Baroudi, J.J. "Studying Information Technology in Organizations: Research Approaches and Assumptions", Information Systems Research (2) 1991, pp. 1-28.

[38] Porter, M.E., 1980. Competitive Strategy. Free Press, New York.

[39] Porter, M.E., 1985. Competitive Advantage. Free Press, New York.

[40] Porter, M.E., 1990. The competitive advantage of nations. Harvard Business Review 68 (2), 73–92.

[41] Sauer, C., Yetton, P.W. and associates, 1997. Steps to the Future. Fresh Thinking on the Management of IT-Based Organizational Transformation. Jossey-Bass, San Francisco, CA.

[42] Talwar, R., 1993. Business re-engineering—A strategy-driven approach. Long Range Planning 26 (6), 22–40.

[43] Yin, R. K. Case Study Research, Design and Methods, 3rd ed. Newbury Park, Sage Publications, 2002.

Targeting Results:

Lessons Learned from UAE National ID Program [36]

DR. ALI M. AL-KHOURI

ABSTRACT: Many governments around the world have invested inestimably in modernizing their identity management systems to enable more complex and secure forms of identification. However, these programs have been challenged to achieve their desired targets due to several factors; political, organizational, technical, etc. This article presents the strategy adopted in one of the major programs in the Middle East region launched in 2003, and key challenges that were identified and addressed during the course of implementation to achieve its strategic objectives. It also presents some key management consideration areas for the purpose of sharing knowledge and experience in the field.

Key words:

[36] Al-Khouri, A.M. (2012) "Targeting Results: Lessons Learned from UAE National ID Program", **Global Journal of Computer Application and Technology**, Vol. 2, No. 1, pp. 830-836 .

1. INTRODUCTION

GOVERNMENTS around the world have been very much attracted to modern identity management systems; more specifically national ID programs [1]. These programs are globally justified on the basis of building an identity management system to achieve primarily two objectives: support national security and improve access to services [2]. More than 30 countries have initiated smart ID card programs in the last decade with a total value of those projects exceeding $100 billion. In fact, India has launched recently its project with a total value of around $33.5 billion. Besides, more than 15 countries are in the process of upgrading their current ID cards to biometric based systems such as Canada, Australia, New Zealand, USA, etc.

GCC countries have been among the first countries to launch biometric based smart ID card initiatives. Due to nature and complexity of such schemes, these initiatives have been challenged to meet its specified projects scope, timelines, and budgets [3]. Our observations of national ID card programs overall show that many countries are struggling with the enrolment of population in their ID schemes. Apart from the technical complexity of such projects, the most significant challenge lies in the fact that these programs include biometric acquisition which entails the presence of individuals. Some countries capture only two fingerprints, others capture a full set of fingerprints including palm prints and writers, while others use a variety of biometric identification systems such facial, iris, and fingerprints.

The practice of biometric acquisition was previously limited to forensic and traditional law enforcement applications. For obvious reasons, developments of systems like fingerprints compared to other biometric systems and hence the maturity of the overall technology, did not take into consideration higher levels of customer or service satisfaction since the intended users were in forensic and police jurisdictions. Therefore, and based on the biometrics and verification procedures, the registration process can be time consuming and inconvenient.

A well thought through enrolment plan that captures an understanding of population demographics and cultural elements, and follows a modular approach of gradual registration based on geographical distribution and other segmentation factors, is likely to yield more successful results. This article presents a case study of the process followed to develop an enrolment plan to register the population of the United Arab Emirates. It touches upon a broader organizational scope, and presents essential lessons learned and important building blocks for government officials working in this field. Though the project size and targeted population is considered relatively small in comparison to other countries, the presented processes and overall thoughts are believed to contribute and advance existing knowledge.

2. UAE NATIONAL ID PROGRAM

The UAE national ID program was launched in 2003 to build a federal identity management system for the country. The government relied primarily on a social marketing strategy to enroll the population and its copious developed strategies only succeeded to enroll less than 20% of the total population over a 5 year period. This represented a challenge to overcome and a difficulty to justify the heavy budget expenses and no clear return on investment (ROI) upshots. Altogether, this forced the government to go through muscular change process to address this problem area.

A four-staged change process was developed to guide the change implementation, as depicted in Figure 1 below. The change process was instigated to enact an organizational mindset change with the aim of developing a service driven and result oriented organization. It also aimed to increase accountability, improve efficiency, overall performance and high quality services.

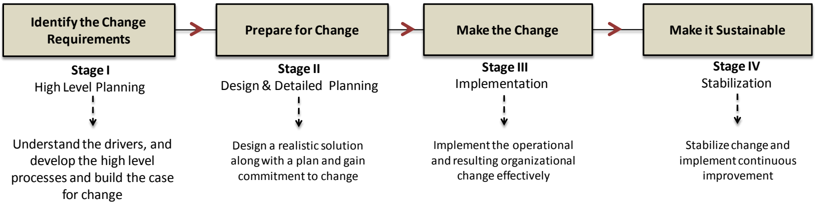

Identify the Change Requirements
Stage I
High Level Planning
Understand the drivers, and develop the high level processes and build the case for change
Prepare for Change
Stage II
Design & Detailed Planning
Design a realistic solution along with a plan and gain commitment to change
Make the Change
Stage III
Implementation
Implement the operational and resulting organizational change effectively
Make it Sustainable
Stage IV
Stabilization
Stabilize change and implement continuous improvement

Figure 1: Change management program components

The initial phase of the change process dealt with the identification of the change requirements and building the overall case for change. The second phase was more of a planning phase, and included detailed assessment of the impact of change to the overall program. The third phase was about implementing the change according to the plan, and the fourth was more of an improvement and sustainability stage. The outcome of the first phase was the development of an operating model that captured the fundamental and evolving functions of the program. It provided the foundation and flexibility required to execute the program initiatives. As depicted in Figure 2, the primary function that needed to be addressed at first was population enrolment. As the project progresses, the function of enrolment will shrink down to become less than 20% of the overall operation. The program role will turn gradually into a service delivery function related to authentication and identification. This model is considered to be a valuable knowledge to existing literature in the field, as it is generic and applicable to all ID card programs.

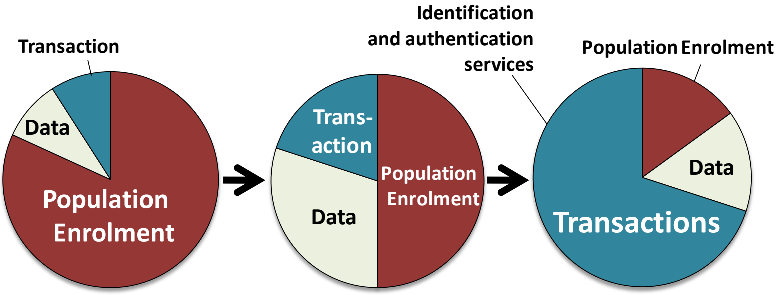
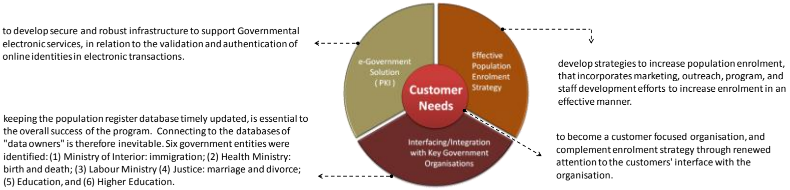


Figure 2: The operating model – shift in core operations over time

Another outcome of the first phase was the development of the core pillars of strategic directions that would determine the success of the overall program. See also Figure 3. They were later used in the development process of the corporate strategy and the design of the consequent initiatives. These pillars included:


e-Government Solution (PKI)
Effective Population Enrolment Strategy
Customer Needs
Interfacing/Integration with Key Government Organisations

to develop secure and robust infrastructure to support Governmental electronic services, in relation to the validation and authentication of online identities in electronic transactions.

keeping the population register database timely updated, is essential to the overall success of the program. Connecting to the databases of "data owners" is therefore inevitable. Six government entities were identified: (1) Ministry of Interior: immigration; (2) Health Ministry: birth and death; (3) Labour Ministry (4) Justice: marriage and divorce; (5) Education, and (6) Higher Education.

develop strategies to increase population enrolment, that incorporates marketing, outreach, program, and staff development efforts to increase enrolment in an effective manner.

to become a customer focused organisation, and complement enrolment strategy through renewed attention to the customers' interface with the organisation.

Figure 3: The core pillars of strategic directions

3. THE EMERGING ENROLMENT STRATEGY

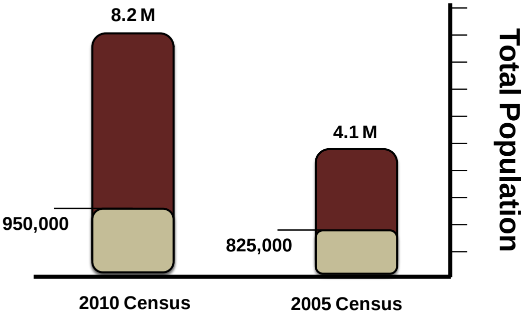


Figure 3: UAE total population

According to the original enrolment strategy, it was envisaged that a total of 5 million people will be registered by the end of 2010. However, the national census revealed that the population in the UAE has grown to over 8 million in 2010 (see also Figure 3). A study conducted to evaluate and forecast enrolment, showed that it would take more than 10 years to register the population with existing enrolment rates. Another factor that forced the development of a new enrolment strategy was the increasing financial cost to the organization and reprehensible revenues. Figure 4 shows that the cost of the card have gone up more than 30% higher than the fees paid by the applicants, as the cost of the card is dependent on specific annual registration.

This meant that for each card, the organization issued, it lost around $68. In fact, it was needed to produce 1.6 million cards a year to make the breakeven point, and as depicted in Figure 4. All together, these factors forced the organization to rethink its value proposition, and rework the overall enrolment strategy, which is discussed next.

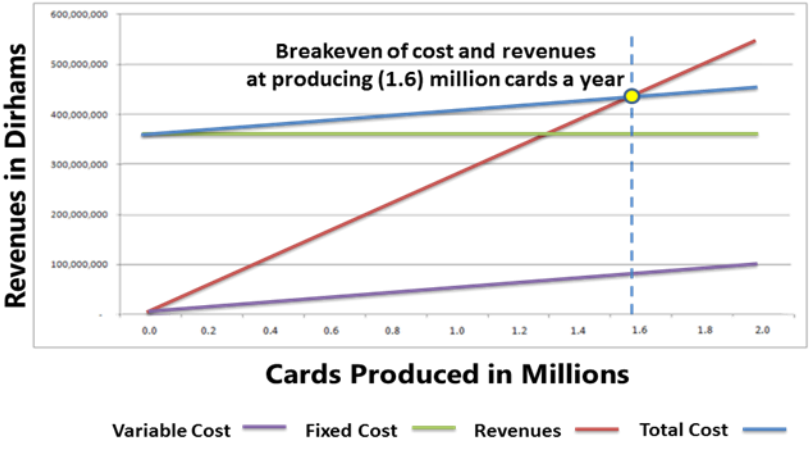


Figure 4: Cost and revenues

4. THE NEW ENROLMENT STRATEGY

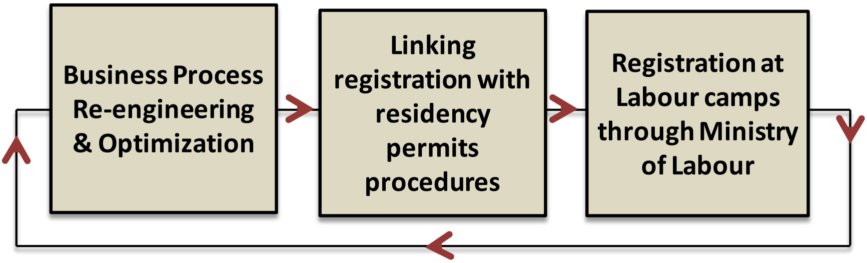

Business Process Re-engineering & Optimization
Linking registration with residency permits procedures
Registration at Labour camps through Ministry of Labour

Figure 5: Focus themes of the new enrolment strategy

As indicated earlier, the previous enrolment strategy adopted in the organization was a marketing based. The fundamental thinking that guided the development of the new enrolment strategy was to follow a process driven approach. The principles of this approach were based on the relationships between business processes that would promote public participation. The new strategy consisted of three main focus themes as depicted in Figure 5, and discussed next.

4.1 The new process: Reengineering of the enrolment process

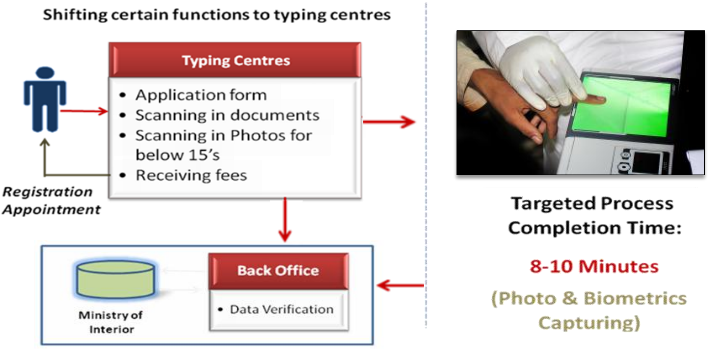


Figure 6: New registration process

The new process divided the registration into three segregated functions, see also Figure 6. More than 3000 typing centers in the government were equipped with a new application form that allowed them to key-in personal information, scan in documents, scan in photos for those below 15's, and accept payments, and automatically generate appointments to applicants.

All these functions apart from the application form were previously done at registration centers. Registration centers new role was limited to do portrait and biometric acquisition only. This implied an 8-10 minute process compared to 20 to 25 minute previously. Applicants' data is then transferred electronically to the internal data audit office (back office) which verifies the complete dossier against the Ministry of Interior's database, and authorizes or rejects applications.

The new process made more than half of the previous procedures invisible to the applicants, as they were shifted to either back end or typing centers. The new process also had a great impact on the existing registration centers layout. The new process was considered as a one stop shopping office, and allowed higher capacity in terms of enrolment rates, and space utilization.

4.2 Linking registration with immigration procedures

The second focus theme of the enrolment strategy was to link the ID registration with the issuance and renewal of residency permits. Taking into consideration that the maximum validity of residency permits is 3 years, then it was assumed that all residents will be enrolled in this timeframe given that all registration sites are operational. In order to make the process more convenient to the applicants, new registration centers were envisaged to be built near existing preventative medicine centers; responsible to issue medical fitness certificates to complete the residency procedures.

According to statistics, there were around 9,000 to 15,000 daily transactions of new and renewal of residencies in the UAE. This process merge between ID card and residency permit, was envisaged to enforce and increase the daily registration rate remarkably. It was also noted in this focus area, that the residents during their application for issuance and renewal of residency permits fill different application forms for different entities, e.g., immigration form, labor form, and ID card form.

Comparing the three forms, it was found that they were almost identical. It was then decided to merge the three forms to be a unified form for the three entities, besides the preventative medicine which also issues separate forms. This step would contribute to prevent double implementation of such procedures and promote data accuracy. The new 3+1 form will also include the feature of central fees collection for all four entities, payable at typing centers. The fees will be automatically transferred to the beneficiary authorities through an electronic clearance system.

4.2.1 Registration Process

The registration process starts with the applicant or a representative visiting the typing centre to fill the unified application form. The form will also include the new functionalities described in section (4.1). Applicants aged 15 and above will go to the preventative medicine centre for medical check up and go through the ID card registration office for portrait and biometric acquisition. Upon the acceptance of the issuance/renewal of residency permit, the immigration database at the Ministry of Interior, electronically notifies the ID card database, which will trigger card printing request, and dispatch it to the applicant through a registered courier. For the purpose of unification, ID card validity is linked with the residency permit. It is envisaged that once the process is streamlined, and reached to a satisfactory level, the residency sticker and labor card will be replaced with the ID card, as a single identity document for residents.

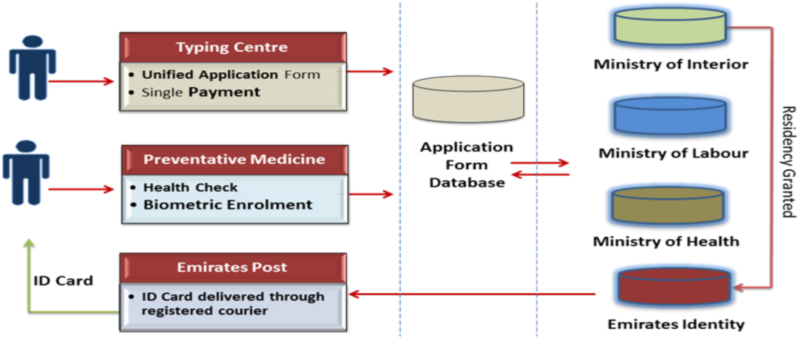


Figure 7: process of registration merged with immigration processes

4.3 Labor Registration

The third focus theme is the registration of labor population through mobile registration devices at labor campus or their workplaces. This will relax the traffic at existing registration centers. Existing statistics refer that the UAE has around two million unskilled labor population. The registration of this category was planned with the

Ministry of Labor to ensure prompt registration and enforcement through their employing companies. Statistics also show that large number of labor camps have been developed in the past five years, with average residents in those camps ranging from 5,000 to 50,000 people.

Having presented the components of the enrolment strategy, the next two sections will briefly discuss the three remaining pillars of the strategic directions presented in section 2.

5. INTEGRATION WITH KEY ORGANIZATIONS

One of the most strategic objectives of building an identity management system in the UAE was to make a central identity reference repository for the UAE government about population demographics, timely available census and statistical surveys. This database was also foreseen to provide decision makers with key data to enable informed planning decisions. Maintaining an up to date and accurate population database is considered an impossible objective without a centralized e-information infrastructure to bring different databases together into one centralized repository.

An initiative was developed called citizen data-hub that aimed to connect six key government databases together that were considered the "primary data owners". The secondary objective of this initiative was to establish dynamic and real-time links between administrative government departments across the country, thus enabling information sharing that ultimately contributes to the better administration of the country and provision of service delivery.

6. SUPPORTING E-GOVERNMENT

Development of a national population infrastructure should consist of enabling the basis for online authentication of users. It should address the overall requirements of trust, identity management and privacy and in the context of electronic governance. The federated identity management initiative was designed to facilitate implementation of e-Government services within the United Arab Emirates. This is envisaged to support advanced development of e-government specifically in areas related to e-inclusion and e-participation, as well as the end-to-end integrated government work processes.

7. CUSTOMER SERVICE ORIENTATION

Given the challenges the UAE ID card program is facing, it is confronted with key building blocks representing accelerating enrolment rates, meeting stakeholders expectations, improving quality of service, etc. The new organization thinking as explained above shifted more towards a customer driven business organization.

The aim was to positively embrace a customer focused culture, where core competencies are identified and developed to deliver value for customers. A customer service standard was developed based on guidelines specified in the International customer service institute [4]. This focus area described a management culture that emphasized centrality of the citizen or customer in the process, as well as accountability for results.

This section concluded the change management program and the developed enrolment strategy overview. The next section presents some key management consideration areas that require management attention.

8. MANAGEMENT CONSIDERATIONS

8.1 Change Management and Communication Plan

Change management as a discipline has grown tremendously over the last few years in the Gulf region. Our close interactions with government organizations in the region show us that a large number of public sector organizations used consultancy firms to develop and implement structured approach to managing change programs. Indeed, a carefully planned change management program is imperative to the overall success of any strategic endeavor.

Figure 8 shows that the success of a change program is determined by the awareness of the involved individuals or groups of the need and objectives of the change program. A change program is likely to be associated with vagueness, rumors, distrust even among those involved in the change process. Strong and consist leadership is needed to draw a clear path and set out performance and expectations of outcomes.

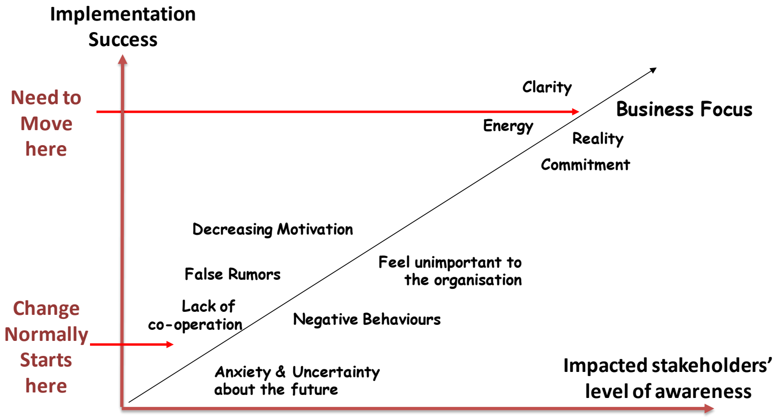


Figure 8: The need for clear communication plan

Management would prefer to implement change and expect least resistance and with the most buy-in as possible. For this to occur, change must be applied with a structured approach so that transition from one type of behavior to another organization wide will be smooth. Management need to carefully assess employees' reaction to an implemented change and attempt to understand the reaction to it.

Although change programs are implemented to achieve organizational goals and objectives, certain changes do sometimes produce tremendous amount of resistance at several operational and management levels. Management is expected to provide support throughout the process of these changes, which are at times very difficult. Managing changes especially in public sector organizations requires a broad set of skills like political, analytical, communication, people, system, and business skills.

8.2 Organizational Development Principles

Due to the enormous pressure on management to create value and bring out tangible results, it is easily found that we get distracted with day to day operations. A commendable framework management need to always keep in mind is the EFQM model (see also Figure 9). The model was found to sustain a management focus on key governance perspectives. It is a good management assessment tool to measure the strengths and improvement areas of an organization across all business operations, and to define the organization's capability and performance.

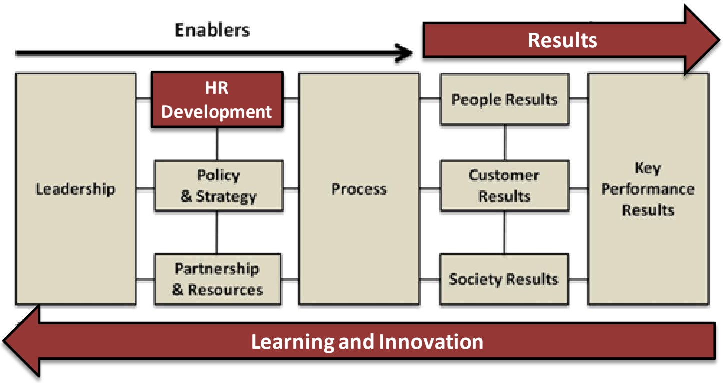


Figure 9: EFQM excellence framework

The three main elements that were considered crucial to the success of the overall organization strategy were: (1) to become a result driven organization, and focus on (2) employing and developing highly qualified and trained staff, who should enable and promote (3) creativity, innovation and learning organization culture. The framework supported management to rethink values, policies, and controls and a restructuring that reflected a renewed sense of mission.

8.3 Users training

User training is a critical success factor for. The routine nature of work at registration centers caused a shortage of workers with the necessary skills to cope with the rapid growth and expansion of centers. This shortage forced the organization to continuously hire and train new employees who lack adequate technology skills, and to accept the chore of constantly retraining present employees. In ID card schemes, fingerprint quality has huge impact on the identification/verification system. Therefore, and to meet these challenges, organizations need to develop a system to manage end-user training, and focus to enhance fingerprint capture quality.

8.4 Media and Marketing Strategy

National ID schemes have been a very much subject to controversial debate on international levels [5,9]. It is seen by privacy advocates to be a 'massive invasion' of their liberty and freedom rights, and promotes the concept of setting up 'big brother' or 'big government'. It was therefore important for the organization to develop a social media marketing strategy to better understand community interests by running customer and market surveys within the social communities, and promote engagement and social participation into the project value proposition.

The second component of the media strategy was related to building visibility about the program through information sharing and interactions. The communication strategy included specific aspects that considered the cultural diversity of the target society (eg. multiple language communication, information leaflets etc).

CONCLUSION

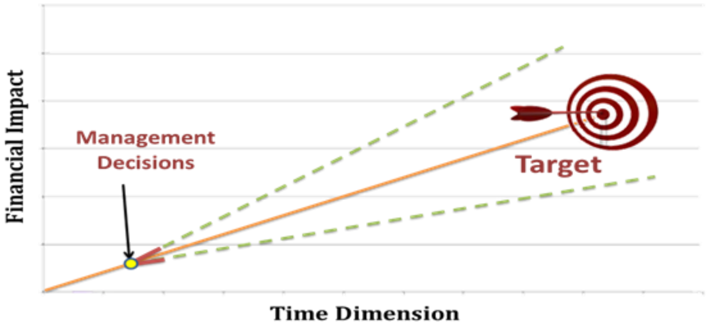


Figure 10: Impact of unfocused management decisions

Without a clear blueprint and plan, organizations are more likely to drift and run in different directions (see for example the illustration in Fig 10). Management critical decisions that are not based on solid understanding of impact and well-deliberated calculations will most probably yield to an unknown outcome [see also 10, 11].

Public sectors projects are to a great degree involve risk and uncertainty. This article was written in an attempt to reveal some of the challenges experienced in the implementation of a strategic and large scale government program. National ID schemes and due to their size and complexity need scrupulous planning to achieve their audacious goals. Population enrolment in such schemes is considered a challenging chore.

The presented case study expounded how the UAE government reacted to this challenge. Though it could be argued that population size in the UAE is lower than many other larger initiatives in other countries, the presented approach in this article is believed to provide a virtuous thinking path to address similar issues. Besides, the presented management consideration areas are assumed to be important knowledge building blocks for those in the field to address fundamental organizational and project management rudiments.

REFERENCES

[1] Lyon, D. (2009) Identifying Citizens: ID Cards as Surveillance. Cambridge: Polity Press.

[2] Al-Khouri, A.M., 2007, "UAE National ID Programme Case Study," International Journal of Social Sciences, vol. 1, no.2, pp.62-69.

[3] 6th GCC ID Cards Interoperability Committee Meeting, Riyadh, Saudi Arabia, November, 2009

[4] The International Customer Service Institute [Online] http://www.ticsi.org/.

[5] Agar, J., 2001, "Modern Horrors: British Identity and Identity Cards," in Documenting Individual Identity: The Development of State Practices in Modern World, J. Caplan & Torpey, J. (eds.), Princeton & Oxford, pp. 101-20.

[6] Lyon, D., 2006, "The border is everywhere: ID cards, surveillance and the other," in *Global Surveillance and Policing: Borders, Security, Identity*, Cullompton: Willan Publishing, pp. 66-82.

[7] Neumann, P. G. & Weinstein, L., 2001, "Risks of National Identity Cards," Communications of the ACM 44, p. 176.

[8] Barton, B., Carlton, D. and Ziehm, O., 2007, "Identity management in the 21st century: Balancing safety, security and liberty in a global environment." [Online]. IBM Global Services. USA. Available: http://www-935.ibm.com/services/us/gbs/bus/pdf/g510-7859-00-id-mgt.pdf [Accessed 14 April 2010].

[9] Greenleaf, G., 2008, "Hong Kongs Smart ID Card: Designed to be Out of Control," in *Playing the Identity Card*, Bennett, C. and Lyon D. (eds.), London: Routledge.

[10] French, S. and Liang, Y., 1993, "Decision support systems: a decision analytic perspective," in Developments in Operational Research, Norman, J. (ed.), Operational Research Society, Birmingham.

[11] Payne, J.W., Bettman, J.R. and Johnson, E.J., 1993, The adaptive decision maker." Cambridge University Press.

About Emirates Identity Authority

The Emirates Identity Authority (Emirates ID) is an independent federal government authority established by virtue of Federal Decree no. (2) issued in 2004. The decree empowered the authority to develop and implement a national country-wide identification infrastructure.

Emirates ID was established in September 29th, 2004, as a federal juridical government body. It has an independent budget and is authorized to craft its own legal frameworks to facilitate achieving its objective.

Emirates ID is mandated to develop, record and update a sophisticated state-of-art identity management system, through enrolling the entire UAE population; citizens and legal residents, and issuing them with unique identification numbers and smart cards that are linked with their biographical and biometric details.

By adopting cutting-edge and innovative technologies in running this promising national program, Emirates ID is keen to play an active and central role in supporting the development initiatives of the country. Emirates ID's contribution includes a comprehensive, accurate and highly secure population register that makes available the needed population demographical data to support decision-making and strategic planning related to resource allocation in the various areas and vital sectors. Its other strategic initiatives aim to allow the government to develop and improve existing service delivery models through advanced identity authentication capabilities.

Author Biography

HE Dr. Ali Mohamed Al-Khouri is the Director General of the Emirates Identity Authority (Emirates ID) since 2009. As Director General, Dr Al-Khouri plays a vital role in leading the Emirates ID team towards achieving the Authority's strategic goals in the development and implementation of:

1. Modern national identity management infrastructure for the government of the United Arab Emirates (UAE),
2. Infrastructure to provide timely information about population demographics to act as a strategic decision support system,
3. Infrastructure to support e-Government initiatives and digital economy, and
4. Organizational systems that adopt the highest international standards of organizational and performance excellence.

Dr. Al-Khouri was responsible for forming and leading an effective team to develop Emirates ID's strategic plan for 2010 - 2013, which included organizational restructuring and business process reengineering of key operations, thereby reducing the cost of the Authority's production line by about 70% (approximately AED 300 million) within the first two years. It also helped enhance efficiency, outputs and the quality of customer service provided by the Authority. Overall, the strategic plan was a quantum leap in terms of improving corporate governance and organisational excellence, and created a work environment that promotes innovation and excellence.

Dr. Al-Khouri had earlier served as Director of the Development Division, and member of the e-Government Committee in Abu Dhabi Police GHQ from 1990 to 2003. Thereafter, he joined the Ministry of Interior as a member of the Executive Committee for the identity infrastructure development program management.
In 2005, Dr. Al-Khouri was moved by a ministerial decree to the Emirates Identity Authority as Assistant Director General for Central Operations and Chairman of the Technical Committee for the Population Register and ID Card (PRIDC). Later, he became Chief Executive for Strategic Planning, and finally the Director General in 2009.

Dr. Al Khouri is a member of various government and professional bodies within and outside the UAE. He is board member of the UAE National Bureau of Statistics, member of the Executive Committee of the Ministry of the Interior supervising the e-Passport project in the UAE, as well as UAE representative and chairman of the technical team of the Steering Committee for the Gulf Cooperation Council (GCC) for Identity Cards and Interoperability. He is also a member of the Leadership and Management Development Association, Strategic Management Association, European Association for Biometrics, Institute of Electrical and Electronics Engineers (IEEE), International Association for Management of Technology in the US, and a member of the American centre of the Project Management Institute. Dr Al-Khouri is also a fellow of the Canadian Society of

Project Managers and Business Administration, and fellow of the British Computer Society (BCS). He was also a visiting faculty at the University of Manchester and the University of Warwick during 2004-2008.

Dr. Al-Khouri holds a Bachelor of Science in Information Technology and Business Management from the University of Manchester, UK, and a Masters in Science in Information Management from the College of Management of Sciences, University of Lancaster, UK. He is also holds an Engineering Doctorate (EngD) from the University of Warwick, UK in Engineering Management with specialisation in strategic and large scale program management in the government sector.

RECOGNITIONS

- Al Owais Award for Studies and Scientific Innovation in 2012.
- Al Owais Award for Studies and Scientific Innovation in 2008.
- Medal of Academic Excellence (1998, 1999, 2000) from the Minister of Interior.
- Medal of Sincere Service from the Ministry of Interior in 2003.
- Rashid Award for Academic Excellence (1999, 2001, 2008).
- UAE President's Medal for the top university graduates in 1998.
- KPMG Peat Marwick Trophy for Best Researcher in the Faculty of Commerce in 1997.
- Barclays Bank Trophy for the best graduate programme in business information technology in 1997

INTERNATIONAL AWARDS

- Most Influential Personality in the Digital Identity World in the Last Decade, 2011, Italy.
- Distinguished Leadership Award in the Middle East, 2010.
- Security Innovation Award (London) in recognition of published scientific papers from the British Institute of Technology & E-commerce, 2010.
- Award of Excellence and Fame (Italy) for prominent role in the field of identity management systems and scientific research at the International Conference for Universal ID cards held in cooperation with the European Union and the Italian Ministry of Interior, 2009.
- Information Security Award from the Asian Continent Association for Government Information, 2007.
- Distinguished Personality of the Year Award (Italy) in the application of advanced identification systems, in the International Conference on Universal ID cards held in cooperation with the European Union and the Italian Ministry of Interior, 2007.
- Young Leadership Award in the field of information technology in the Middle East - United Nations and the Arab League, 2006.

INNOVATIONS

Dr. Al-Khouri has developed an innovative methodology called PROMOTE for strategic planning and management of government sector projects, during his research study at the University of Warwick, UK, between 2002-2007 (patented in the UK).

RESEARCH AND STUDIES

Dr. Al-Khouri has published over (50) articles in the past 10 years in various international journals. He is an active researcher in the field of organizational development and transformation, e-government, digital economy and in many other specialized fields. He has a book under print titled: "Strategic Management in Government Sector: an Innovative Methodology". Below is a recent list of some of these publications.

Some Recent Articles for the Author:

1. Al-Khouri, A.M. (2012) **"Emerging Markets and Digital Economy: Building Trust in the Virtual World"**, International Journal of Innovation in the Digital Economy, Vol. 2, No. 3, pp. 57-69.

2. Al-Khouri, A.M. (2012) **"Biometrics Technology and the New Economy"**, International Journal of Innovation in the Digital Economy, Vol. 2, No. 4.

3. Al-Khouri, A.M. (2012). **"PKI in Government Digital Identity Management Systems"**. Surviving in the Digital eID World, European Journal of ePractice, No. 14, pp. 4-21.

4. Al-Khouri, A.M. (2012) **"The Role of Digital Certificates in Contemporary Government"**, International Journal of Computer Science Engineering and Information Technology Research, Vol. 2, No. 1, pp. 41-55.

5. Al-Khouri, A.M. (2012) **"PKI Technology: A Government Experience"**, International Journal of Computer Science Engineering and Information Technology Research, Vol. 2, No. 1, pp. 115-141.

6. Al-Khouri, A.M. (2012) **"Population Growth and Government Modernisation Efforts: The Case of GCC Countries"**, International Journal of Research in Management and Technology, Vol. 2, No. 1, pp. 1-9.

7. Al-Khouri, A.M. (2012) **"Targeting Results: Lessons Learned from the UAE National ID Program"**, Global Journal of Computer Application and Technology, Vol. 2, No. 1, pp. 830-836.

8. Al-Khouri, A.M. (2011) **"Optimizing identity and access management (IAM) frameworks"**. International Journal of Engineering Research and Applications, Vol. 1, No. 3, pp. 461-477.

9. Al-Khouri, A.M. and Bechlaghem, M. (2011) **"Towards Federated e-Identity Management across GCC – A Solution's framework"**. Global Journal of Strategies & Governance, Vol. 4, No. 1, pp. 30-49.

10. Al-Khouri, A.M. (2011) **"An innovative approach for e-Government transformation"**. International Journal of Managing Value and Supply Chains, Vol. 2, No. 1, pp. 22-43.

11. Al-Khouri, A.M. (2011) **"PKI in government identity management systems"**. International Journal of Network Security & Its Applications, Vol.3, No.3, pp. 69-96.

12. Al-Khouri, A.M. (2011) **"Re-thinking Enrolment in Identity Schemes"**. International Journal of Engineering Science and Technology, Vol. 3, No. 2, pp. 912-925.

13. Al-Khouri, A.M. (2011) **"Improving Organizational Performance through understanding Human Motivation"**. Chinese Business Review, Vol.10, No.5, pp. 384-394.

14. Al-Khouri, A.M. (2011) **"Targeting Results"**. Proceedings of the 2011 International Conference on Industrial Engineering and Operations Management, Kuala Lumpur, January 22-24, 2011, pp.104-111.

15. Al-Khouri, A.M. (2011) "**When Strategic Focus is Needed in Organizations**", Proceedings of the 1st International Conference on Changing Perspective of Management: Revisiting the Existing and Explore the Novel Ideas, Nepalese Academy of Management, Nepal, 10-12 March 2011, Vol. 2, No. 1, pp. 336-340.

16. Al-Khouri, A.M. (2010) "**Facing the Challenge of Enrolment in National ID Schemes**", The Biometric Landscape in Europe', Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, BIOSIG 2010, Darmstadt, Germany, September 09 -10, 2010, pp.13-28.

17. Al-Khouri, A.M. (2010) **"The Question of Identity"**. Proceedings of the 21st-Century Gulf: The Challenge of Identity, University of Exeter, U.K., 30 June - 3 July 2010.

18. Al-Khouri, A.M. & Al-Mazrouei, N.M. (2010) "**A strategy framework for the risk assessment and mitigation for large e-government projects**", International Journal of Computer Science and Network Security, Vol. 10 No. 10 pp. 34-39.

19. Westland, D.D. and Al-Khouri, A.M. (2010) "**Supporting Use of Identity Management to support e-Government progress in the United Arab Emirates**," Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

20. Al-Khouri, A.M. (2010) "**Improving Organisational Performance**", Proceedings of 18th Annual International Conference on Modern Workforce Challenges, Responsibilities, and Rights in the Global Community, The Association on Employment Practices and Principles (AEPP), 29 September to 01 October 2010, University of San Francisco, San Francisco, CA. pp. 24-37.

21. Al-Khouri, A.M. (2010) "**The Challenge of Identity in a Changing World: The Case of GCC Countries**," Proceedings of the 21st-Century Gulf: The Challenge of Identity, University of Exeter, U.K., 30 June - 3 July 2010.

22. Al-Khouri, A.M. (2010) "**Succeeding with Transformational Initiatives: Practical Approaches for Managing Change**," Management Research and Practice Journal, Vol. 2, No. 1, pp.108-131.

23. Al-Raisi, A.N. & Al-Khouri, A.M. (2010) "**Public Value and ROI in the Government Sector**," Advances In Management, Vol. 3, No. 2, pp.33-38.

24. Al-Khouri, A.M. (2008) "**Why Projects Fail? The devil is in the detail**," Project Magazine [Online]. Available from:www.projectmagazine.com.

25. Al-Raisi, A.N. & Al-Khouri, A.M. (2008) "**Iris recognition and the challenge of homeland and border control security in UAE**," Telematics and Informatics, Vol. 25, pp.117-132.

26. Al-Khouri, A.M. & Bal, J. (2007) "**Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics**," Journal of Computer Science, vol.3, no. 5, pp.361-367. This paper was quoted for its innovative approach in the: Summer '07 Intelligence section in MIT Sloan Management Review.

27. Al-Khouri, A.M. & Bal, J.(2007) "**Electronic Government in the GCC Countries**," International Journal Of Social Sciences, Vol. 1, No. 2, pp.83-98.

28. Al-Khouri, A.M. (2007) "**Using Quality Models to Evaluate National ID systems: the Case of the UAE**," International Journal Of Social Sciences, Vol. 1, No. 2, pp.117 -130.

29. Al-Khouri, A.M. (2007) "**UAE National ID Programme Case Study**," International Journal Of Social Sciences, Vol. 1, No. 2, pp.62-69.

30. Al-Khouri, A.M. (2007) "A **Methodology for Managing Large-Scale IT Projects**," Proceedings of Warwick Engineering Conference, Warwick University, Warwick, United Kingdom, May 23, pp.1-6.

31. Al-Khouri, A.M. (2007) **"Quality Models for IT Systems,"** Proceedings of World Academy of Science, Engineering and Technology, Vienna, Austria, Vol. 21.

Thoughts with impact – Part 3

Critical Thoughts

From a Practitioner Mindset

ISBN978-9948-16-568-2

Author Biography:

Dr. Al-Khouri is the Director General (Under Secretary) of Emirates Identity Authority; a federal government organisation established in 2004 to rollout and manage the national identity management infrastructure program in the United Arab Emirates. He has been involved in the UAE national identity card program since its early conceptual phases during his work with the Ministry of Interior. He has also been involved in many other strategic government initiatives in the past 22 years of his experience in the government sector.

He holds an engineering doctorate degree in strategic and large scale programs management from Warwick University, UK; Masters Degree (M.Sc.) in Information Management from Lancaster University, UK; and a Bachelors Degree (B.Sc., Hons.) from Manchester University, UK. He is also a member in several academic and professional institutions.

He is an active researcher in the field of advanced technologies implementation in government sector, and the approaches to reinventing governments and revolutionising public sector services and electronic business. He has published more than 50 research articles in various areas of applications in the past 10 years.

Articles In This Book:

The New Digital Economy

e-Government Practices

Identity and Access Management

Contemporary Identity Systems Implementation

ISBN 978-9948-16-568-2