

THOUGHTS
WITH IMPACT - PART 5

Critical Insights

from
a Government
Line of **Attack**

Dr. Ali M. Al-Khouri

A SERIES OF PUBLISHED PAPERS
IN INTERNATIONAL JOURNALS (2013-2014)

THOUGHTS WITH IMPACT PART 5

Critical Insights

from a Government Line of Attack

Dr. Ali M. Al-Khour

A SERIES OF PUBLISHED PAPERS
IN INTERNATIONAL JOURNALS (2013-2014)

Critical Insights from a Government Line of Attack

Emirates Identity Authority

Abu Dhabi, United Arab Emirates

Version 1 Printed in 2014

ISBN 978-9948-20-683-5

Index

Forward	5
Preface	8
i - Smart Government	
1 - Technological and Mobility Trends in e-Government	13
2 - Exploring the Role of Technology in a Joined up Government: A Proposed Framework for Service Governance	61
3 - Connected Government: UAE Government Integration Strategy	91
ii - Digital Identity	
4 - Digital Identity: Transforming GCC Economies	125
5 - Federated e-Identity Management across the Gulf Cooperation Council	153
6 - Identity Management in the Age of Mobilificaiton	183
iii - Identity Applications	
7 - Privacy in the Age of Big Data: Exploring the Role of Modern Identity Management Systems	219
8 - Identity Management in the Retail Industry: The Ladder to Move to the Next Level in the Internet Economy	241
9 - Environment Sustainability in the Age of Digital Revolution: A Review of the Field	265
About Emirates Identity Authority	291
About the Author	292

Foreword

The contemporaneous challenges and issues associated with the field of identity management in today's world is attracting the attention of policy-makers from all over the globe, regardless of the sector that they work in. This is, in principle, due the precious role of modern identity management systems that could play a role in laying down the building blocks of the overall social security systems, and citizen safety aspects. Modern identity management technologies are showing disruptive positive potential to contribute toward supporting ambitious governmental efforts seeking to uplift public sector services and its overall performance, and stimulate transformation toward digital economy operating models.

In this sense, scientifically conducted action-research, that focuses on distinctive and contemporary challenges facing governments in the real world of practice, has a higher potential to contribute toward enhancing the current limited knowledge base and increasing the chances of more successful endeavors. The exchange of learned lessons, along with



His Highness Sheikh
Saif Bin Zayed Al Nahyan

practical insights from government initiatives and projects, would allow governments to develop a more vigorous understanding of things, and should all together guide national and international practices to address the dynamically transforming world of today. If jointly carried out by all governments, for example, this should raise the quality and performance of government organizations and institutions, and support overall societal development and progress.

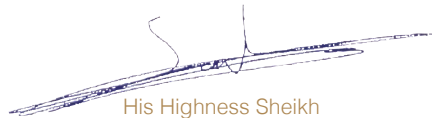
The articles within this book are felicitous attempts to shed light on various initiatives and experiments in the field of identity management, and the UAE national identity infrastructure in particular. The United Arab Emirates has made unremitting efforts, and showed strong determination, to ensure the success of its experience in the development and implementation of a world-class identity management infrastructure which is based on sophisticated and modern technologies. The aim of the infrastructure is to create new and compelling mechanisms to identify, authenticate, and verify identities both in the physical and virtual spheres. The infrastructure will then play a critical enabling role in supporting national and individual security requirements, enhance strategic decision-making, promote public sector development, and revolutionize how services are provisioned in public and private sectors. These are, all together, part of the UAE government efforts to improve its global competitiveness, and play a leadership role in the race of excellence, which are again part of a bigger picture: the “UAE 2021 Vision” that seeks to position the UAE government to become one of the best governments in the world.

The articles are designed to be pragmatic and provide in-depth and dexterous content that should constitute an added value to the field of practice, and enrich future research into this rapidly evolving field.

We are absolutely certain that the more qualitative research that takes place, from within and by government institutions, that attempts to critically examine its own initiatives and follow scientific methods to clarify and/or determine relationships between events and facts, the more likely such research will aid in solving the complex problems of today. Such

research should also become the means through which we must base our practices and development efforts, and should constitute the framework for our perpetual pursuit to make a better world for our people to live and prosper in.

As the world shrinks in light of the precipitous technological developments, the pressure on governments will continue to raise the bar for efficiency, effectiveness, and efficaciousness in order to meet people's expectations. Building a global best practices repository through sharing and exchanging knowledge is the only way to develop a better world. This should support virtuous governmental efforts that aim at building a more responsive generation of future governments, and aim to raise the quality standard of living in our communities.

A handwritten signature in blue ink, consisting of a large, stylized 'S' followed by a horizontal line that tapers to the right.

His Highness Sheikh
Saif Bin Zayed Al Nahyan

Deputy Prime Minister, Minister of Interior,
Vice-President, Emirates Identity Authority,
United Arab Emirates.

Preface

This book is the fifth in a series. It represents a collection of published research articles in several international journals between 2013 and 2014. They cover topics related mainly to one of the most perilous fields of practice; namely: the advances and use of modern identity management systems for contemporary applications.

In principle, the articles provide critical insights of how the UAE government mainly, and GCC countries in broader sense, envisage and use modern identity management infrastructure, to lay down the building blocks of digital economy. Throughout the articles, identity management is contemplated as a source of growth, with the potential to support more productive and stronger national economies, to foster innovation, competitiveness and user participation, and to contribute effectively to the prosperity of societies as whole.

To allow better reading, articles included in this book were grouped into three categories: smart government, digital identity, and identity applications. They bring in various experimented practices and portray UAE government intentions to fabricate trusted and secure cross-border infrastructure to authenticate and validate electronic identities and for different applications.

Once again and as we emphasized in previous series, these articles are distinguished from those available studies in the existing body of knowledge conducted in the Middle East. Research studies in general are normally conducted by researchers who are very much interested in the academic rigor, rather than its practicality. Also very limited information is normally exposed and distributed about government projects which are by and large characterised to be classified, which makes existing research studies lack some fundamental understanding of issues that makes up the bigger picture.

The research work in this book was written by a senior government official and brings forward key critical insights from several strategic government initiatives, management frameworks, imperative thoughts, reflections, and fundamental lessons learned. This should allow management to deepen their understanding of such projects and practices and better manage the associated risks, and fuse their lines of attack in terms of how similar projects are approached, managed and implemented.

In short, the intention of this work is to support the advancement of the researched fields and contribute towards global development of knowledge in order to make this world a better place to live in for everybody.

I hope that you will find this book usable and practical.

Dr. Ali M. Al-Khouri

2014



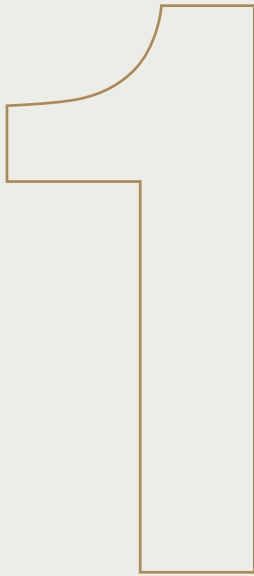
1

2

3

Smart Government

- 1 - Technological and Mobility Trends in e-Government
- 2 - Exploring the Role of Technology in a Joined up Government: A Proposed Framework for Service Governance
- 3 - Connected Government: UAE Government Integration Strategy



Technological and Mobility Trends in E-Government¹

1

Abstract

Electronic government (e-government) has been attracting the attention of the world for the past two decades, and specifically, upon the advent of the internet. Governments worldwide have spent billions of dollars to date to transform themselves into e-government. However, their efforts and large investments resulted mainly in online portals and scattered electronic services. Various studies indicate that e-government initiatives are failing to meet citizens' expectations for convenient service delivery systems. Nonetheless, the rapid pace at which technology is innovatively evolving and its disruptive nature is forcing new realities to be accepted in e-government domain. The new forms of mobility made possible by the transforming technologies are not only changing how people live their lives today, but also redefining business models, employee productivity, customer relationship, and even how governments are structured. The growing usage of smartphones and tablets have significant impact on all industries, but at large how government services are delivered. This study attempts to provide some qualitative input to the existing body of knowledge. It sheds light on some trends that have high impact to disrupt existing technological-based channels of interaction between governments and citizens, and ultimately on service delivery. It also sheds light on the role of modern identity management infrastructure in enabling higher levels of trust and confidence in mobile transactions.

Keywords: *e-government, digital identity, mobile government, NFC technology, identity management.*

¹ Please quote this article as follows:

Al-Khoury, A.M. (2013) "Technological and Mobility Trends in e-Government". *Business and Management Research*, Vol. 2, No. 3, pp. 90-112.

1. Introduction

Today's world is going through rapid transformation owing to the fast pace of change in technological development and adoption. The constant evolution in the field of technology is pushing governments and businesses alike to move from a product-based to an information-based mentality and practice. However, this is not easy to achieve in light of the vacuum of revolutionary digital concepts and substances with which we live. Success in the e-government domain is very much determined by the agility and flexibility of organizations to evaluate and strategically align their businesses to the growing choices of enabling technologies.

In principle, enabling technologies can come in two forms: sustaining or disruptive innovation (Christensen, 1997; 2003). Sustaining innovation are those existing but incrementally evolving technologies that can be incorporated into present practices and structures of organizations to establish a positive and sustainable impact on capabilities, business operations, and models. On the other hand, disruptive innovation simply forces changes in existing business practices and models, bringing a new twist to existing markets and technologies, and displaces them over time. The effect of disruptive innovation is new and revolutionary.

In practice, organizations get locked-in with their legacy systems and technologies, and usually get used to focusing on development possibilities of such legacies. Such systems and technologies may well help organizations, for instance, to improve performance in marketing, sales, and customer support, lower costs, and improve margins, among other ways. However, disruptive innovation attempts to bring to niche markets similar capabilities, but adds real value to customers (Piao & Okhuysen, 2012). In other words, disruptive innovation seeks to offer a technology that pays higher attention to simplicity, convenience, ability to customize, and/or price dimensions (Dombrowski & Gholz, 2009; Robb, 2006). Disruptive innovation is about delivering innovations aimed at a set of customers whose needs are being ignored (Gilbert, 2012). As depicted in Figure 1, once a truly disruptive product or service takes root in simple applications at the bottom of a market, it can move relentlessly up market, eventually displacing established competitors.

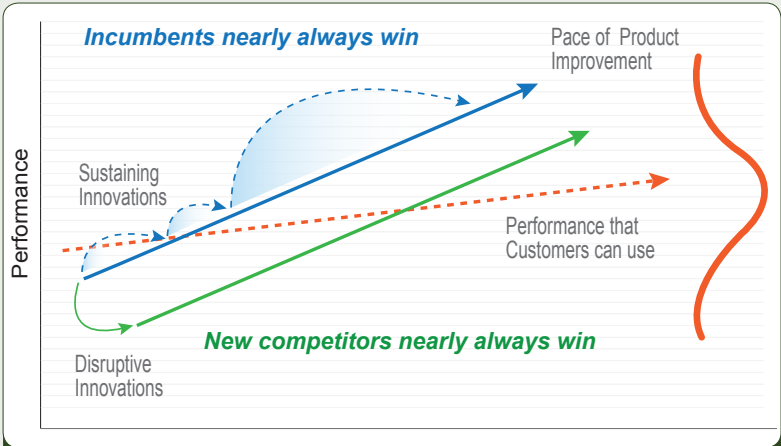


Figure 16. Utilisation rates monitoring dashboard.



Market trends indicate that the coming years will witness a storm of both sustaining and disrupting innovations, which will shake and reshape all markets and industries (Hang & Kohlbacher, 2008; Kim & Mauborgne, 2005; Paap & Katz, 2004; Tellis & Golder, 2003). This in turn will also have a significant impact on global economies and government work in relation to e-government development.

There is a strong relationship between e-government progress and technological developments as we highlighted earlier. E-government is still struggling to move to more advanced levels of development amidst the growing choices of technologies. Although the full transformative upshots of e-government loiter unrealized in principal, the precipitous augmentation in interest and resources dedicated to e-government initiatives is likely to contribute to the development of this cardinal field of practice.

In this article we focus on shedding light on some technological trends that governments need to heed in their e-government initiatives. These trends are expected to have a high disruptive impact on existing e-government service delivery methods, as well as the interactions channels between governments and citizens. The design and content of this article aims to contribute towards providing a helicopter-level view of what policymakers and practitioners need to be paying attention to in terms of conceptual and technological developments in the field of e-government.

This article is structured as follows. Section 2 provides a short overview of the field of e-government. Section 3 outlines five major technological developments and trends that governments need to address in their e-government initiatives. Section 4 stipulates the evolving role of modern identity management infrastructures in enabling identification and authentication methods on smart mobile phones. Section 5 provides a brief discussion and reflection on areas surrounding the implementation and progress of e-government, and the article is concluded in the following section, section 6.

2. e-Government: A State of Constant Change and Revolution

According to the World Bank e-government refers to the use, by government agencies, of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government (World Bank, 2011). These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management (World Bank, 2011). Among the many potential contributions include lessening corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions.

There are hundreds of other definitions in the current literature of what e-government means (Andersen & Henriksen, 2005; Atkinson, 2003; Brown, 2003; CDT, 2002; De, 2004; Devadoss et al., 2002; Grönlund, 2002; Satyanarayana, 2004; Shailendra et al., 2007; UNDESA, 2003). Most definitions in the field of practice take a governance perspective (Grönlund & Horan, 2004). All in all, e-government globally is viewed to not only to be about computerization of a government system or a technology endeavor but a belief in the ability of technology to achieve high levels of improvement in various areas of government (APT, 2012). Accordingly, various models have been developed to implement e-government and leverage IT in facilitating organizational change in government business (Zarei et al., 2008). E-government implementation (or maturity) models primarily use the X and Y dimensions of complexity and integration levels to illustrate the development as we move from one phase to another.

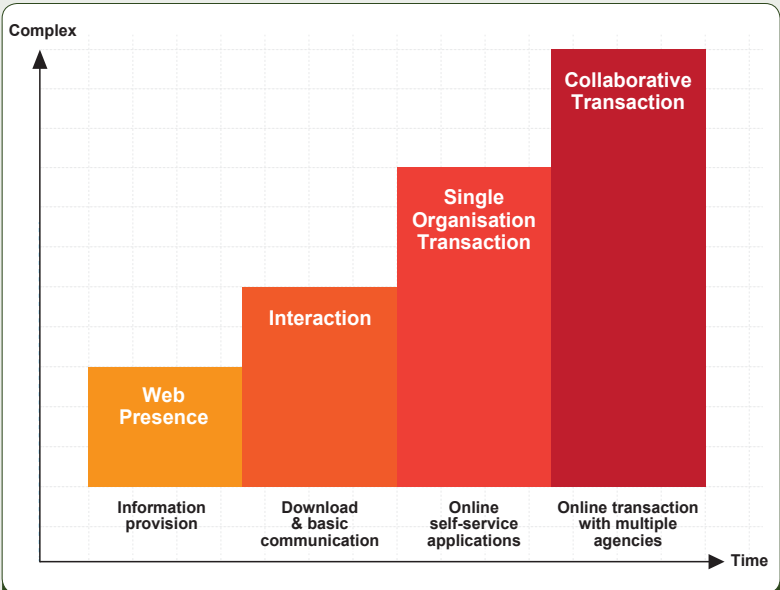
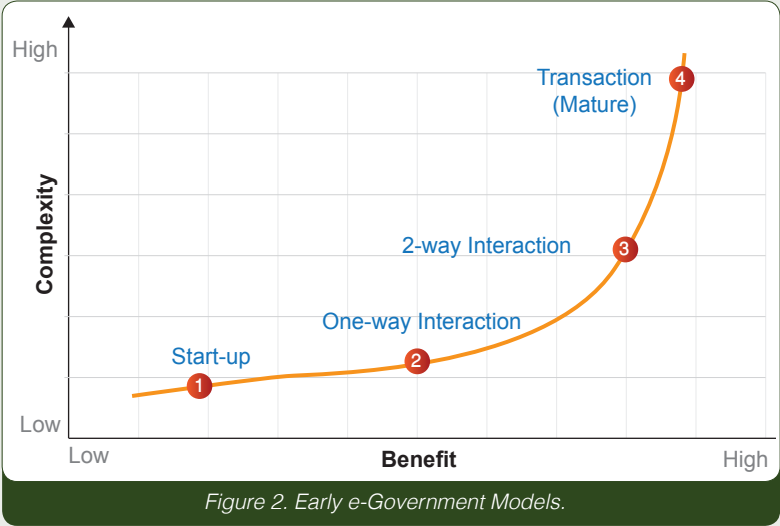
Figure 2 depicts one of the early e-government models that consist of four phases. The first phase embodies an early and very basic online presence, where governments start creating websites and use them for informational and very limited interactions with citizens. Phase two involves creating links to archived information that is easily accessible to citizens,

as for instance, documents, forms, reports, laws and regulations, and newsletters. In the third phase, governments develop interactive portals that provide online services and aim to enhance online user experience, e.g., downloadable forms for tax payments and applications for license renewals. The fourth phase is where all government transactions are conducted online, and available on a “24/7” basis.

Another model is depicted in Figure 3. It provides a more enhanced view of e-government development stages. Although the first and second phases are similar to the ones in the earlier diagram, the third and fourth phases are a little different in the below diagram. The online services provided in the third phase are limited to a single organization. Services at this stage include not only traditional internet-based services, but are delivered on various electronic channels, some of which might be considered disruptive, like iPad apps for instance. Services in the fourth phase are cross boundaries, and involve concepts like a “one-stop-shop” where some kind of collaboration is needed between government agencies to enable such business models.

The third e-Government model is depicted in Figure 4. Compared to the earlier (second) model, this model pushes the transactional phase one step back to phase two, and breaks down the third phase into two new phases. The third phase is where governments initiate the transformation of their processes and services rather than the automation. The focus at this stage is on integration of government functions at different levels, such as those of local governments and central/state governments. The fourth phase focuses on the integration of different functions from separate systems so as to provide citizens with a unified and seamless service and true one-stop-shopping experience (Layne & Lee, 2001). The authors indicate that the integration of heterogeneous requirements and resolving conflicting system requirements across different functions are typically major stumbling blocks for any government to reach this stage.

Figure 5 depicts other models that specify the level of maturity or development of e-government.



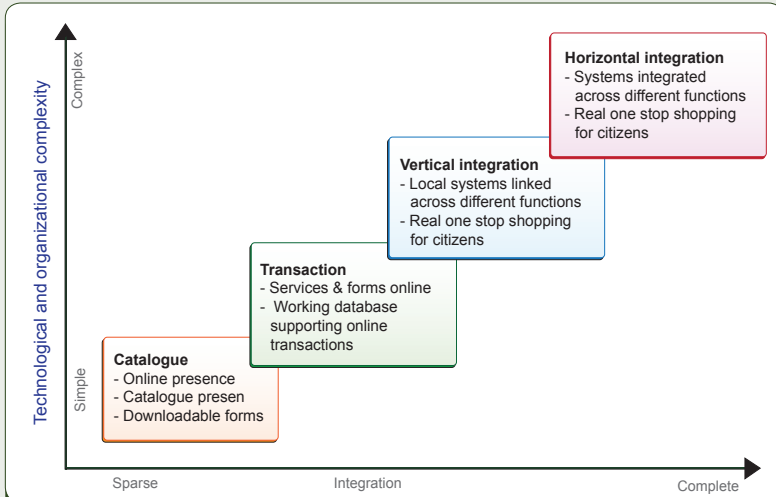


Figure 4. e-Government Evolution to Vertical and Horizontal Integration.

Gartner	Publish → Interact → transact → integrate
UNDESA	emerging → enhanced → interactive → transactional → networked
OECD	information → interaction → transaction → and transformation

Figure 5. e-Government Maturity Models.

Source: Baum and Maio (2000); Field et al. (2003); UNDESA (2003)

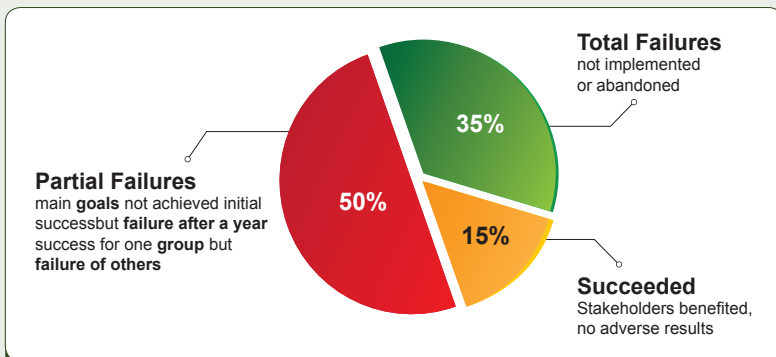


Figure 6. Survey Results of e-Government Implementations.

From our view point, Layne and Lee's four-stage model (2001) is more applicable to guide current development efforts. Our research and studies in the field indicate that governments have had limited successes in practice (Al-Khoury, 2013; Al-Khoury & Bal, 2007). There is no real evidence of success stories of true vertical and horizontal integration projects. Nonetheless, many of the announced successes in integration projects are superficial and cannot elevate to enable seamless and real-time transactions.

Various studies also indicate that almost 85 percent of e-government projects are failures (Heeks, 2006; Stanforth, 2010). See also Figure 6. This sounds horrific if we take into consideration the gigantic investments in this field (Gubbins, 2004). Despite this fact, the field of practice and academia did not succeed to present a clear recipe to achieve success and avoid failure, but rather we find hundreds of approaches, frameworks, and methodologies to support successful implementation.

Despite all the work and reasons listed in the existing literature, as practitioners we tend to believe that the evolving nature of technologies is among the many reasons for such stories of failure and the confusion in the field. Let us look at Gartner hype cycles to explain our point here.

The Gartner hype cycle depicted in Figure 7 graphs the visibility and adoption of a technology and its applications over time. Each hype cycle drills down into five key phases of a technology's life cycle: technology trigger, peak of inflated expectations, trough of disillusionment, slope of enlightenment, and plateau of productivity. Table 1 provides an explanation of each hype cycle. Simply put, these stages typically show technology evolution and industry excitement about it. These technologies have two ways of changing: either they disappear as they fail to meet the wild expectations of the industry, or they will evolve further to become more relevant to solving real business problems and present new opportunities. The overhyping and ever increasing technological options put governments in a dilemma of what to choose and what path to follow. See also Figure 7.



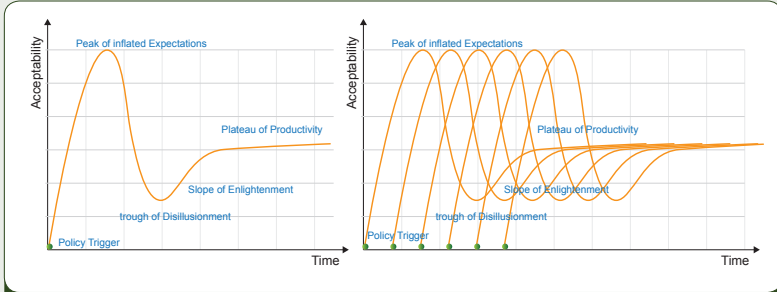


Figure 7. Gartner Hype Cycle.

Table 1. Five Phases of a Gartner’s Hype Cycle

Hype Cycle	Description
Technology Trigger	A potential technology breakthrough kicks things off. Early proof-of-concept stories and media interest trigger significant publicity. Often no usable products exist and commercial viability is unproven.
Peak of Inflated Expectations	Early publicity produces a number of success stories, often accompanied by scores of failures. Some companies take action; many do not.
Trough of Disillusionment	Interest wanes as experiments and implementation fail to deliver. Producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.
Slope of Enlightenment	Another instance of how the technology can benefit the enterprise starts to crystallize and becomes more widely understood. Second- and third-generation products appear from technology providers. More enterprises fund pilots; conservative companies remain cautious.
Plateau of Productivity	Mainstream adoption starts to take off. Criteria for assessing provider viability are more clearly defined. The technology’s broad market applicability and relevance are clearly paying off.

The point that we would like to make here is that of the dynamic nature of technological evolution and the somewhat reasonably slow government responsiveness. Governments have been characterized as “big elephants” for a long time. They move slowly, and sometimes their bureaucratic style is controlled by their political nature and context. This makes them the slowest and very last adopters of a given technology hype. Once governments implement a technology, it stays there for long. This is not the case in the private sector, where they tend to sustain and develop such technologies, and plan for incremental breakthroughs. However, despite the excuses we use, disruptive innovations are turning things around. Figure 8 depicts the emerging technologies, some of which are expected to re-shape organizations both in public and private sectors.

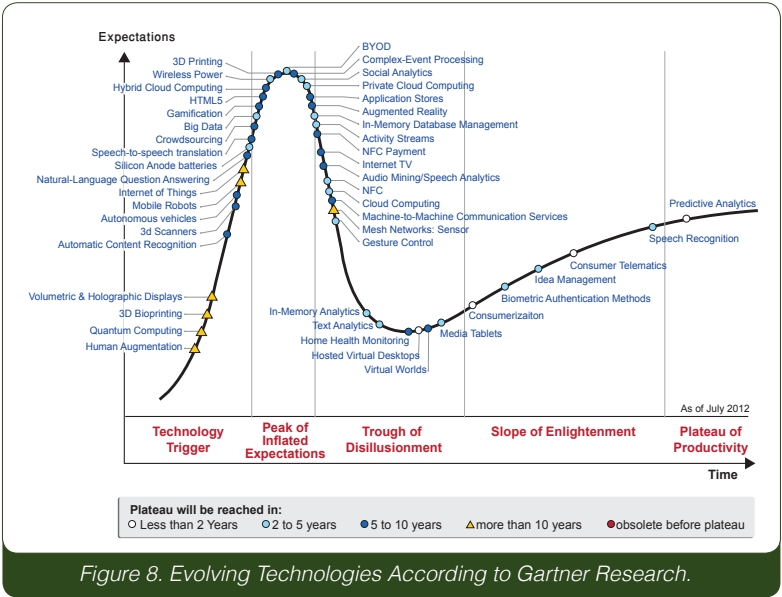


Figure 8. Evolving Technologies According to Gartner Research.



From a different standpoint, the decentralized approach of implementation has opened room for diverse interests in dissimilar technologies to be adopted in the government sector. Each organization has its own standpoint and view of sustaining or disruptive innovation adoption. The level of responsiveness varies greatly from one to another government organization. Each government organization may have its own technological implementation and readiness level. The complexity arises when different and silo systems need to talk to each other, but are confronted with a reality that makes this a nightmare. In other words, the integration of systems, be they vertical or horizontal, becomes a moving target because of interoperability, (non)-standardization, and other network effects (Cave and Simmons, 2007).

This is perhaps why e-government is facing difficulty in moving up the development phases of vertical and horizontal integration levels, at least from a technical perspective. Having said that, the next section provides an overview of some critical technological trends that governments need to take into account in their e-government plans. These have considerable implications for practitioners in the field of e-government.

3. Technology Trends

Technological developments are driving e-governments to address growing citizens demand for 'better government' in terms of convenience, accessibility, efficiency, effectiveness of government operations. The recently published reports by Deloitte and International Data Corporation (IDC) indicate the need to pay higher attention to five technological hype cycles: social, mobile, analytics, cloud and cyber technologies (Deloitte, 2013; IDC 2013). The reports also indicate that these are likely to converge in the short future and contribute towards having the most significant impact on businesses. These are discussed next subsequently.

3.1 Social Business Process Re-engineering

The traditional concept of business process re-engineering (BPR) focuses on the analysis and re-design of workflows and processes within an organization (Hammer & Champy, 1993). Much of the earlier BPR initiatives leveraged information technology to automate manual tasks, and/or to minimize processes in order to attain dramatic improvement in critical performance measures, such as cost, quality, service, and speed. Recent developments in the field of technology are shifting the focus of BPR initiatives to not only aim merely on the optimization of existing processes and applications, but also to the innovation possibilities through the use of social media technologies (Thames, 2011). See also Figure 9.

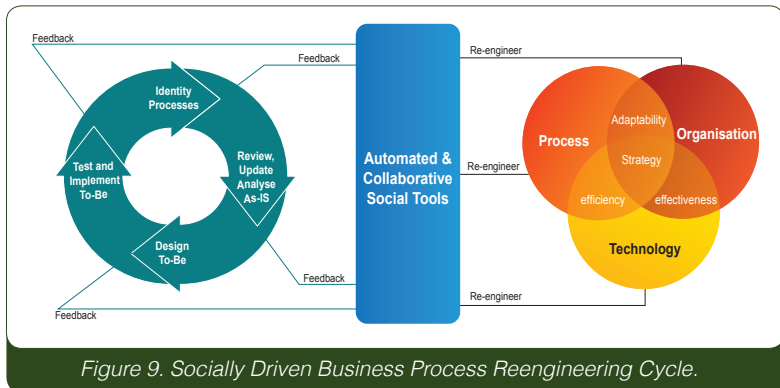


Figure 9. Socially Driven Business Process Reengineering Cycle.

Social BPR leverages social tools and automation of collaboration to integrate the output of collaborative (human) steps to enhance process output (Thames, 2011). It focuses not only on efficiencies but also on maximizing the value of process output. Social BPR recognizes that the output of business processes can be significantly improved if the process can harness the power of collaborative and conversational activities between parties that have logical input into the process. This is to say that social tools provide new capabilities like capturing, analyzing, and accommodating conversational steps that can be integrated into core business processes. Social reengineering by design is about creating new ways to motivate employees and customers, and reshaping the content and context of work to improve business performance (Ferguson, 2013). It is a course driven by mindshare and engagement with a more enlightened, user-centric approach to problem-solving and knowledge management (Clifford, 2013; Davenport & Patil, 2013; Raftery, 2013).

Governments need to pay more attention to aspects of social tools to once again re-engineer their processes, systems, and the overall organization. Social platforms can be used to fundamentally change the hierarchal and bureaucratic approaches in government agencies, e.g., how the work gets done, solutions are reached, and innovation is stirred (Bornstein, 2013). The ultimate goal of social re-engineering should be directed towards reducing silos and systematically putting data, people, and processes in the operational contest in communication (Manifesto, 1999). Social collaboration approaches and tools have the potential to play a vital role to support e-government progress. As such, governments need to embark on social-based business processes and re-engineering initiatives to address business improvement opportunities.

3.2 Mobile Adoption Era

Mobile government (or m-government, referring to the extension of e-government to mobile platforms) is an important area of practice to improve the productivity of public services and the responsiveness of government (McMillan, 2010). The hi-tech and fast-moving innovation engine in the mobile industry is re-shaping business operating models

and marketplaces. Mobile phones and smart devices are spreading ubiquitously as portable mini computers across the planet (Perez, 2012). Global mobile penetration grew ten-fold in the last 10 years and is likely to reach almost 100% by 2018 (Rannu, 2010).

A study by Morgan Stanley reports that by 2014, internet access through handheld devices will surpass laptops and desktops (Meeker, 2010). See also Figure 10. Forbes points out that smartphones and tablets are progressively becoming the “remote control” of the world (Olson, 2013). The following two sections will outline two trends of mobility that are considered to be adding significant value to e-government services.

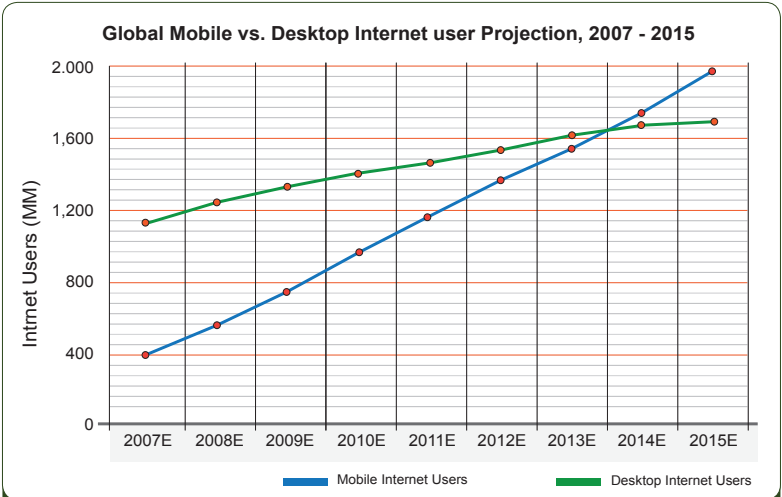


Figure 10. Mobile and Desktop Internet Users.

Source: Meeker (2010)



3.2.1 Mobile Applications (mobile apps)

Mobile applications (mobile apps). Mobile application (or mobile app) is a software application designed to run on smartphones, tablet computers, and other mobile devices. The term app is becoming popular as its usage has become increasingly prevalent across mobile phone users (Ludwig, 2012). Market research shows an increase in mobile app adoption in recent years (Hughan, 2013; Ludwig, 2012). It is estimated that 1.2 billion people worldwide were using mobile apps at the end of 2012 and this number is forecasted to grow to 4.4 billion users by 2017 (Whitfield, 2013). See also Table 2.

Table 2. Users of Mobile Apps Worldwide by Region, 2012-2017.

Region	2012	2013	2017
App users worldwide	1.2 billion	N/A	4.4 billion
Asia Pacific	30%	32%	47%
Europe	29%	28%	21%
North America	18%	17%	10%
Middle East & Africa	14%	13%	12%
Latin America	9%	10%	10%

Source: Whitfield (2013)

There are serious implications for governments and businesses in this domain. Mobile apps allow the leverage of nearly infinite resources of information and services. It is important to consider mobile apps as a central part of the e-government strategy to benefit from the opportunity of engaging new, constantly connected citizens. Governments could leverage the growing network of mobile citizens to improve the delivery of convenient and highly efficient public services (Su et al., 2010). In Australia, the share of citizens using mobile devices to interact with government doubled in just two years, with 35% of them using a mobile app at least monthly (Grandy & Newman, 2013). Mobile devices are the today's "killer" solutions for e-government to connect with those who were left behind in the digital gap.

3.2.2 BYOD and CYOD

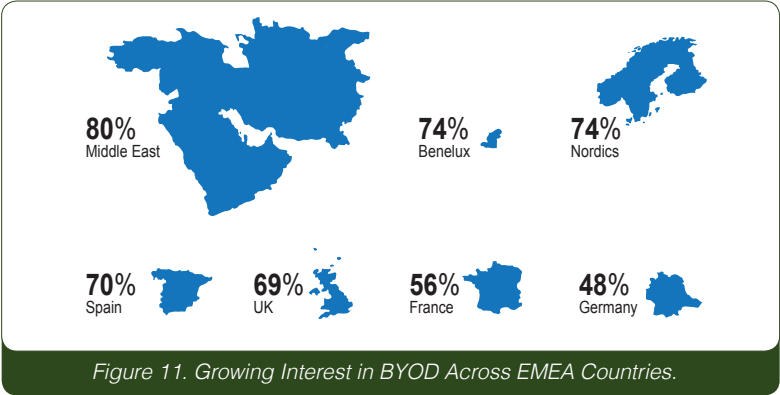
In enterprise terms, concepts like bring your own device (BYOD) and choose your own device (CYOD) are prompting changes in the patterns in enterprise application development (Hayes & Kotwica, 2013). BYOD is where people can bring their own personal devices such as laptops, tablets, and smart phones to access corporate networks and data. CYOD is where employees choose from a pre-approved list of devices, owned by the company, but can be used from anywhere. Both concepts are viewed to enable organizations to take advantage of new technology faster, and have the potential to reduce traditional hardware costs and improve organizational productivity and flexibility (Azoff, 2013). Despite the security concerns, it is indicated that it would be nearly impossible to prevent BYOD from occurring, and that the only option is to try to manage the risks posed by it (Barbier et al., 2012; Drury & Absalom, 2013; Wiech, 2013).

Solutions like mobile device management (MDM) address much of the concerns related to data security, policy, and integration (Redman et al., 2011). MDM solutions allow agencies to have much tighter control on how smartphones and tablets are used to conduct official business (Klett & Kersten, 2012). Most MDM solutions prevent unauthorized devices from accessing a network, allow phones to be remotely disabled, and can be used to deploy enterprise applications (Johnson, 2011).

Once again, governments need to take advantage of mobility and develop a phased approach to build an ecosystem that supports BYOD plans. Government employees, similar to their colleagues in other sectors, will continue to add devices to the corporate network to make their jobs more efficient and enjoyable. Therefore, organizations must plan for this legally, operationally, and culturally (Symantec, 2012).

We strongly believe that more government agencies will start implementing policies for dealing with both corporate-owned and personally-owned devices to address needs of workers for reliable

access from anywhere at any time, who can stay connected and productive outside normal business hours (see also Abdul, 2013). Figure 11 depicts the results of a survey conducted by Aruba Network in 2012 that revealed growing interest in the development and implementation of the BYOD phenomenon in private and public sector organizations across Europe, the Middle-East, and Africa (EMEA). The study indicated that organizations are taking considerable steps towards BYOD adoption. Of those organizations polled, 69% allowed some form of BYOD, ranging from strictly limited to internet connectivity, to some access to corporate applications on employee-owned devices. In short, BYOD is not an option to ignore.



3.3 Cloud Computing

Cloud computing appears to be a transformative change and a revolutionary concept for many businesses, governments, and citizens (Collier, 2012). Cloud computing is “a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (NIST, 2010). The concept itself has a huge impact on cost savings, operations improvements, and scalability (Erl et al., 2013). According to Gather, by 2012, 20% of businesses have adopted cloud services and owned no IT assets (Veljanovska & Zdravevska, 2013).

Cloud computing emphasizes a shift from stand-alone legacy systems to integrated public and private cloud computing solutions. Tables 3 provides the service models enabled by cloud computing.

Table 3. Cloud Computing Service Models. Source: Simic et al. (2012)

Cloud Service	Description
Infrastructure as a Service (IaaS)	A potential technology breakthrough kicks things off. Early proof-of-concept stories and media interest trigger significant publicity. Often no usable products exist and commercial viability is unproven.
Platform as a Service (PaaS)	PaaS provides the consumer with the capability to deploy consumer-created or acquired applications, which are produced using programming languages and tools supported by the provider, onto the cloud infrastructure.
Software as a Service (SaaS)	SaaS provides the consumer with the capability to use the provider's applications, running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a web browser (e.g., web-based email).

1

In e-government terms, cloud provides a solid foundation for the introduction of widespread provision of services to various stakeholders (Simic et al., 2012). Applications designed using the principles of service-oriented architecture and deployed in cloud architectures will help governments to reduce operational costs and radically scale the delivery of services (Simic et al., 2012). Cloud architectures is argued to have the potential to accelerate the adoption and use of e-government and e-services (Mukherjee & Sahoo, 2010; Naseem, 2012; Veljanovska & Zdravevska, 2013).

Migration towards cloud-based services is becoming an option which must be implemented. It is becoming more viable as citizens demand more timely and cost effective e-government services. The “cloud of public services” should be viewed by governments as a catalyst for e-government development, and as a means to attain higher levels of productivity and innovation.

3.4 Big Data

With the ever increasing and explosive amount of data in today's world, the ability to analyze large data sets has the potential to fuel new waves of productivity, growth, innovation, and have a dramatic impact on the economy, scientific field, and society at large (Mayer-Schonberger & Cukier, 2013). The term big data has come to refer to these very large datasets. It also refers to the analytical capabilities to process and gain deeper insights from such datasets. The concept is not new, but the terminology of big data and its modern definition are relatively novel.

According to research conducted by McKinsey Global Institute, big data has the potential to generate substantial annual value in various sectors: \$300 billion to U.S. health care, €250 billion to Europe's public sector administration, and \$600 billion in consumer surplus from using personal location data globally (Manyika et al., 2011). Big data emphasizes a shift from basic analytics to sophisticated visualization, where attention is given to pattern discovery to making real meaning and value. The emphasis is on enabling data-driven decision-making, which should in turn enable faster speed to value, and should have a positive impact on the public sector (Simon, 2013; Yiu, 2012).

In e-government terms, big data analysis presents enormous opportunities for governments to improve the way in which services are delivered to citizens and to businesses, and to make better, targeted use of the limited resources governments have today (Bender, 2013). Research suggests that big data strategies are "the defining element to unlocking the potential" of growing mountains of information and overcoming the diverse challenges (Konkel, 2003). Figure 12 depicts some of the major challenges associated with big data, as per a survey conducted by the Government Business Council in 2013. The challenges reported in the survey included a lack of adequate resources (61%), lack of data visibility (55%), misaligned budget priorities (50%), and technological barriers to accessing data (49%).

From an e-government perspective, big data can play a critical role in

paving the way for more focused and evidence-based policy design and service implementation (Archer, 2003). However, there is a clear need for a big data strategy to enhance cross-agency data analytic capability (Cattie & Riper, 2013). Big data strategies should be designed to enable governments to build knowledge and generate growth. Strategy initiatives need to focus on (1) delivering more personalized public services that are tailored to meet citizens' needs and preferences, and (2) improved productivity as resources can be directed towards projects with greater confidence of the outcome.

Big data promises to bring fundamental change to government work. Governments need to capitalize on the power of big data to generate insights for capitalizing on new opportunities to transform government and society itself, a similar objective of what e-government attempts to achieve.

3.5 Cyberspace: The Issue of Security and Privacy

Communication is one of the foremost mediums that has unquestionably been influenced by the invention of the Internet. Without a doubt, earlier outlined technologies will use the Internet as a platform for communication.

It is critical to that for technological trends outlined in this article to evolve, security and privacy must remain the largest issues today in the cyber world (Ponemon, 2012). The notion that “as long as you are connected, that connection can go both ways” has its own psychological impact on the progress of e-government, and public acceptance and participation.

A study developed by Norton in 2013 revealed that the annual cost of cybercrime exceeded \$388 billion (Norton, 2013). See also Figure 13. More than 556 million people from 24 countries were victimized by cybercrime according to the same study. Emerging technologies including mobile and cloud computing that have recently insinuated into corporate spheres, blending personal and professional communication, were reported to have opened up new security impacts (Detica, 2011).



As more and more devices and technologies are getting ubiquitously connected and widespread, threats against nations' critical infrastructures are mounting too. Establishing trust is therefore critical not only for the development of e-government, but also for the successful convergence and evolution of the earlier-outlined four forces.

Trust is defined as “confidence in or reliance on some quality or attribute of a person or thing, or the truth in a statement” (Furman, 2009). In an earlier study that we have conducted, we found that establishing trust and security in online environments were among the primary reported impediments to e-government development (Al-Khoury & Bal, 2007). It is widely argued that building trust is a gateway for new service paradigms to emerge, thereby developing passive citizen participation into active citizen participation in public service delivery (van Duivenboden, 2002).

Commercially, there are hundreds of products and solutions that are designed to optimize trust, and are widely used in private sector. However, in the e-government context, trust is more talked about but less practiced. Trust is envisaged to be very much associated with the ability to develop a robust identity management system to identify and authenticate individual identities in physical and virtual environments.

Establishing trust through advanced identity management is considered fundamental to unleash the opportunities posed by the technological trends outlined in this article or any other ones. The next section will shed light on some government practices worldwide.



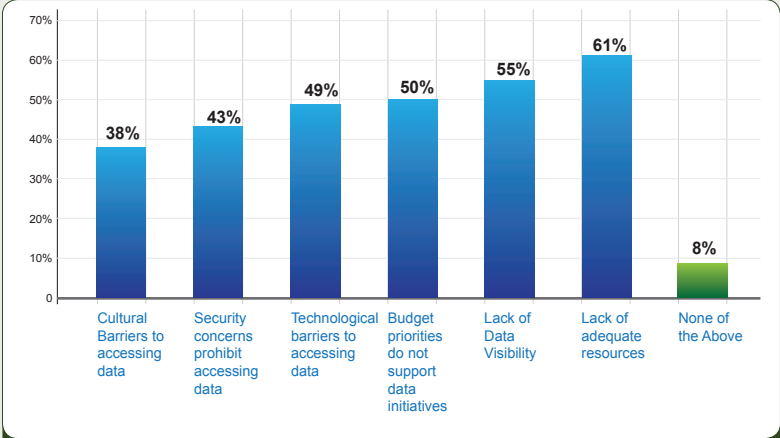


Figure 12. Challenges Associated with Big Data.

Source: Government Business Council (2013)



Figure 13. Cybercrime Source: Norton (2012).

4. National Identity Management Infrastructure

Many governments around the world have initiated advanced identity management infrastructures to support citizen identification and authentication needs (Al-Khouri, 2012). Some of the advanced programs produce secure IDs to encourage users to be engaged more actively and more expansively in the digital world (Al-Khouri, 2012b). For instance, countries like Estonia, Belgium, and UAE create digital identity profiles for their citizens, packaged in a secure smart card. This provides advanced capabilities such as those presented in Figure 14.

Modern identity cards are designed to provide multi-factor authentication capabilities. This should in turn provide higher levels of protection to individuals' security and privacy needs. With such infrastructure, e-government service providers are given verification and authentication services to enable secure remote transactions. Service seekers would remain anonymous on the Web, as only digital certificates or biometrics would be used to establish credential verification. Interestingly, some countries have already started extending their identity management infrastructures to include initiatives related to mobile identity.

Currently, Finland, South Korea, and Singapore are known to have m-enabled government services. They also use NFC² technology for transactions on mobile devices (generally for m-wallet). Oman is trying to implement this and Saudi Arabia and Qatar are in the planning stages. The United States, the United Kingdom, France, and Germany have e-commerce transactions using NFC in the retail industry to enable m-payments.

However, NFC-based authentication has not been used by anyone so far—especially in conjunction with a national ID. The issue has been that most of the countries that have implemented NFC-based mobile transactions have not used any national ID system and are instead driven

2 NFC is an abbreviation for Near Field Communication, and is a technology in smart phones that can enable contactless transactions and other data exchange with a variety of devices.

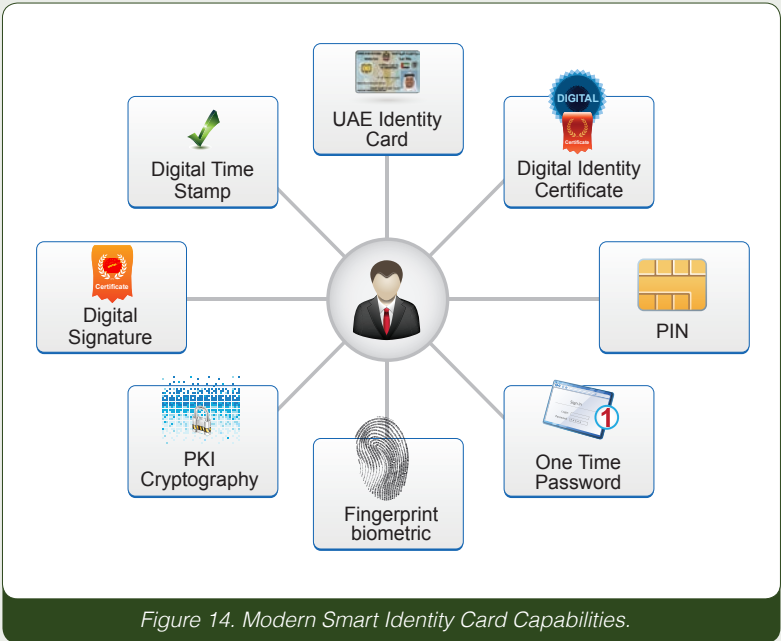


Figure 14. Modern Smart Identity Card Capabilities.



by commercial needs. The UAE government has recently started taking a lead in this particular domain.

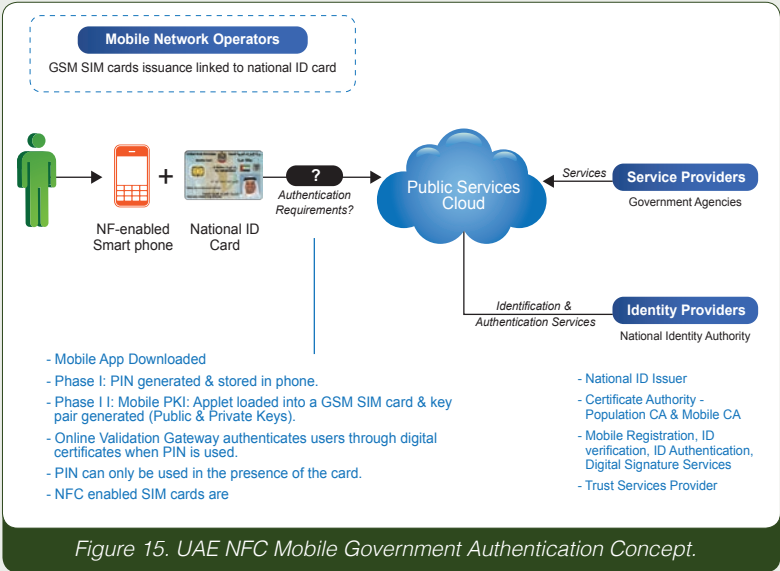
UAE is currently working to enable all its government services through mobile and smart devices by 2015 (Al-Khoury, 2012). It is trialing NFC-enabled authentication methods based on its national identity card to support the transformation process. The UAE has just enrolled all its legal residents and citizen population and issued them with smart identity biometric and PKI-based cards.

The UAE smart card is a hybrid card with contact and contactless features. The contactless feature enables NFC capabilities and allows smart phones to communicate securely with the national ID card. The rollout of the mobile ID authentication using the national ID card is planned in three phases:

1. A mobile ID application that is downloadable from an online portal.
2. A SIM-loadable mobile ID applet with the mobile PKI.
3. Using the PKI credentials in the ID card for authentication on the mobile devices.

The UAE implementation provides a highly secure ID management and user and device authentication mechanisms in mobile transactions. Figure 15 depicts a high level framework which shows how the NFC solution will be implemented.

The next section will provide a short discussion and reflection on areas surrounding the implementation and progress of e-government.



5. Reflection

The outlined technological developments are important matters for policymakers and practitioners in the field of e-government. Social media have empowered citizens in ways never seen before, increasing the influence that customers can bring to bear on important issues (Thys & Lacourt, 2013). Electronic transactions and services are also subject to this unforgiving scrutiny, so getting it right is vital (Thys & Lacourt, 2013). Mobile technologies will indeed change the way governments deliver services. Government practices and trials of NFC technologies in service delivery are likely to promote new innovations. Modern identity management systems have the potential to play a key role in enabling delivery of services over smart mobile phones. The case of the UAE is likely to solve the endemic problem of identity in the mobile domain. We would expect more governments to follow suit and implement similar projects.

However, it is important that we do not mix up technological developments and the role of e-government. Indeed, technologies will continue to evolve at a faster pace than what can be practiced in government domains. Practitioners should not look at e-government from a purely technical window. E-government should be viewed as being about citizen well-being and prosperity. There are two points that are critical to comprehend in this regard. These are related to the concepts of citizen centricity and the approach of e-government implementation, which are discussed in the following two sub-sections.

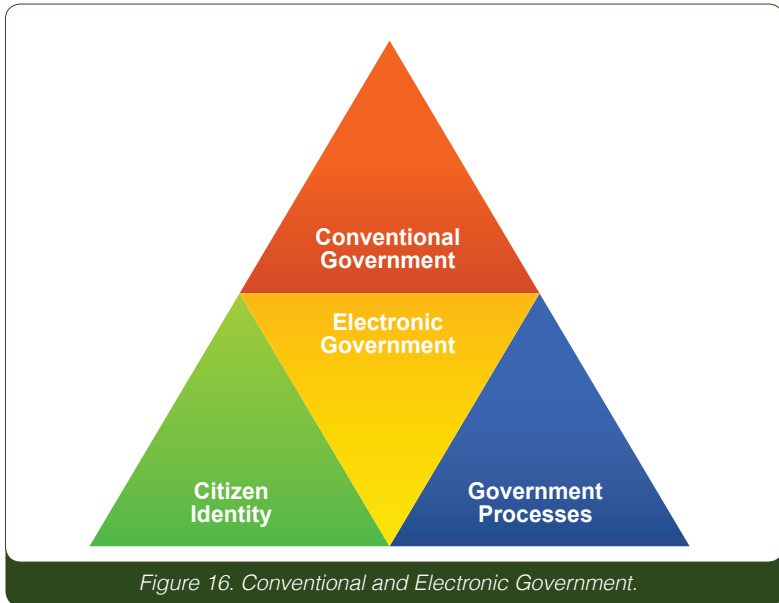
5.1 Citizen Centricity

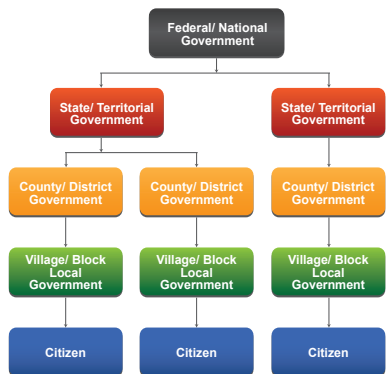
e-Government should be an electronic representation of the conventional government service delivery system. Besides, all governance systems and processes should be reflected in the e-government systems as in normal government processes. Yet, for e-government to succeed, it is essential that the identity of service-seekers and beneficiaries be protected and that trust in transactions be established securely. See also Figure 16. Without this, e-government initiatives will face challenging

times to progress forward.

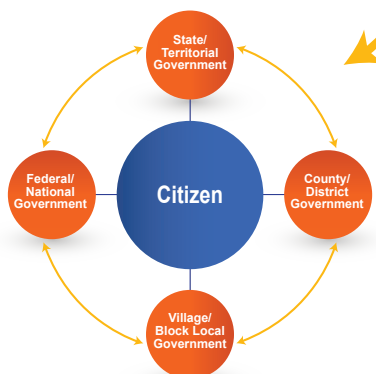
It is also critical to comprehend the evolving government structures, where citizens should come at the heart of the design when e-government is constructed. The historic focus on technology has overshadowed the organizational, structural, and cultural changes needed in the public sector (OECD, 2009). Citizen-centric service involves designing of services from citizens' point of view rather than of the government agencies. See also Figure 17.

The traditional bureaucratic silo systems approach would not support such endeavors (Chakravarti & Venugopal, 2008). User centrality is not simply about facilitating interactions and making processes and information more accessible to citizens; it is more about an alignment of government work with citizen needs to create economic and social public welfare.





Conventional Government



Mature Conventional e-Government

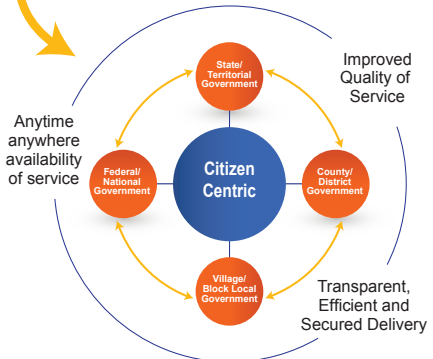


Figure 17. Evolving Government Structures.

5.2 Centralized vs. De-Centralized e-Government

Another point here is related to the notion of a centralized e-government or a decentralized approach. We tend to subscribe to the notion of a centralized e-government authority that should direct and implement an e-government model for a country to achieve a good level of success. If we examine the nature of governments and the government models themselves, we see that they are decentralized in nature.

A government is built on the blocks of a local self-government where governance at its grassroots levels is the village or small community. The different forms of government (democratic, monarchy, dictatorial, communist, etc.) are then at a federal or a central level. Any policy or regulation is from the center, and the implementation is local.

This thus presents a strong case for a central e-government authority. When government itself is central in nature, why are we attempting to create e-government in a decentralized way, where planning, regulation, and implementation are all decentralized? This comes across as rather oxymoronic and self-contradicting. This leads us to believe that it is one of the major reasons for the failure of e-governments in many countries.

Heeks (2002, 2003, 2006) presented an e-government failure model as a design-reality gap using seven factors (ITPOSMO: information, technology, processes, objectives, staffing, management systems, and other resources). This is probably the only scientific work done in this domain, but it looks at the e-government failure purely from an implementation perspective. See also Figure 18.



While this model is still valid at the implementation level, it does not seem to address the hierarchy of the government and government structure. A central e-government entity (similar to the central government) does seem to be a very good solution. This entity would design the e-government, implying policymaking, regulation, standardizing, and more importantly be responsible for compliance. Thus, this entity would define the meta-processes and meta-services for e-government, much like the central government.

This would be the blueprint for the country and thus this central entity would manage the gap that is presented in Heeks model in ensuring that e-government implementation is taken to the grassroots of governance where the citizen is the focus. Thus the much-touted citizen inclusion and empowerment becomes a reality. See also Figure 19.

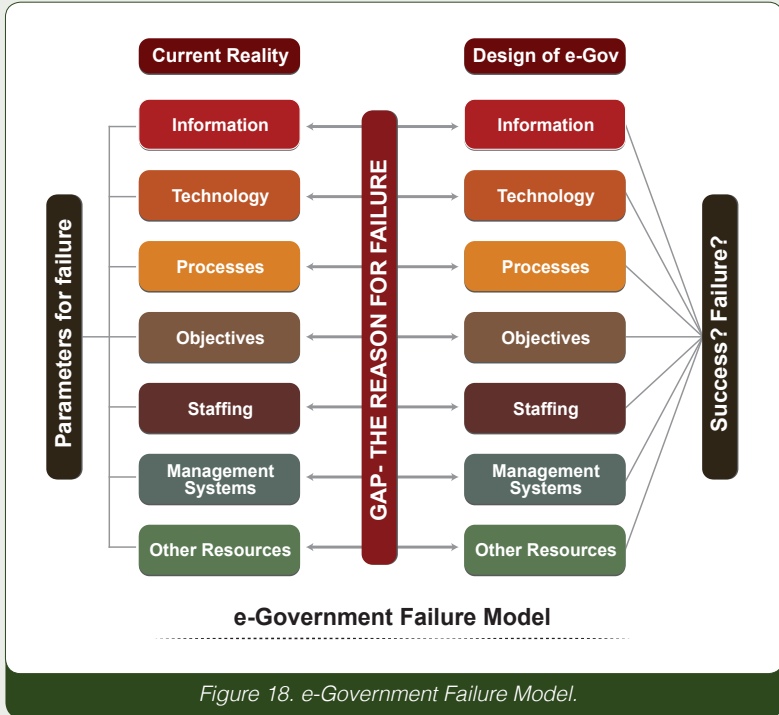


Figure 18. e-Government Failure Model.

Source: Heeks (2006)

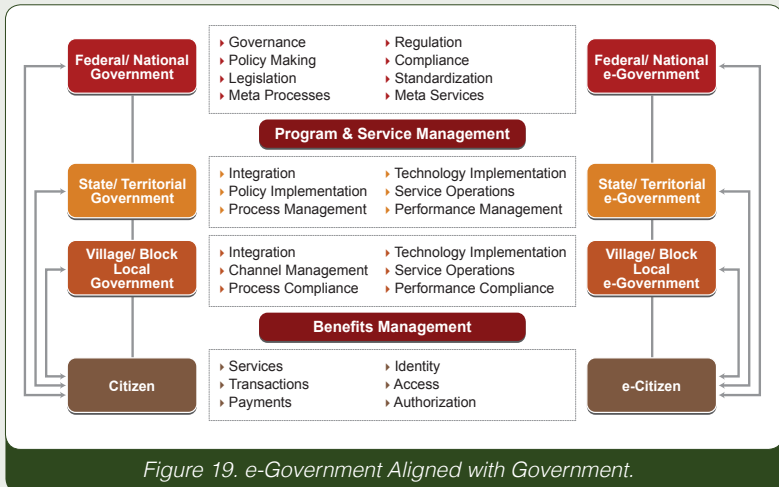


Figure 19. e-Government Aligned with Government.

6. Concluding Remarks

This article attempted to shed light on some important technological developments that governments need to consider in their e-government strategies and implementation programs. The thoughts presented around these technologies, and the short overview of government implementations in the field of identity management, should be used as a basis for developing a more enriched context to guide practice domains. Indeed, empirical research is imperative to develop more comprehensive understanding and further support the existing body of knowledge.

Overall, e-government is to a great extent associated with the evolving nature of information and communication technologies, which have a consequent impact on the integration and orchestration of services in the digital world. Governments need to shift their orientation from systems to capabilities development, and from merely solving technical issues to creating business impact. Undoubtedly, fragmented legacy IT processes and systems will typically hinder organizational efforts to effectively deliver on business needs. Governments need to re-think public sector jobs in order to keep up with the pace of change and growing technological options. Governments may need to re-invent their businesses, and technology will indeed play a strategic role. However, the road ahead is likely to be very sloppy!

The world we live in today is full of uncertainties and our view of the future is getting foggier as we move forward in time. Hierarchical structures that may have worked at some times in the past are not applicable today. See Figure 20. The world today is more chaotic, where instability is the status quo and the comfort zone in which we live and operate.

With such challenges, governments need to change its thinking hat. To truly reap the potential promises of the knowledge economy, governments need to focus more on research and development. This should in turn fuel innovation and improve the scale and magnitude of change needed in light of mind-boggling technological developments.

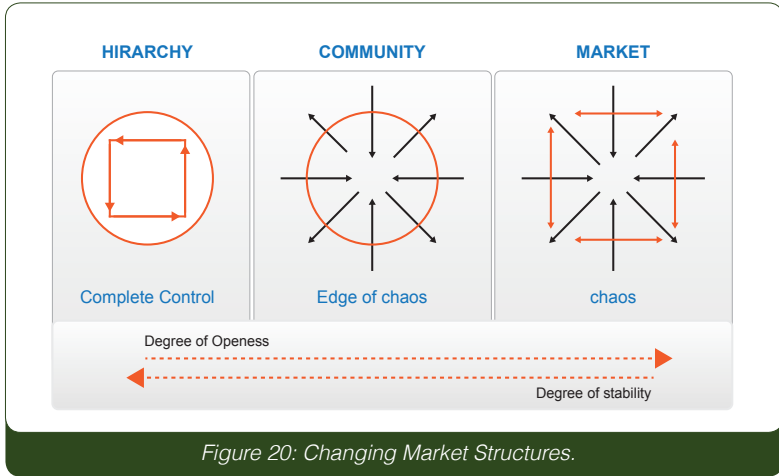


Figure 20: Changing Market Structures.

Governments need to take into consideration the three dimensions of change associated with any new technology: long-term versus short-term impact, big versus little shifts, and technocratic versus political and institutional alterations (West, 2004). Given the complexity of change assessments, it is indeed a difficult exercise to determine how much innovation and how long a period of time is required before something can be considered a “complete change in character, and condition,” something that is classically defined as a transformation (West, 2004).

In simple terms, there are five phases of e-government transformation that practitioners need to comprehend, as depicted in Figure 21. Essentially, governments start with a presence on an electronic channel, disseminating information. They move through the maturity stages to reach a utopic state where the citizens are fully empowered and are fully participative in the governing process. While this ideal state is far from reality, the information, interaction, transaction, and involvement stages are a reality within the grasp of implementation. While the level of involvement itself is a function of the type of government in place in a country and is political in nature, the other three stages—information, interaction, and transaction—are commercial in nature and are driven by economic considerations.

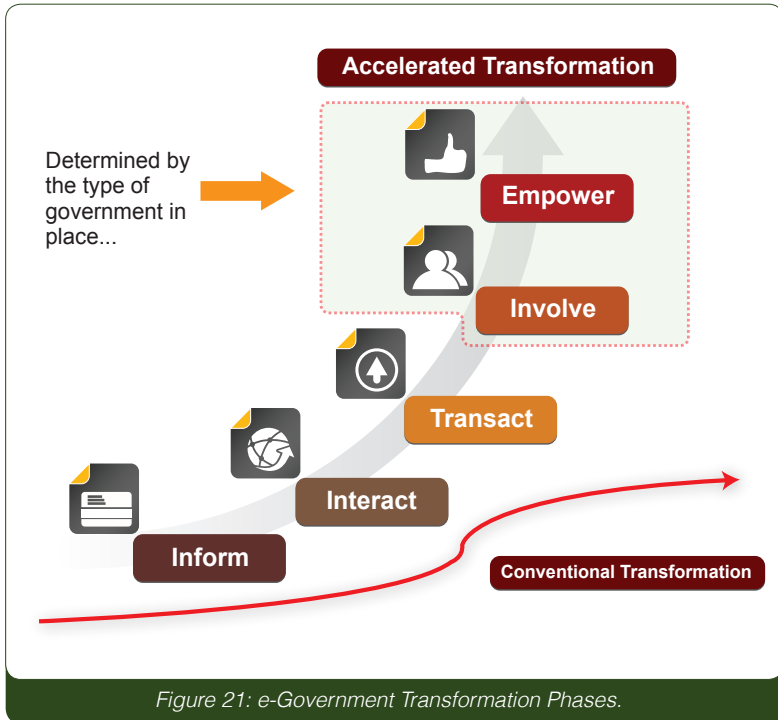


Figure 21: e-Government Transformation Phases.

Having said that, we need to spend some quality time to try to teach those around us that e-government is not just about enabling existing processes and using digital means, but rather about rethinking and transforming the ways government institutions operate, with the citizens' benefits and expectations at the core of such re-conceptualization (Capannelli, 2013). Only then may see some success stories of electronic services and transactions crossing boundaries of different government institutions, agencies, and departments. We should also then see some similar stories of vertical and horizontal integration between government systems. Until then, let us do the homework of changing the mindsets of those around us!

6.1 Limitations & Directions for Future Research

The impact of technological development trends and the concept of mobility will have significant impacts on how businesses in both government and the private sector are designed and perform. The ultimate goal in the field of practice will always be focused on achieving higher levels of responsiveness, efficiency, and effectiveness. In light of the evolving technological enablers, the game of change for the better and hence the continuous development of efforts will never end. To avoid re-inventing the wheel, governments and private sector organizations need to share and publish more insightful data about their practices but in a more useful way, i.e., not limiting their reports and published articles to show only the rosy side of what was successfully implemented. Also, organizations must aim to build a more comprehensive body of knowledge around the field of practice. There are few qualitative case studies from within organizations specifically in the government sector. This raises a call for further research and investigation. Future research, for example, could be conducted in order to verify the trends identified in this study. Conceivably, some more qualitative case studies of government practices from both emerged and emerging market countries will be useful. Perhaps research from emerging markets is more appealing as organizations in these countries are likely to be interested in innovation and creativity to better position themselves for economic competitiveness and growth.

References

Abdul, S. (2013) Bring Your Own Device (BYOD) – Provides Tremendous Boost In Employee Satisfaction. Content Loop. <http://www.content-loop.com/bring-your-own-device-byod-provides-tremendous-boost-in-employee-satisfaction/>

Al-Khouri, A.M. & Bal, J. (2007). Electronic Government in the GCC Countries. International Journal of Social Sciences, 1(2), 83-98. <http://www.waset.org/journals/ijhss/v1/v1-2-13.pdf>

Al-Khouri, A.M. (2012). eGovernment Strategies: The Case of the United Arab Emirates. European Journal of ePractice, 17, 126-150. http://www.epractice.eu/files/Journal_Volume_17-Part11_0.pdf

Al-Khouri, A.M. (2012a). Population Growth and Government Modernisation Efforts. International Journal of Research in Management & Technology, 2(1), 1-8. <http://www.ircast.org/ijrmt/papers/Vol2no12012/1vol2no1.pdf>

Al-Khouri, A.M. (2012b). PKI in Government Digital Identity Management Systems. European Journal of ePractice, 4, 4-21. http://www.epractice.eu/files/Journal_Volume_14_FINAL_28.2.2012_Part3.pdf

Al-Khouri, A.M. (2013). e-Government in Arab Countries: A 6-Stage Roadmap to Develop the Public Sector. Journal of Management and Strategy, 4(1), 80-107. <http://www.sciedu.ca/journal/index.php/jms/article/view/2433/1347>

Andersen, K.V., Henriksen, H.Z. (2005). The First Leg of E-government Research: Domains and Application Areas 1998-2003. Center for Research on IT in Policy Settings (CIPS), Department of Informatics, Copenhagen Business School. <http://www.researchgate.net>

APT. (2012). E-Government Implementation in Asia-Pacific Developing Countries and Its Challenges and Obstacles. ASTAP Working Group on Policies, Regulatory and Strategies. Asia-Pacific Telecommunity. <http://www.apr.int/sites/default/files/Upload-files/ASTAP/Rept-5-e-Govt.pdf>

Archer, G. (2003). Big Data Strategy – Issues Paper. AIIA Big Data Summit. Australian Government: Department of Finance and Deregulation. <http://agimo.gov.au/files/2013/03/Big-Data-Strategy-Issues-Paper1.pdf>.

Aruba Networks (2012). BYOD Adoption is Growing Amongst EMEA Enterprises. <http://www.arubanetworks.com/news-releases/byod-adoption-is-growing>

Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal. <http://www.rfidjournal.com/articles/view?4986>

Atkinson, R. (2003). *Network Government for the Digital Age*. Washington: Progressive Policy Institute.

Azoff, M. (2013). Mobile app development takes center stage as BYOD adoption increases. OVUM. <http://ovum.com/2013/05/22/mobile-app-development-takes-center-stage-as-byod-adoption-increases/>

Barbier, J., Bradley, J., Macaulay, J., Medcalf, R. and Reberger, C. (2012). *BYOD and Virtualization: Top 10 Insights from Cisco IBSG Horizons Study*. Cisco. <http://www.cisco.com/web/about/ac79/docs/BYOD.pdf>

Baum, C. and Di Maio (2000). *Gartner's Four Phases of E-Government Model*. Gartner Group. <http://www.gartner.com>

Bender, A. (2013). Australian government to write big data strategy. http://www.cio.com.au/article/456202/australian_government_write_big_data_strategy

Bornstein, D. (2012). Social Change's Age of Enlightenment. <http://opinionator.blogs.nytimes.com/2012/10/17/social-changes-age-of-enlightenment>

Brown, M.M. (2003). *Electronic Government*. In Jack Rabin (ed.). *Encyclopedia of Public Administration and Public Policy*, Marcel Dekker, 427–432.

Capannelli, E. (2013). *eGovernment Transformation: From Nice-to-Have to Must-Have*. <http://www.worldbank.org/en/news/speech/2013/05/31/speech-eGovernment-transformation>

Cattie, C. and Riper, K. (2013). From big data to better decisions. *The Business of Federal Technology*. <http://fcw.com/articles/2013/03/29/comment-ceb-big-data-decisions.aspx>

Cave, J. and Simmons, S. (2007). *Innovative and adaptive pan-European services for citizens in 2010 and beyond: Domain Mapping and Impacts*. European Commission, Information Society & Media DG. http://www.euregov.eu/deliverables/reports/eGov_WP1_D1_domain_mapping.pdf

CDT (2002). *The E-Government Handbook for Developing Countries*. infoDev, Center for Democracy Technology, Washington, DC. www.cdt.org/egov/handbook

Chakravarti, B. and Venugopal, M. (2008). *Citizen Centric Service Delivery through e-Governance Portal*. A White Paper published by National Institute for Smart Government, Hyderabad, India http://www.nisg.org/knowledgecenter_docs/D01010001.pdf

Chakravorti, B. (2003). *The Slow Pace of Fast Change: Bringing Innovations to Market in a Connected World*. Harvard Business Review Press.

Christensen, C.M. (1997). *The innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston, Massachusetts: Harvard Business School Press.

Chui, M., Löffler, M. and Roberts, R. (2010). *The Internet of Things*. McKinsey Quarterly. http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things

Clayton, H.M. (2003). *The Innovator's Solution: Creating and Sustaining Successful Growth*. Harvard Business Press.

Clifford, S. (2012). *Social Media Are Giving A Voice to Taste Buds*. NYTimes.com, 30 July 2012. http://www.nytimes.com/2012/07/31/technology/facebook-twitter-and-foursquare-as-corporate-focus-groups.html?_r=0

Colesca, S.E. (2009). *Increasing e-Trust: A Solution to Minimize Risk in e-Government Adoption*. *Journal of Applied Quantitative Methods*, 4(1), 31-44. <http://jaqm.ro/issues/volume-4,issue-1/pdfs/colesca.pdf>

Collier, D. (2012). *2012 Federal Cloud Review*. <http://cagw.org/sites/default/files/pdf/issue-brief-2012-12-cloud-report-web.pdf>

Davenport, T.H. and Patil, D.J. (2012). *Data Scientist: The Sexiest Job of the 21st Century*. *Harvard Business Review*, October, p. 2. <http://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century/ar/1>

De, R. (2004). *E-Government Systems in Developing Countries: Some Research Issues*. PreICIS workshop on eGovernment, Washington, December.

Deloitte. (2013). *Tech Trends 2013: Elements of Post-digital*. <http://www.deloitte.com/assets/Dcom-UnitedKingdom/LocalAssets/Documents/Services/Consulting/uk-c-tech-trends-2013-full-report.pdf>

Detica. (2011). *The cost of cyber crime: a Detica report in partnership with the office of cyber security and information assurance in the cabinet office*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Devadoss, P.R., Pan, S.L., and Huang, J.C. (2002). *Structurational Analysis of e-Government Initiatives: a Case Study of SCO*. *Decision Support Systems*, (34), 253-269.

Dombrowski, P. and Gholz, E. (2009). *Identifying Disruptive Innovation: Innovation Theory and the Defense Industry*. *Innovations*, 4(2), 101-117. http://www.utexas.edu/lbj/archive/news/images/file/INNOVATIONS-4-2_dombrowski-gholz.pdf

Drury, A. and Absalom, R. (2013). *BYOD: an emerging market trend in more ways than one*. [http://www.logicalis.com/pdf/Logicalis White Paper Ovum\(2\).pdf](http://www.logicalis.com/pdf/Logicalis%20White%20Paper%20Ovum(2).pdf)

Eggers, W.D. and Jaffe, J. (2013). Gov on the go: Boosting Public Sector Productivity by Going Mobile. Deloitte University Press. <http://dupress.com/articles/gov-on-the-go>

Erl, T., Puttini, R. and Mahmood, Z. (2013). Cloud Computing: Concepts, Technology & Architecture. Prentice Hall.

European Commission. (2005). Information Society - eEurope 2005. http://europa.eu.int/information_society/eeurope/2005/index_en.htm

Evans, D. (2011). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco Internet Business Solutions Group (IBSG). http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Ferguson, R.B. (2012). It's All About the Platform: What Walmart and Google Have in Common. MIT Sloan Management Review, December 5. <http://sloanreview.mit.edu/improvisations/2012/12/05/its-all-about-the-platform-what-walmart-and-google-have-in-common>

Field, T., Mield, T., Muller, E. and Law, E. (2003). The e-Government Imperative. Organization for Economic Co-operation and Development, ISBN 92-64-10117-9, Paris, France, 2003. <http://213.253.134.43/oecd/pdfs/browseit/4203071E.PDF>

Furman, S. (2009). Building Trust. <http://www.usability.gov/articles/092009news.html>

Gilbert, J. (2012). Confronting Disruptive Innovation. <http://www.lexicon-systems.com/pubs/itinsight/ITInsight1212.pdf>.

Government Business Council (2013). Turning Optimism into Reality: How Big Data Is Transforming Government. http://cdn.govexec.com/media/gbc/docs/gbc_bah_big_data_lake_insight_report_pub.pdf

Grandy, D. and Newman, D. (2013). Smartphones and even smarter government. The Age National. <http://www.theage.com.au/national/public-service/smartphones-and-even-smarter-government-20130503-2iz41.html>

Grönlund, Å. (2002). Electronic Government – Design, Applications, and Management. Hershey, PA: Idea Group.

Grönlund, A. and Horan, T.A. (2004). Introducing e-Gov: History, Definitions, and Issues. Communications of the Association for Information Systems, 15, 713-729.

Hammer, M. and Champy, J. A. (1993). Reengineering the Corporation: A Manifesto for Business Revolution. New York: Harper Business Books.

Hang, C., & Kohlbacher, F. (2008). Disruptive innovations and the greying market. Industrial Engineering and Engineering Management Conference, 2-4 December 2007, 1915-1919.

Hay, M. (2003). Managing Big Data. eGov. <http://egov.eletsonline.com/2013/01/managing-big-data/#sthash.hbzcIbDJ.dpuf>

Hayes, B. and Kotwica, K. (2013). Bring Your Own Device (BYOD) to Work: Trend Report. Elsevier.

Heeks, R. (2002). Informaiton Systems and Development Countries; Failure, Success and Local Improvisation. The Information Society, 18(2), 101-112.

Heeks, R. (2003). Most eGovernment for Development Projects Fail: How can Risks be Reduce?. iGovernment Working Paper Series, Paper no. 14. Manchester: Institute for Development Policy and Management.

Heeks, R. (2006). Analysing the Software Sector in Developing Countries Using Competitive Advantage Theory. Development Informatics Working Paper Series, No.25/2006. Manchester: Institute for Development Policy and Management.

Hughan, K. (2013). Mobile App Adoption is on the Rise, But Not All Retailers Have Caught Up. <http://www.themobileretailblog.com/mobile-commerce-strategies/mobile-app-adoption-is-on-the-rise-but-not-all-retailers-have-caught-up>

IDC. (2013). IDC Predictions 2013: Competing on the 3rd Platform. <http://www.idc.com/research/Predictions13/downloadable/238044.pdf>

Issenberg, S. (2012). How President Obama's Campaign Used Big Data to Rally Individual Voters, Part 1. MIT Technology Review, December 16. <http://www.technologyreview.com/featuredstory/508836/how-obama-used-big-data-to-rally-voters-part-1>

Johnson, M. (2011). Mobile Device Management: What you Need to Know for IT Operations Management. Tebbo.

Kalba, K. (2008). The Global Adoption and Diffusion of Mobile Phones. Harvard University. http://www.pirp.harvard.edu/pubs_pdf/kalba/kalba-p08-1.pdf

Kim, W. C., & Mauborgne, R. (2005). Blue Ocean Strategy – How to Create Uncontested Market Space and Make the Competition Irrelevant. Boston, MA: Harvard Business School Publishing.

Klett, G. and Kersten, H. (2012). Mobile Device Management. Verlag: MIT Publishing.

Konkel, F. (2003). Bullish on big data? Better make a plan. <http://fcw.com/Articles/2013/04/01/big-data-booz-allen.aspx?Page=1>

Layne, K and Lee, J. (2001). Developing Fully Functional e-Government: A four Stage Model'. *Government Information Quarterly*, 18(2), 122-136.

Ludwig, S. (2012). VentureBeat: Study: Mobile app usage grows 35%, TV & web not so much. <http://venturebeat.com/2012/12/05/mobile-app-usage-tv-web-2012/>

Manifesto, C. (1999). *Social Business Process Reengineering*. Harvard Business Review. <http://socialbusinessmanifesto.com/social-business-process-reengineering/>

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. and Byers, A.H. (2011). Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute. http://www.mckinsey.com/~media/McKinsey/dotcom/Insights_and_pubs/MGI/Research/Technology_and_Innovation/Big_Data/MGI_big_data_full_report.aspx

Mayer-Schonberger, V. and Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Eamon Dolan/Houghton Mifflin Harcourt.

McMillan, S. (2010). Legal and Regulatory Frameworks for Mobile Government. Proceedings of mLife 2010 Conferences. October 27-29, Brighton UK. <http://www.egov.vic.gov.au/trends-and-issues/mobile-government/legal-and-regulatory-frameworks-for-mobile-government.html>

Meeker, M. (2010). *Internet Trends*, Morgan Stanley. [http://www.sherpalo.com/resources/INTERNET_TRENDS_RI_041210\[1\].pdf](http://www.sherpalo.com/resources/INTERNET_TRENDS_RI_041210[1].pdf)

MobiThinking. (2013). Global mobile statistics 2013 Section E: Mobile apps, app stores, pricing and failure rates. <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/e#appusers>

Mukherjee, K. and Sahoo, G. (2010). Cloud Computing: future Framework for eGovernance. *International Journal of Computer Applications*, 7(7), 31-34.

Naseem, S. (2012). Cloud Computing and E-Governance. *International Journal of Scientific & Engineering Research*, 3(8), 1-6.

Navarrete, C. (2010). Trust in E-Government Transactional Services: A Study of Citizens' Perceptions in Mexico and the U.S. Proceedings of the 43rd Hawaii International Conference on System Sciences – 2010. <http://www.computer.org/csdl/proceedings/hicss/2010/3869/00/04-05-07.pdf>

NIST. (2010). Definition of Cloud Computing. National Institute of Standards and Technology (NIST). <http://csrc.nist.gov/groups/SNS/cloud-computing>

Norton. (2012). 2012 NORTON Cybercrime Report. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

OECD (2009). A Paradigm Shift Towards Citizen Centricity. OECD, Rethinking e-Government Services: User-Centred Approaches. OECD Publishing. doi: 10.1787/9789264059412-2-en

Olson, P. (2013). 10 Predictions For The Mobile Industry In 2013. Forbes. <http://www.forbes.com/sites/parmyolson/2013/01/02/10-predictions-for-the-mobile-industry-in-2013/>

Paap, J. and Katz, R. (2004). Anticipating Disruptive Innovation. Research Technology Management. <http://www.jaypaap.com/articles/Paap-Katz-Disruptive%20Innovation-sep-04-p13-mod.pdf>

Perez, S. (2012). comScore: In U.S. Mobile Market, Samsung, Android Top The Charts; Apps Overtake Web Browsing. <http://techcrunch.com/2012/07/02/comscore-in-u-s-mobile-market-samsung-android-top-the-charts-apps-overtake-web-browsing/>

Piao, M. and Okhuysen, G. (2012). Reexamining the Paradox of Sustaining Innovation and Disruptive Innovation. https://www.sbrconferences.com/uploads/Nash2012-Piao_Ming.pdf.

Ponemon. (2012). 2012 Cost of Cyber Crime Study: United States, Benchmark Study of U.S. Companies, Ponemon Institute, Michigan, USA http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6.pdf

Raftery, T. (2012). Sustainability, Social Media and Big Data. The Energy Collective, 2 November. <http://theenergycollective.com/tom-raftery/138166/sustainability-social-media-and-big-data>

Rahav, A. (2011). From user centricity to Citizen Centricity. <http://www.icentered.com/from-user-centricity-to-citizen-centricity>

Rannu, R., Saksing, S., Mahlakõiv, T. (2010). Mobile Government: 2010 and Beyond White paper. European Union Regional Development Fund. [http://www.mobisolutions.com/files/Mobile Government 2010 and Beyond v100.pdf](http://www.mobisolutions.com/files/Mobile%20Government%202010%20and%20Beyond%20v100.pdf)

Redman, P., Girard, J. and Wallin, L. (2011). Magic Quadrant for Mobile Device Management Software. Gartner, http://www.sap.com/campaigns/2011_04_mobility/assets/GartnerReport_MDM_MQ_April2011.pdf.

Robb, D. (2006). Balancing Sustaining and Disruptive Innovation. Center for Corporate Renewal. [http://www.ctrforcorporaterenewal.com/docs/Balancing Sustaining and Disruptive Innovation.pdf](http://www.ctrforcorporaterenewal.com/docs/Balancing_Sustaining_and_Disruptive_Innovation.pdf)

Sarah, R. (2013). BYOD Recommendations and Dilemmas. Government Technology. <http://www.govtech.com/education/BYOD-Recommendations-and-Dilemmas.html>

Satyanarayana, J. (2004). E-Government: The Science of the Possible. India: Prentice Hall.

Scholl, H.J. (ed.) (2010). E-Government: Information, Technology, and Transformation. Armonk, N.Y.: M.E. Sharpe.

Seifert, J.W. (2003). A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance. <http://www.fas.org/sgp/crs/RL31057.pdf>

Shailendra, C. Palvia, J. and Sharma, S.S. (2007). E-Government and E-Governance: Definitions/Domain Framework and Status around the World. Foundations of E-government. http://www.iceg.net/2007/books/1/1_369.pdf

Simic, K., Dadic, J., Paunovic, L., Milutinovic, M., Bogdanovic, Z. (2012). Delivering Mobile Government Services Through Cloud Computing. http://www.fos.unm.si/media/pdf/Delivering_Mobile_Government_Services_Through_Cloud_Computing_maj.pdf

Simon, P. (2013). Too Big to Ignore: The Business Case for Big Data. Wiley.

Stanforth, C. (2010). Analysing e-Government Project Failure: Comparing Factoral, Systems and Interpretive Approaches. Centre for Development Informatics, Manchester, UK. <http://www.sed.manchester.ac.uk/idpm/research/publications/wp/igovernment/documents/iGovWkPpr20.pdf>

Su, C., China, W. and Pei, Z. (2010). Application Model of Mobile E-Government in Wuhan Urban Circle. IEEE International Conference on Multimedia Information Networking and Security (MINES), Nanjing, Jiangsu, 738 – 741.

Symantec. (2012). State of Mobility Survey. Symantec Corporation. http://www.symantec.com/content/en/us/about/media/pdfs/b-state_of_mobility_survey_2012.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Feb_worldwide_StateofMobility

Tellis, G.J. and Golder, P.N. (2003). First to Market, First to Fail? Real Causes of Enduring Market Leadership. In R. Katz (ed.) The Human Side of Managing Technological Innovation. New York: Oxford University Press.

Thames, C. (2011). Business Process Reengineering & Enterprise Collaboration. http://www.istryve.com/images/stories/Stryve_Advisors_Social_BPR.pdf

Thys, G. and Lacourt, S. (2013). Mobile Payments: Three Steps to NFC Testing Success (White Paper). <http://www.nfcworld.com/wp-content/uploads/2013/05/>

clear2pay-nfc-mobile-payments-testing-0205.pdf

UNDESA. (2003). e-Government at the Crossroads. World Public Sector Report 2003. United Nations Department of Economic and Social Affairs. United Nations, New York.

UNDESA. (2003). UN Global e-government survey. UNDESA, Division for Public Administration and Development Management, Department for Economic and Social Affairs – UNDESA. <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan016066.pdf>

van Duivenboden, H.P.M. (2002). Citizen Participation in Public Administration: The Impact of Citizen Oriented Public Services on Government and Citizen, paper presented at the eGovernment Working Group of OECD Public Management Service (PUMA): Paris (March 2002).

Veljanovska, K., Zdravevska, V. (2013). E-Government Based on Cloud Computing. Journal of Emerging Trends in Computing and Information Sciences, 4(4), 377-381.

Warkentin, M., Gefen, D., Pavlou, P.A and Rose, G.M. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. Electronic Markets, 12(3), pp.157-162.

West, D.M. (2004). e-Government and Transformation of Service Delivery and Citizen Attitudes. Public Administration Review, 64(1), pp. 15-27.

Whitfield, K. (2013). Fast growth of apps user base in booming Asia Pacific market. Portio Research. <http://www.portioresearch.com/en/blog/2013/fast-growth-of-apps-user-base-in-booming-asia-pacific-market.aspx>

Wiech, D. (2013). "The Benefits and Risks Of BYOD. Manufacturing Business Technology. <http://www.mbtmag.com/articles/2013/01/benefits-and-risks-byod>

World Bank. (2011). Definition of E-Government. <http://go.worldbank.org/M1JHE0Z280>

Yiu, C. (2012). The Big Data Opportunity: Making Government Faster, Smarter and More Personal. Policy Exchange. http://www.policyexchange.org.uk/images/publications/the_big_data_opportunity.pdf

Zarei, B., Ghapanchi, A & Sattary, B. (2008). Toward national e-government development models for developing countries: A nine stage model. The International Information and Library Review, 40(1), 199-207.

Zink, T. (2012). The Pros and Cons of BYOD (Bring Your Own Device). CircleID. http://www.circleid.com/posts/20121010_the_pros_and_cons_of_byod_bring_your_own_device/

2

Exploring the Role of Technology in a Joined up Government:

A Proposed Framework for National-Level Service¹

Abstract

The current economic and social environment is pushing governments to transformational change in order to meet increasing public expectations of public-sector value and cost effective outcomes. Modern information and communication technology (ICT) has shown its potential to enable government service availability and delivery, but governments are relying on their agencies to create their own value systems without reference to national-level service and value oriented agendas. This article explores the role of technology in developing more effective and joined up government. It proposes a framework for governments and policy makers to guide them in the field of service provision and overall governance. The components of the proposed framework reflect fields of practice that in which governments should engage to ensure that their agencies comply with strategic national information technology (IT) objectives.

Keywords: *joined up government, eGovernment, citizen centricity, service governance, service quality, TQM.*

2

¹ Please quote this article as follows:
Al-Khoury, A.M. (2013) "Exploring the Role of Technology in a Joined up Government: A Proposed Framework for Service Governance", *International Journal of Electronic Governance and Research*, Vol. 2, No. 2, pp. 196-204.

1. Introduction

The situation in the world today is dynamic and full of uncertainty. Governments are faced with multiple, complex and multi-disciplinary challenges. During the last decades of the twentieth century, the world witnessed the emergence of new political, social, technological and economic environments. Societies today are demanding new forms of governance, to allow greater scope for democracy, decentralization, participation and pluralism [1]. Globalization is shaping the world economy, and the current information revolution is resulting in a knowledge-based society (ibid.).

A recent survey conducted by Accenture revealed that efficiency targets, demands for improved services and cost pressures top the list of key challenges facing governments today [2]. See also Fig. 1.

Governments around the world have invested heavily in ICT in the past two decades, especially in e-government programs aiming to increase internal efficiency and service levels to constituents. However, almost few e-government programs around the globe have realized their full potential. An interesting model presented by Gartner [3] shows how the evolution of new technologies has been associated with excessive enthusiasm and media attention, followed by corrective public disillusionment, leading on overtime, for some technologies at least, to the gradual restoration of public expectation, with consequent realization of mass market business benefits. See Fig. 2.

Researchers argue that governments today need to make more effective use of new technologies to enable transformation and to “join up”² services. Governments should aim to integrate processes and deliver seamless services across the boundaries of their agencies (e.g. [4]-[8]). Governments have been relying on their agencies to create their own value systems without national-level service and value oriented agendas. E-government initiatives have been focusing on somewhat narrow sets of objectives that focus on quick wins, automation of some internal processes and the introduction of poorly integrated online services.

² The term «joined-up government» was coined several years ago in the United Kingdom, when Prime Minister Tony Blair presented the first U.K. e-government strategy. This strategy's goal was to «join up» electronic services by 2005. Since then, the term has been widely used worldwide to describe the integration of services, processes, systems, data and applications necessary to achieve a seamless, citizen-centered government.

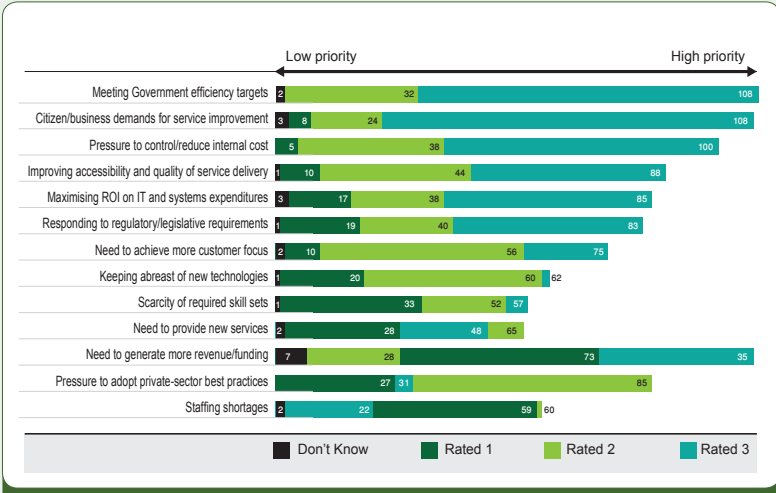


Fig. 1. Accenture survey results on key government challenges

2

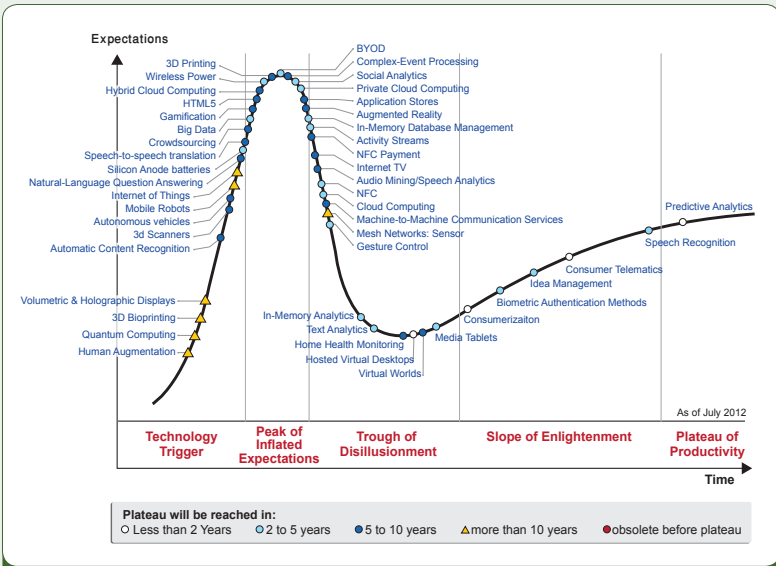


Fig. 2. Gartner Hype Cycle of New Technologies

The aim of this article is to explore the potential role of ICT in enabling and building a joined-up and more responsive government. It calls for national-level governance initiatives to ensure alignment of all government agencies. A simplified framework is proposed to guide governments and policy makers in fields of service provision and overall IT governance. The components of the proposed framework reflect fields of practice in which governments should engage to ensure that their agencies comply with strategic and national information technology (IT) objectives.

This paper is organized as follows: Section 2 discusses the evolution of citizen centered governments, and how public service delivery is being shaped; Section 3 provides an overview of a conceptual government maturity model and the concept of a 24-hour available government; Section 4 explores the role of ICT in supporting the development of enhanced government capacities; Section 5 highlights the need to develop knowledge of and engage with customers in order to sustain competitive advantage and fulfill government responsibilities; Section 6 discusses the link between service quality and the need for supporting technologies to create an acceptable degree of trust in the emerging communication channels for service delivery; Section 7 presents the proposed service governance framework and discusses its components; Section 8 concludes the article, summarizing the new perspectives generated.

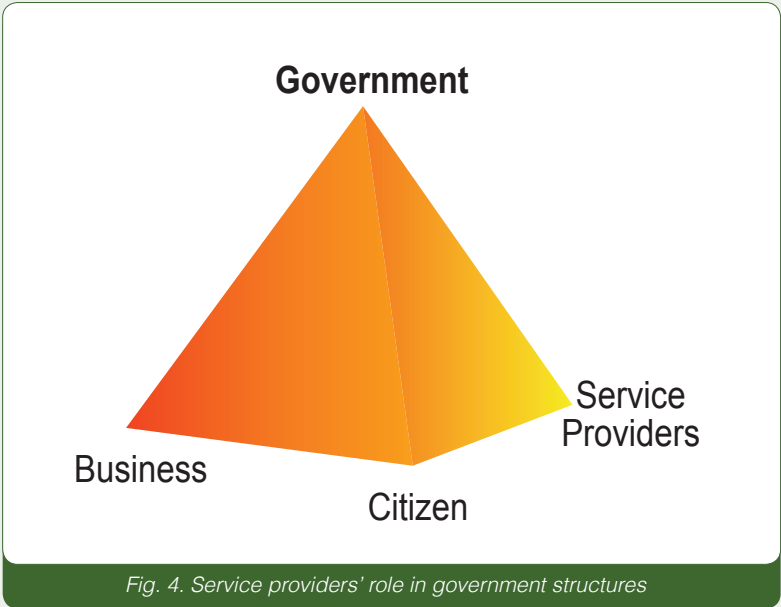
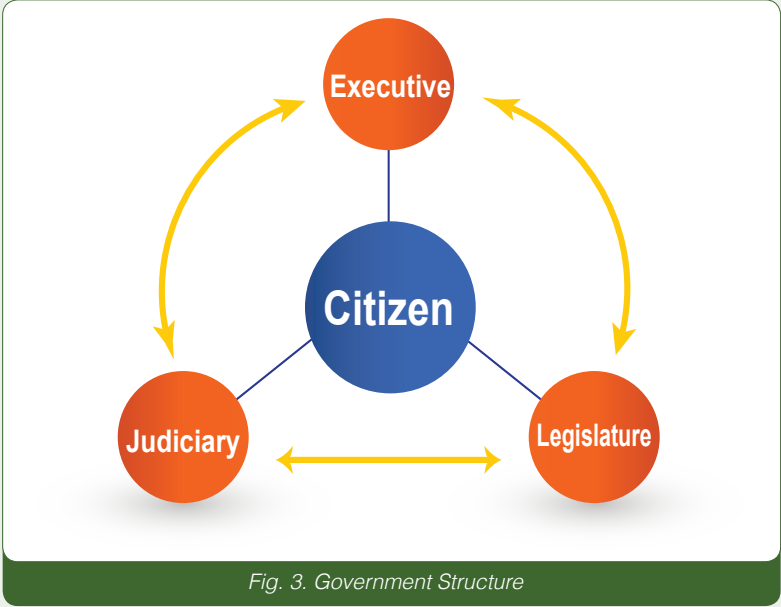
2. Service Oriented Government

Governments, globally, have been striving to transform themselves to fit with more service oriented, citizen centered models (e.g. [9]-[12]). This paradigm shift in the orientation of governments is bringing change in the ways citizens interact with their governments. Citizens are being transformed from human entities to 'e' entities, commonly referred to in the literature as the 'e-citizens'. Rapid advancements and revolutionary changes in Information and Communication Technologies (ICT) have helped governments to take proactive steps in this transformation.

Regardless of the form, be it a Monarchy, a Democracy, or a Communist state, a modern government incorporates three pillars of society: (1) the Executive: representing the rulers, (2) the Judiciary: administering the legal system, and (3) the Legislature of law makers. See also Fig. 3. These three pillars are established to ensure the safety and security of their residents and citizens. A good government thus has the citizen as the center of its focus.

Conventionally, governments have been represented in the context of the citizens and businesses forming a triad. A key entity that is often missed out is the service provider. See also Figure 4. The service providers are the locus of interaction between the government, businesses and citizens. Service providers include telecommunication providers, electricity and water providers, transport providers, etc. Their services range from provision of basic infrastructure to offering luxurious living conditions. The service providers are positioned in Fig. 4 so as to transform the triadic structure into an interactive pyramid.

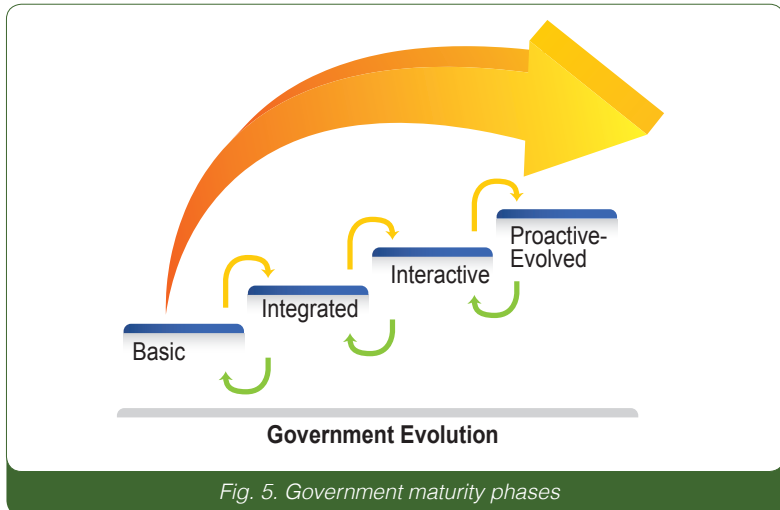
It is extremely important to understand the role of the government in the citizen context. Governments go about their tasks differently in the way they service individuals separately and the nation and collectively. It is important to understand this difference. This has a direct bearing on how individuals should view the government' responsibilities and those of the providers enabling service delivery (e.g. [13]-[14]).



3. Government Maturity

As governments strive to discharge their responsibilities and fulfill their tasks, they evolve structurally, building on their own infrastructure to levels of operational maturity. There are four stages of this maturational model as represented in Fig. 5: (1) Basic, (2) Integrated, (3) Interactive and (4) Proactive. At the basic level, the government fulfills its duties and goes about its tasks, each department of government independently providing services. At the Integrated stage the different government departments begin to integrate through data sharing processes. As systems evolve further, business processes and their applications integrate to provide interactive services with increased citizen participation in government. The most evolved government would be one offering its services with 24-hour availability government and the citizen, as its central focus, given a say in all the administrative processes that affect daily life. This model such an evolution brings me to the present focus one-Government.

In the e-Government context, integration and citizen participation are functions of the availability of the government for citizens. Greater availability would imply more citizen participation. More participation would mean a more pro-active government, sharing the responsibilities and duties with its citizens and ensuring delivery of quality services to citizens to improve quality of life [13,15]. Let us explore the role of ICT in its government context in the following section.



4. ICT Role In Government

The role of ICT in government transformation and evolution cannot be overstated. Let us look at an example of government practice in this domain. Fig. 6 depicts a diagram developed by the European Commission that illustrates the role of ICT in enabling various e-government models for the European Union (EU) in 2020 [16]. It illustrates the projected adoption of technology in six distinct stages. The first stage concentrates on the development of a clear taxonomy of value-based government roles and the identification of key areas of transformation where ICT can make a substantial impact. The second stage involves identifying 'promising' technologies that may contribute to the enhancement of (future) governmental tasks and activities. The third stage represents the identification of what have been labeled the 'hot spots' of government transformation. This stage should result in the identification and clustering of combinations of roles and technologies in various 'hot spots'.

The fourth stage depends upon the way future trends manifest themselves. They might present as scenarios in which the consequences of promising ICT-developments are actualized as new e-government services and new e-government models. These ICT innovation based service models might show themselves in the broader context of related social, economic, institutional and organizational trends. The fifth stage represents the future-oriented framework in which the benefits and impacts of e-government are measured. The sixth stage represents research work towards, and framing of, apt policy changes that enable successful e-transformation.

The components presented in the above diagram form the crux of this model for ICT in a government context. The model provides an archetype for government transformation and can inform long-term strategic planning. It can be applied to identify emerging trends and opportunities arising in the process of evolution of new information and communication technologies, in order to enhance government performance and capacity for governance in 2020 [16].

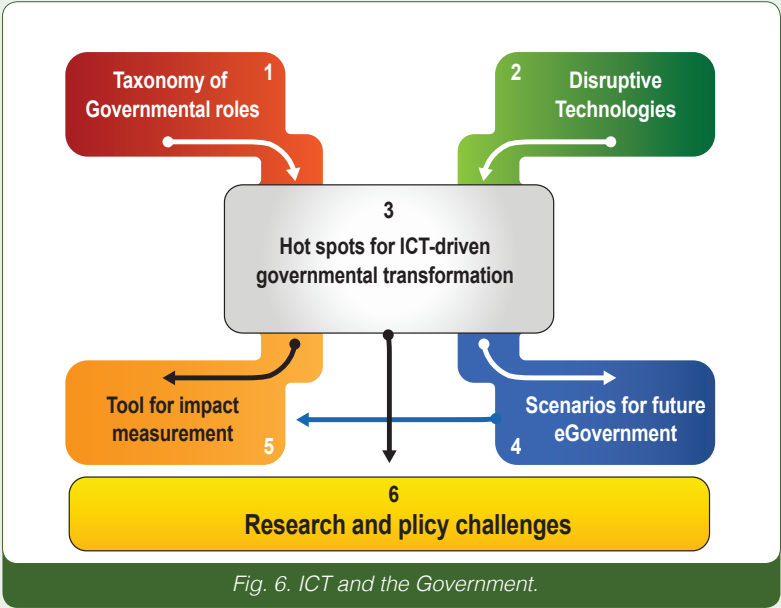


Fig. 6. ICT and the Government.

Source: [16]

5. The Transition To The Customer Age

In today's climate of political and socioeconomic change, communication is playing a decisive role in promoting development [1]. We are living in the age of information and its digital world of instant communication. The information revolution has dramatically increased the potential for sharing information across the globe [17]. This information age is now evolving.

The emergence of a series of new communications concepts and applications in this age of information revolution has created more opportunities and possibilities for both users and services providers. Forrester's research has identified this new age as the age of the customer [18]. See also Fig. 7. Forrester points out that the Age of Customer is not about 'customer-centricity' thinking or 'the customer is always right.' Rather, it is about the empowerment of customers so that focus on the customer now matters more than any other strategic imperative (ibid.).

Empowered customers are disrupting every industry. In this age of the customer, the only sustainable competitive advantage is knowledge of customers and engagement with them. Citizens are becoming more digitally aware. They are mobile in the digital world, and they have more power than ever before. The balance of power has shifted. With online reviews, social media, and smart phones, citizens know more about services, living standards, and how other governments operate. They share their opinions with their friends and the online community.

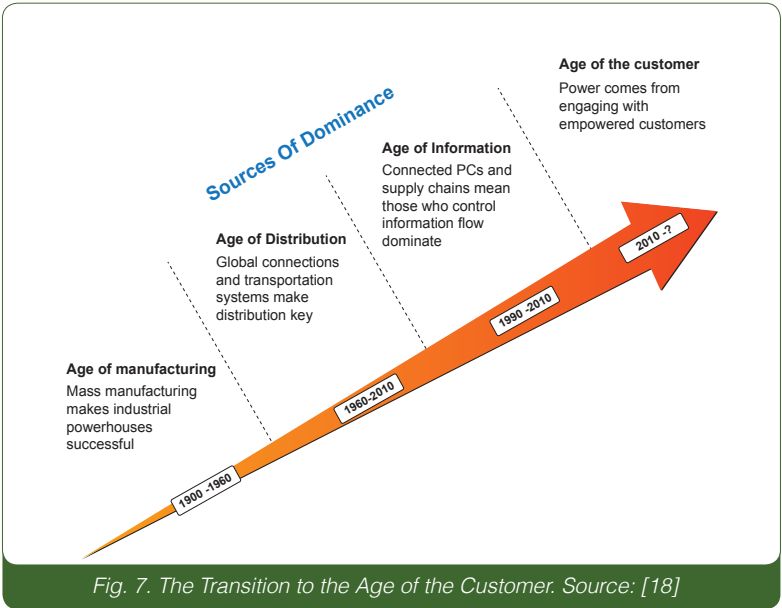
The world has been witnessing a paradigm shift in government, as governments are being prompted to adopt radical reform initiatives to in their redesign in order to address public needs and services from contemporary consumer perspectives. It is also pushing governments to give the nod to more innovative public management methods and tools in the public sector, thus creating a significant and sustainable impact through economic growth, better public services, higher government productivity and increased efficiency.

As new communication technologies are being developed and made more widely available, governments have withdrawn from certain functions that are now being taken over by private enterprise [1]. We have experienced in the recent past how interactions on social networks have transformed the societal outlook on government.

Government organizations in many parts of the world underwent dramatic transformation over the last two decades, becoming more citizen friendly and more importantly, available on demand. Many governments have adopted different channels of communication and setup their information networks to be directly accessible, at a click or a call, for their citizens. This has brought about a vast change in service availability and the quality of service.

In this age of the customer, governments are expected to reach out to their citizens and provide services on a personalized level [19]. Some argue that government priorities should be directed towards citizens and that governments should focus on the development of compelling business cases to support and create roadmaps for such transformation, showing measurable returns on the enhancement of service quality and capacity for delivery.

The next section of this paper discusses the link between public perceptions of service quality and the promotion of trust in technologies supporting service delivery.



Source: [18]

6. Government And Quality Of Service (Qos)

As governments transformed themselves and evolve into inclusive e-governments, quality models have evolved to measure the effectiveness and delivery of services (e.g. [20]-[23]). Service orientation has become critical in all aspects of today's organizations. Government quality programs in many countries around the world are actively promoting quality and excellence in operations, project outcomes and service delivery [24]. Excellence programs are perceived by governments as a tool to achieve sustainable growth and enhanced performance, create breakthroughs in public sector productivity, and boost engagement (e.g. [25]-[26]). The European Framework for Quality Management (EFQM) is one of the most common frameworks used in public and private sector organisations (e.g. [27]-[29]). Fig. 8 depicts the overall EFQM excellence model.

The foundation on which the European Foundation for Quality Management stands comes from the concept of Total Quality Management (TQM), management that seeks to deliver tangible improvements in quality of life for society as a whole and for individual citizens as beneficiaries and consumers of government products and services. TQM, and other concepts such as Customer Relationship Management (CRM) and Business Process Reengineering (BPR) are all seen as reform initiatives that have been used to achieve higher levels of quality in alignment with the New Public Management (NPM) approach (e.g. [30]-[33]). ICTs are central to these methodologies because of their utility in data collection and work flow structuring, and their ability to embed structure within newly designed work processes [32]. Technology plays a critically enabling role.

A result of the adoption of such technology is the vast improvement in the availability of various channels of interaction and service delivery for the citizens. See Fig. 9. This is facilitated by the implementation of different networks that enable communication and data exchange. See also Fig. 8. Enhancement of security systems has enabled the different networks to interact with each other to provide a rich, seamless environment for service delivery.

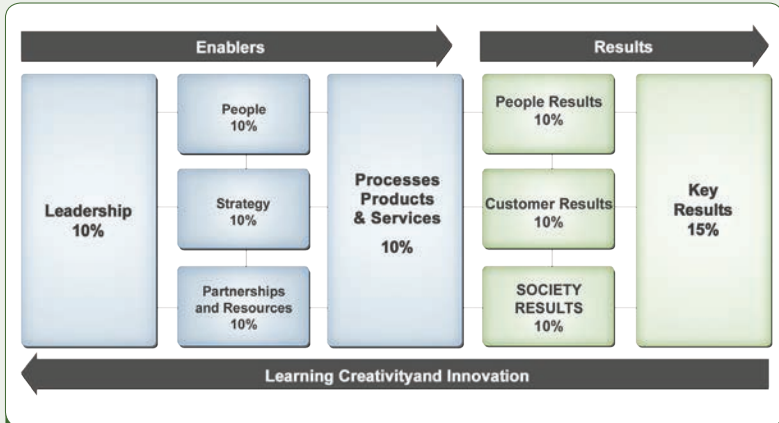


Fig. 8. Governments and the Quality of their Services

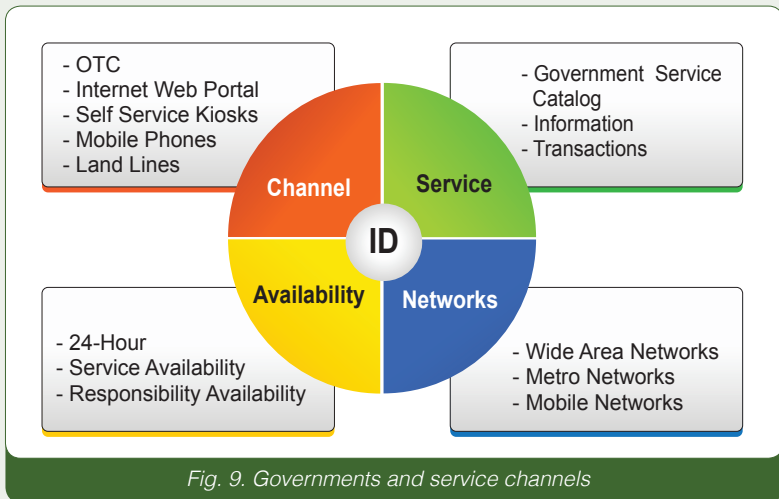


Fig. 9. Governments and service channels

The digital identity³ of the service beneficiary and the service provider is central to these processes. Trusted transactions are enabled by verified and authenticated digital identities. Digital identification technologies are envisaged to enable secure delivery of services to the correct beneficiaries with a clear audit trail [34]. The literature reports strong evidence of the use of digital identification technologies⁴ as effective tools in practice to lowering barriers in citizen access and for promoting equitable public service delivery (e.g. [34]-[38]).

Digital identification is seen as key foundation for governments to offer an increased portfolio of public services to citizens in an efficient and cost effective manner. Various forms of identification technologies have enabled citizens to access more joined-up and comprehensive services in one-stop-shops with a single website and telephone number, providing information and a single point of contact (e.g. [12],[34],[39]-[40]).

The matrix in Fig. 10 provides an overview of the interwoven technologies and the role of ICT in enabling the services and service delivery channels. With the integrated applications and networks, the citizen is provided with smart systems for interaction with the government across multiple channels.

We would like to emphasize the challenge posed by disruptive technologies. Evolving government's management of technology protects its investments, especially in the public service domain e.g., governments have invested vast multi protocol label switching (MPLS)⁵ networks for providing seamless communications experiences on phones and internet, combining the voice and data communications. Technologies such as voice over internet protocol (VoIP)⁶ have proven disruptive to

3 Digital Identity: refers to an identity in the domain of cyberspace. It encompasses a set of data & attributes that associates a person's to his/her digital identity and uniquely describes a person in electronic environments.

4 We refer here to Identity and Access Management (IAM) systems that are related to managing the critical function of authentication and authorization to access an organizations data and resources. Many governments have initiated identity management systems that involve smart cards, biometrics, and encryption technologies to authenticate their citizens' identities and improve public service delivery. See for example [24],[37].

5 MPLS is an abbreviation for Multiprotocol Label Switching. It is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols.

6 Voice over IP (VoIP, abbreviation of voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks. One of the biggest advantages of VoIP is that the telephone calls over the Internet do not incur a surcharge beyond what the user is paying for Internet access, much in the same way that the user doesn't pay for sending individual e-mails over the Internet.

conventional telecommunications. Tablets have disrupted the personal computing and communications domains.

Proper regulation of technology adoption thus is advocated to protect investments, citizens with freedom to choose their service channels, and improve customer satisfaction (e.g. [41]-[42]). Regulation of the adoption of technology supports the investment in it and enables citizens to obtain better services.

Contemporary audit trail⁷ systems and digital identification technologies are emerging as effective mechanisms to ensure that transactions can be carried out from anywhere, independent of geographic and time limitations. See for example: (e.g. [43]-[47]). Integrated processes for technical and business processes ensure that complicated transactions can be carried out quickly. This also enables us to track and maintain the service agreements with a very high level of assurance. Such technologies would enable higher levels of transparency in transactions and thereby assurance of the reliability of remote transactions is achieved.

Service Components	Technology Components		
	Voice Communications	Data Communications	Networking & Connectivity
Citizen Contact	- Voice Over IP - IVR	- SMS - e-mail - Web Portal - Kiosks	Unified Networks & Communications
Service Catalog Citizen Transactions Issues & Complaints General Information	Speech Applications	- CRM Application - Web Services - Service Oriented Architecture, & Business Process Integration - Relational Databases	Social Networking
Backend Data	Network Connectivity & Applications for Business Process Automation		
Service Delivery Channels	- Phones - Mobiles - VOIP	- SMS - IInternet Kiosks - web portals	- Social Network Channels
Analytic	Analytical Tool with embedded Business Intelligence (Data warehousing & Data Mining)		

Fig. 10. ICT as the enabler for Channel Integration

⁷ An audit trail (or audit log) is a security-relevant chronological record(s) that provides documentary evidence of the sequence of activities that have affected a specific operation, procedure, or event at any given time.

7. The Proposed Service Governance Framework

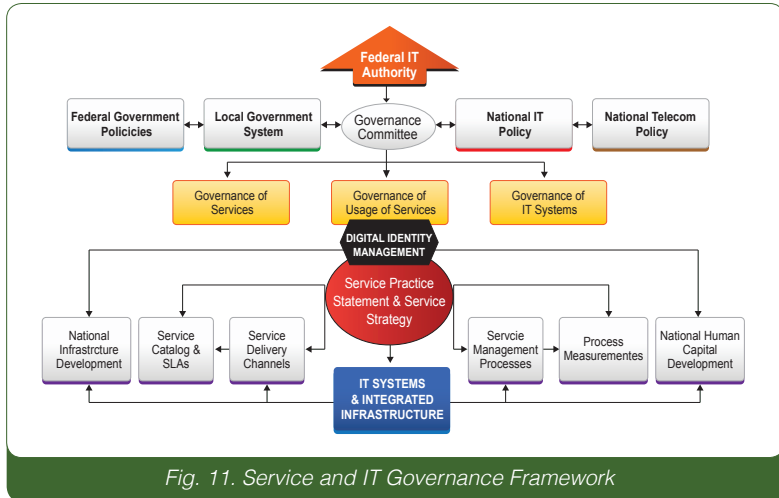


Fig. 11. Service and IT Governance Framework

When the public expects availability of quality services, assurance of service levels becomes a priority. A proper framework for service governance is required. Several models exist for service and IT governance frameworks. CoBIT 5 (control objectives for information and related technologies)⁸ and ITIL (information technology infrastructure library)⁹ provide excellent guides. These standards are technical in nature. CoBIT is developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and for information services (IS) audit, control and security practitioners. ITIL is one of the global standards on which CoBIT is based. ITIL describes the service

8 CoBIT is an abbreviation for Control Objectives for Information and Related Technologies. It is a framework created by an international organization called the Information Systems Audit and Control Association (ISACA). The framework is developed to support IT management and governance. In short, it is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. CoBIT was first released in 1996, the current version, COBIT 5 was published in 2012.

9 ITIL is an abbreviation for the Information Technology Infrastructure Library. It is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

management processes and recommends security and control practices but does not have a standard for them, which is where CoBIT comes in, because it provides a serviceable framework from which to perform audits on ITIL processes.

Based on these standards and the author's experience, a simplified service governance framework was constructed for potential deployment on a national level as depicted in Fig. 11. The framework is developed on the understanding that availability of services and quality of services need to be managed in order to address rapidly changing citizen preferences. The framework is designed to stress the need for a structured approach to program management with a focus on two principles:

- 1 Strategic Alignment: Focuses on ensuring the linkage of overall government strategic objectives with the IT plans of its agencies;
- 2 Value Delivery: Focuses on executing the value proposition throughout the delivery cycle, and ensuring that IT delivers the benefits promised from the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

The framework objects are broken down into several sub-components. These are discussed next.

First, the framework assumes that a federal authority at a national level is charged with the responsibilities and vested with the executive authority required to guide and manage government services. This authority would serve as the apex service regulation body for the country and would also serve as an arbitration body for services rendered by various government departments. See Fig. 12.

A central governance committee would oversee the functions of the authority and thus be responsible for assuring services and service delivery to the citizens. This committee would be subject to federal and local government policies and would rely on the country's legal system to

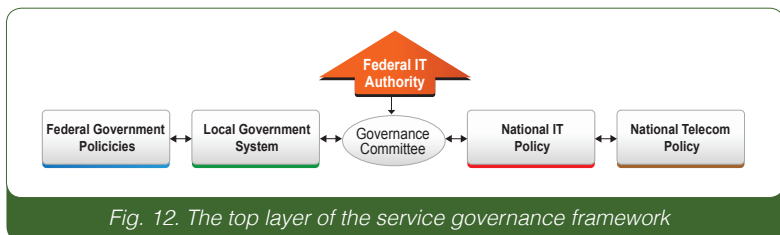
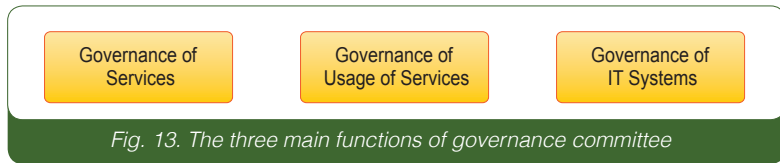


Fig. 12. The top layer of the service governance framework

provide it with necessary authority. Two other policies that would define the functioning of this governance committee would be the National IT Policy and the National Telecom Policy. These are fundamental sets of policies that should guide delivery of the services across multiple e-channels and automated processes, leading to efficiency in service delivery and optimization of service delivery processes. This would also lead to standardization of quality of service (QoS) across the country.

Guided by these national level policies, the Service Governance Committee would have three major domains of function: (1) Governance of Services, (2) Governance of Usage of Services, and (3) Governance of the IT Systems (supporting services and service delivery). We will briefly discuss each. See also Fig. 13.



• **Governance of Services:**

This would oversee the overall service definition, management of the service catalog and definition of the different types of services and different service channels. This would provide the basis for defining standards for quality of services.

• **Governance of Usage of Services:**

This would deal with the beneficiaries' management and the actual delivery of the services. It would oversee the availability of the services and qualify the service beneficiaries and regulators of the service delivery channels. 'How', 'When', 'Where', 'Why' and 'Who' are the components of the usage of services, while governance of services would deal with the 'what'.

• **Governance of IT Systems:**

That IT plays a major role in service delivery and the service processes is undeniable. IT Governance would deal with technical processes, standardization of technical infrastructure and processes required to facilitate service delivery.

The next level is about service governance framework components. See Fig. 14. These components could be grouped as implementation objects of the framework. This is guided by a clear service practice statement (SPS) and a well-defined service strategy. The SPS would be an unambiguous statement providing the vision and a set of practices that would lay the foundation for the service delivery and a state a commitment regarding the quality of service and service delivery.

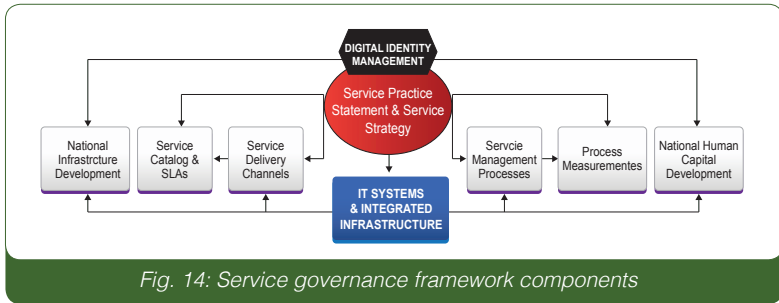


Fig. 14: Service governance framework components

As the Federal IT Authority would act as the central authority for guiding and managing government services, it would need to deal with the development of national infrastructure, enabling services and service delivery. This would not merely include the logical infrastructure but also the physical infrastructure. Thus, development of IT infrastructure/ computing systems, service centers, and service channels would be handled here.

At the other end of the development spectrum lies human capital development. Service development and delivery is not just a function of faceless machines but necessitates human interfaces. While humans are the beneficiaries of the services, would delivery of these services be driven by machines? Not so! It would essentially be driven by people. Human capital development would contribute greatly to the development of the service organization.

The four other components that form the implementation objects of the services framework are the service catalog with all the services, service owners, service responsibilities, service beneficiaries, and the channels that make services available. Service channels would handle the different devices, locations and means of the service delivery. It is critical to manage the chain of delivery right through to its last link, which more often than not defines the end of customer satisfaction. Management of the

service processes and the associated performance measures provide the closed the loop for process control.

At the base of the framework is the actual IT Infrastructure and the necessary technical devices covering backbone connectivity, computing infrastructure, security infrastructure and the integration of the technical and business processes delivering quality services.

The key component in the national services framework is the identity management process, specifically digital identity management. Digital Identity is the e-profile of a service seeker/beneficiary/provider, along with the unique identity and related credentials that establish—not just the identity but also trust between the different stakeholders [37]. This is the key to seek, deliver and benefit from the services across multiple channels of delivery in a seamless and flexible manner. Service beneficiaries and service providers would also interact with a high level of assurance in secure electronic transactional environments. This should lay the foundation for 24 hour service availability and the necessary security in the service delivery.

The next section concludes the article.

8. Concluding Remarks

In this article, we presented a conceptual framework for service governance on a national level. We intend this tool to be useful for governments and policy makers. The proposed framework could guide and motivate governments to develop and refine policy and practice and to self-regulate fields of service provision and governance. The components of the proposed framework reflect fields of practice that governments should engage in to ensure that their agencies comply with the national IT objectives, and that good management and effective monitoring of performance occur. Further research into practice within such a frame could provide useful insights to guide, develop and refine the framework.

We have also pointed out that today's governments have evolved over centuries in their practices in relation to the management and development of economic and social resources. ICT has played a central role in supporting government efforts in multi-faceted domains while making them more transparent and answerable to their citizens.

In the context of globalization, governments need to understand the links between citizen satisfaction and the quality of services provided by government agencies. The development of citizen centered government systems would be in the interests of public welfare, improving both citizen satisfaction and cost effectiveness of the public sector. See also Fig. 15.

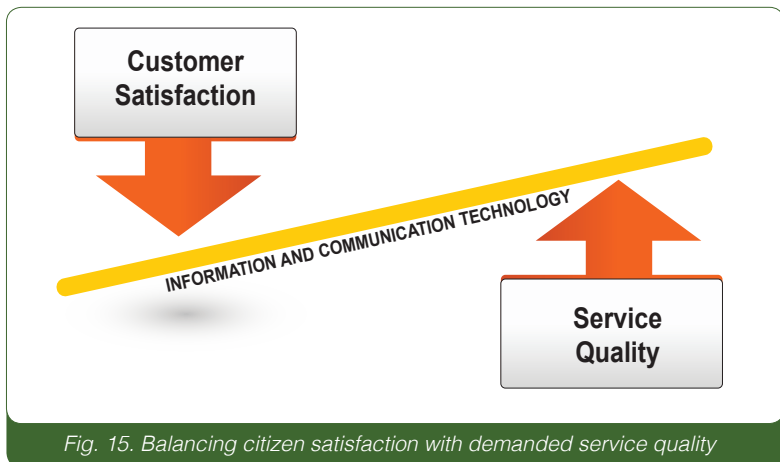


Fig. 15. Balancing citizen satisfaction with demanded service quality

Government quality programs involving TQM, BPR, and CRM should focus on improving manageable aspects of service-delivery systems, and should aim to measure citizen satisfaction and monitor reactions to change [48]. If quality programs are initiated, based on research with structured science and proven best practice, then improvement in quality should lead to greater satisfaction (ibid).

Modern digital identification technologies should be viewed as disruptive technologies. They have the potential to create new value systems, and to disrupt and displace existing public sector systems and technologies. Digital identification technologies provide higher levels of identity assurance and promote the development of more innovative and secure models of service delivery, enabling greater accessibility of government systems and facilitating choice of delivery channels.

Finally, the application of carefully chosen ICT could be seen as a “silver bullet” that has the potential to improve the overall performance and service delivery in the public sector. The link between citizen satisfaction and service quality should be addressed by government initiatives.

References

- [1] S. Balit, "Voices for change: Rural women and communication," Economic and Social Development Department, 1999. [Online]. Available: <http://www.fao.org/docrep/X2550E/X2550e01.htm>. [Accessed Jan. 10, 2013].
- [2] Accenture, "Driving High Performance in Government: Maximizing the Value of Public-Sector Shared Services," 2005. [Online] Available: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Driving_High_Performance_in_Government_Maximizing_the_Value_of_Public_Sector_Shared_Services.pdf. [Accessed Jan. 10, 2013].
- [3] Gartner, "Gartner's 2012 Hype Cycle for Emerging Technologies Identifies 'Tipping Point' Technologies That Will Unlock Long-Awaited Technology Scenarios", 2012. [Online]. Available: <http://www.gartner.com/it/page.jsp?id=2124315> [Accessed Jan. 10, 2013].
- [4] P. Dunleavy, "The Future of Joined-up Public Services," London School of Economics, 2010. [Online]. Available: http://eprints.lse.ac.uk/28373/1/The_Future_of_Joined_Up_Public_Services.pdf. [Accessed Jan. 10, 2013].
- [5] A. Di Maio, "Move 'Joined-Up Government' From Theory to Reality," Gartner Research, 2004. [Online]. Available: <http://www.gartner.com/id=456935>. [Accessed Jan. 10, 2013].
- [6] Hyde, J. "How to make the rhetoric of joined-up government really work," Aust New Zealand Health Policy, 5(22), 2008 [Online]. Available: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2613881/>. [Accessed Jan. 10, 2013].
- [7] Pollitt, C. "Joined-up Government: A Survey," Political Studies Review, 1, 34-49, 2003.
- [8] Wilkins, P., "Accountability and Joined-up Government," Australian Journal of Public Administration, 61(1), 114-119, 2008.
- [9] B. Chakravarti, and M. Venugopal, Citizen Centric Service Delivery through e-Governance Portal, 2008. [Online]. Available: http://www.nisg.org/knowledgecenter_docs/D01010001.pdf. [Accessed Jan. 10, 2013].
- [10] A.W. Guerrini, "E-Government and Online Government-Citizen Interaction: A Prospective Theoretical and Analytical Framework for Investigating Their Effects on the Organisation of Public Administrations and Service Delivery," 2008 [Online]. Available: <http://www.uoc.edu/in3/dt/eng/waksberg.pdf>. [Accessed Jan. 10, 2013].
- [11] Kaczorowski, W. (Ed.) Connected Government, Premium Publishing, London, 2004.

- [12] OECD, "Rethinking e-Government Services: User-Centred Approaches," OECD Publishing, Paris, 2009.
- [13] Halperin, R. and Backhouse, J., "Citizen Centric or Government Centric? Perceptions of Risk in New Identity Management Systems," In Reddick, C.G. (Ed.) Citizens and e-Government: Evaluating Policy and Management, Information Science Reference, Hershey, PA, 2010.
- [14] Yong, J.S.L. "Promoting Citizen-Centered Approaches to e-Government Programmes: Strategies and Perspectives from Asian Economies," Proceedings of Second APEC High-Level Symposium on e-Government, Acapulco, Mexico, October 2004. [Online]. Available: http://www.egov-in-asia.com/egov-2/cms_data/egov-paper-for-apec.pdf. [Accessed Jan. 10, 2013].
- [15] Jansen, V., Zeef, P., "Vision and Valuation of Citizen-Centric Shared Information Portal," Proceedings of 19th Bled eConference: eValues, Bled, 2006.
- [16] V. Frissen, N. Huijboom, J. Millard, "The future of eGovernment: an exploration of ICT-driven models of eGovernment for the EU in 2020," European Commission, Joint Research Centre, Institute for Prospective Technological Studies, 2007 [Online]. Available: <http://ftp.jrc.es/eur22897en.pdf>. [Accessed Jan. 10, 2013].
- [17] Kaul. V. "The Changing World of Media & Communication", Journal of Mass Communication and Journalism 2(6), 2012.
- [18] J. Bernoff, "Competitive Strategy in the Age of the Customer," Forrester Research, Inc., 2011 [Online]. Available: http://info.getsatisfaction.com/rs/getsatisfaction/images/Get_Satisfaction_Forrester_Age_of_Customer.pdf. [Accessed Jan. 10, 2013].
- [19] Heeks, R. Implementing and Managing eGovernment: an International Text. Sage, London, 2006.
- [20] G. Longford, "Rethinking E-Government: Dilemmas of Public Service, Citizenship and Democracy in the Digital Age," 2002. [Online]. Available: <http://www.innovation.cc/news/innovation-conference/longford.pdf>. [Accessed Jan. 10, 2013].
- [21] Omar, K., Scheepers, H., and Stockdale, R., "e-Government service quality assessed through the public value lens," In M. Janssen et al., (Eds.), EGOV 2011, Lecture notes in computer science, 6846, 431–440, Springer Verlag, Berlin, 2011.
- [22] G. Quirchmayr, S. Funilkul, and W. Chutimaskul, "A Quality Model of e-Government Services Based on the ISO/IEC 9126 Standard,"

2007. [Online]. Available: <http://www.sit.kmutt.ac.th/wichian/Paper/eGovServiceQualityModel.pdf>. [Accessed Jan. 10, 2013].
- [23] Ray, S. and Rao, V.V., "Evaluating Government Service: A customers' Perspective of e-Government," The 4th European Conference on e-Government, Dublin, June 17-18, 2004. [Online]. Available: <http://www.iimahd.ernet.in/egov/documents/evaluating-government-service.pdf>. [Accessed Jan. 10, 2013].
- [24] Al-Khouri, A.M., "eGovernment Strategies: The Case of the United Arab Emirates", *European Journal of ePractice*, 17, 126-150, 2012.
- [25] Evans, J.R., *Quality & Performance Excellence*, South-Western College Pub, 2010.
- [26] Tyagi, R.K. and Gupta, P.K. *A Complete and Balanced Service Scorecard: Creating Value Through Sustained Performance Improvement*, FT Press, 2008.
- [27] Kaufmann, M. and Serban, V. "The New EFQM 2010 Model for Business Excellence and its Fundamental Concepts in Light of the Economic Crisis," *The Romanian Economic Journal*, XIV(40), 99-116, 2011.
- [28] Hendricks, K. and Singhal, V., "Quality Awards and the Market Value of the Firm: An Empirical Investigation," *Georgia Tech, Management Science* , 42(3), 415-436, 1996.
- [29] Michalska, K., "Using the EFQM excellence model to the process assessment," *Journal of Achievements in Materials and Manufacturing Engineering*, 27(2), 203-206, 2008. [Online]. Available: http://www.journalamme.org/papers_vol27_2/27222.pdf. [Accessed Jan. 10, 2013].
- [30] Deloitte Research, "E-government's Next Generation: Transforming the Government Enterprise through Customer Service", New York: Deloitte Consulting (Global), 2001. [Online]. Available: http://www.deloitte.com/assets/Dcom-Global/Local_20Assets/Documents/DTT_DR_eGovNextGen.pdf. [Accessed Jan. 10, 2013].
- [31] Hammer, M. and Champy, J., *Reengineering the Corporation: A manifesto for Business Revolution*, Nicholas Brealey Publishing Limited, London, 1993.
- [32] D.D. Navarra, and T. Cornford, "ICT, Innovation and Public Management: Governance, Models & Alternatives for e-Government Infrastructures," 2005. [Online]. Available: <http://ifiptc8.org/asp/aspecis/20050137.pdf>. [Accessed Jan. 10, 2013].
- [33] Richter, P, Cornford, J. and McLoughlin, I., "The e-Citizen as talk, as text and as technology: CRM and e-Government," *Electronic Journal of e-Government*, 2(3), 2004.

- [34] Al-Khouri, A.M., "An innovative approach for e-Government transformation". *International Journal of Managing Value and Supply Chains*, 2(1), 22-43, 2011.
- [35] Al-Khouri, A.M. and Bal, J., "Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics," *Journal of Computer Science*, 3(5), 361-367, 2007.
- [36] Al-Khouri, A.M., "Optimizing identity and access management (IAM) frameworks". *International Journal of Engineering Research and Applications*, 1(3), 461-477, 2011.
- [37] Al-Khouri, A.M., "PKI in Government Digital Identity Management Systems", *European Journal of ePractice*, 4, 4-21, 2012.
- [38] Yanez-Pagans, M., Chong, A. and Salas, G.M., "Information Technologies and Provision of National Identification Cards by the Bolivian Police: Evidence from two Randomized Natural Field Experiments," *Proceedings of the Annual Bank Conference on Development Economics (ABCDE)*, A conference organised by the World Bank on the theme "Accountability and Transparency for Development", Washington, D.C., 2012. [Online]. Available: [http://siteresources.worldbank.org / EXTABCDE/Resources/7455676-1315933592317/8143947-1335963402037/8622235-1336401580364/Session-5-Monica_Yanez_Pagans.pdf](http://siteresources.worldbank.org/EXTABCDE/Resources/7455676-1315933592317/8143947-1335963402037/8622235-1336401580364/Session-5-Monica_Yanez_Pagans.pdf). [Accessed Jan. 10, 2013].
- [39] Kubicek, H. Hagen, M., "One-Stop-Government in Europe: An Overview," In Hagen, M., and Kubicek, H.(Eds.) *One-Stop-Government in Europe: an Overview and Results of 11 National Surveys*, University of Bremen, 1-36. [Online]. Available: <http://www.egov.vic.gov.au/pdfs/OneStop.pdf>. [Accessed Jan. 10, 2013].
- [40] PWC, "Transforming the citizen experience One Stop Shop for public services, PriceWaterhouse Coopers," *PriceWaterHouseCoopers*, 2011. [Online]. Available: <http://www.pwc.com.au/industry/government/assets/Transforming-the-Citizen-Experience-One-Stop-Shop-Feb12.pdf>. [Accessed Jan. 10, 2013].
- [41] Fransman, M., *The New ICT Ecosystem: Implications for Policy and Regulation*. Cambridge University Press, 2010.
- [42] Saith, A. and Vijayabaskar, M. (Eds.) *ICTs and Indian Economic Development: Economy, Work, Regulation*, SAGE Publications, 2005.
- [43] Birch, D.G.W. (ed.) *Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, Gower Publishing Limited, England, 2007.

- [44] Brancik, K.C. (ed.) Insider computer fraud: an in-depth framework for detecting and defending against insider IT attacks. Auerbach Publications, Boca Raton, FL, 2007.
- [45] EPC, "The Use of Audit Trails in Security Systems: Guidelines for European Banks," European Payments Council, 2001. [Online]. Available: [http://www.europeanpaymentscouncil.eu/documents/EPC153-10 20Audit 20Trails 20in 20Security 20Systems 20v1.0 20Approved.pdf](http://www.europeanpaymentscouncil.eu/documents/EPC153-10%20Audit%20Trails%20in%20Security%20Systems%20v1.0%20Approved.pdf). [Accessed Jan. 10, 2013].
- [46] Sullivan, C., Digital Identity: an emergent legal Concept - The role and legal nature of digital identity in commercial transactions, The University of Adelaide Press, Australia, 2010. [Online]. Available: http://www.adelaide.edu.au/press/titles/digital-identity/Digital_Identity_Ebook.pdf. [Accessed Jan. 10, 2013].
- [47] Windley, P. Digital Identity, O'Reilly Media Inc., Sebastopol, CA., 2005.
- [48] Iacobucci, D., Ostrom, A. & Grayson, K., "Distinguishing Service Quality and Customer Satisfaction: The voice of the Consumer," Journal of Consumer Psychology, 4(3), 277-303, 1995. [Online]. Available: <http://www.kentgrayson.com/Grayson%20Archive/satisfcationjcp.pdf>. [Accessed Jan. 10, 2013].
- [49] Dobkin, B.A. and Pace, R.C., Communication in a Changing World: An Introduction to Theory and Practice, McGraw-Hill, Nueva York, 2006.
- [50] Ogunsola, L.A., "Information and Communication Technologies and the Effects of Globalization: Twenty-First Century "Digital Slavery" for Developing Countries--Myth or Reality?," Electronic Journal of Academic and Special Librarianship, 6(1-2), 2005. [Online]. Available: http://southernlibrarianship.icaap.org/content/v06n01/ogunsola_l01.htm. [Accessed Jan. 10, 2013].

3

Connected Government: An Exploration of the UAE's Identity Management Integration Strategy¹

Abstract

The subject of connected government is coming once again to the forefront of national development priorities around the world. This stems from the need to address various local & global necessities in light of the changing landscape of the new digital world we live in today. In a connected government context, public service agencies are needed to act as a single enterprise so that citizens feel they are being served by one organization rather than a number of different public authorities. Identity management is considered here a fundamental pillar to enable such operating models and support single sign-on (SSO) & online identity validation capabilities for e-government & e-commerce environments. This article explores & describes the United Arab Emirates (UAE) government integration strategy with relation to keeping its national identity management infrastructure (population register) updated as life events take place. The integration strategy also aims to support federal & local government entities to verify citizen & resident information using their own applications in a secure, reliable, and integrated manner. Another expected contribution of the integration platform is to support decision-making & strategic planning dimensions of government work.

Keywords: identity management, identity lifecycle, connected government, e-government

¹ Please quote this article as follows:
Al-Khouri, A.M. (2013) "Connected Government: UAE Government Integration Strategy". Business and Management Horizons, Vol. 1, No. 1, pp.74-95.

1. Introduction

In a world characterized by rapid change driven by globalization, governments around the world are under extreme pressure to renovate their operating models and provide quality e-government services with secure interconnected systems and applications (Dunleavy et al., 2008; OECD, 2011; Saha, 2012). Despite the enormous number of strategic projects and gigantic investments, governments around the world have been facing challenging times to achieve interconnection between their “silo living” backend systems (Backman, 2009; Bertucc, 2008; Kubicek et al., 2011; O'Brien, 2012). Governments' attention have been shifting lately toward a “whole-of-government” approach that focuses on the provision of services at the front end supported by integration, consolidation, and innovation in back-end processes and systems to achieve maximum cost savings and improved service delivery (UNPAN, 2008).

In the past ten years or so, many governments have launched modern identity management programs in an attempt to address a number of national priorities (Al-Khouri, 2012a). Among these are objectives related to building an infrastructure to support the authentication of online users. These programs are also based on a strong belief that a robust and secure government-owned identity management system is crucial in addressing many of today's needs and challenges. This is to say that such identity management systems can be designed and architected to develop digital identities and online identity validation capabilities to support e-government and e-commerce environments (Al-Khouri, 2012b).

However, the primary focuses of these programs, from our reading and knowledge in the field, have been on the enrolment of the population and the issuance of smart identity cards but without sufficient attention to the overall management of the identity lifecycle. This is to say that, once a person is enrolled, his or her personal data may change, e.g., legal residency status, education, marital status, etc. Such updates are considered critical in such programs to fulfilling their mandate of being the primary reference for personal data.

One of the internationally recognized countries for its innovative and state-of-the-art identity management programs that have recently drafted a strategy to address this particular need is the United Arab Emirates (UAE). Having completed the enrolment of the population, the UAE government has recognized that it is imperative to maintain an up-to-date national population register. To achieve this strategic objective, the government has conducted a detailed analysis of how citizen and resident information can be updated instantaneously as life events take place. This article aims to outline the UAE's government integration strategy to enable a connected government concept and to support its federal e-government strategy. The explored integration strategy is, in principle, related to identity life cycle management.

The article is structured as follows. In section 2, we shed light on some of the global trends with regard to identity management and enterprise integration, as well as some key challenges faced by governments in this field of practice. In section 3, we provide information about the UAE national identity management infrastructure and the government's need to architect an enterprise integration strategy to keep the population register up to date. In section 4, we provide an overview of the UAE integration strategy, objectives, and priorities. In section 5, we describe the integration framework adopted by the UAE government and briefly describe the integration models, services, architecture, and governance aspects. We also address a high-level plan and the phases of the onboarding of government entities, and we outline key projects and initiatives and the roadmap set for the implementation of the integration strategy. In section 6, we present some key success factors identified by the government to ensure a successful implementation. In Section 7, we summarize and discuss the integration strategy, and we conclude the article in Section 8 with some perspectives, and opportunities for further research.

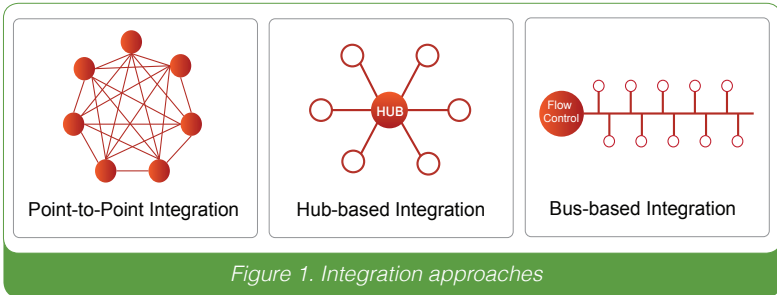
2. Global Trends of Identity Management and Enterprise Integration

Governments around the world have been very much attracted to national identity programs (Al-Khouri, 2012a; Al-Khouri, 2012c). These programs are globally justified on the basis of building identity management systems to achieve two primary objectives: to support national security and improve access to services. Many countries have initiated smart identity card programs in the last decade, with the total value of those projects exceeding \$24 billion. Further, more than 15 countries are in the process of upgrading their current identity cards to biometric-based systems.

Around the world, governments are struggling to maintain an up-to-date national population register to provide the different government entities with accurate information on citizens and residents. Typically, a citizen or resident will require multiple identification and supporting documents to access government-provided services. According to a recent United Nations report, even in highly ranked countries, the population and the governments are still in the process of understanding the role of national identity cards and how they can leverage such a valued asset in simplifying the lives of both the public and government entities in uniquely identifying a person and maintaining an up-to-date snapshot of information (UNPAN, 2012).

For example, in Sweden, government entities rely on bank-issued identification cards to register and apply for government services. In the U.S.A. and the U.K., different forms of ID are accepted, with the U.S.A. being more complicated given the different IDs issued at the federal and state levels with minimal integration or interoperability between the government departments. Korea and Singapore are the leading countries that have achieved a good level of success in providing a single ID that is issued to every citizen and resident, providing them with access to government services. Let us explore some common integration approaches in the next sub-section.

2.1 Enterprise Integration



One of the key factors to establish successful identity management is the integration between the different government entities and the entity responsible for managing identities (Bertino and Takahashi, 2010; Chappell, 2004; Williamson et al., 2009; Windley, 2005). For many years, integration has been handled at a system level where the primary focus is to identify what data is needed and how to send it to another system, creating a point-to-point integration pattern. As the number of systems grew, adding more point-to-point integration interfaces led to complex implementations and maintenance of such interfaces, presenting government entities with additional costs, limited flexibility in addressing new requirements, and other risks (Gottschalk and Solli-Saether, 2009; Pollock and Hodgson, 2004).

The challenges mentioned earlier led to the introduction of hub-based and bus-based integration patterns (Li et al., 2009; Watson and Ariyachandra, 2005). See also Figure 1. In hub-based integration, government entities can connect to a central or federated hub to send and receive data between them securely through re-usable messaging and integration interfaces providing performance improvements and scalability.

Bus-based integration introduced the concept of decentralizing messaging between different applications by sending and receiving data in a similar fashion to radio technology, where government entities can connect and send information that can be received by one or many government entities without the need to physically connect to the

government entity infrastructure. This provides the flexibility of sending a data set to multiple government entities using a single message.

The aforementioned patterns facilitated the integration between government entities whose focus was to send and receive specific data sets. With time, there has been a shift in emphasis from systems and data integration to overall enterprise integration with an increased focus on inter-enterprise operations, processes, and services, as depicted in Figure 2 (see also Ross et al., 2006).

This shift from system integration to enterprise integration provided government entities with the ability to link their integration needs with their overall strategic objectives by identifying which services a government entity can provide or need and leverage enterprise integration as a way to provide and consume these services (Daigneau, 2011; Wu, 2007).

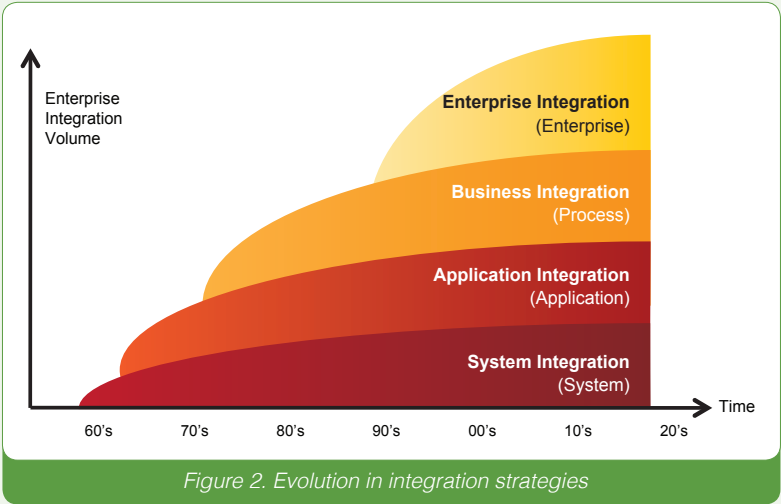
Combining identity management and enterprise integration, global trends provide government entities with the capability to provide integrated identity management solutions that will facilitate up-to-date population registers and provide identity owners with the capability to provide innovative ID-based services to other government entities and possibly businesses.

2.2 Challenges Faced by Governments

With the global trends in mind, a number of lingering challenges still face governments in achieving integrated identity management as follows:

- Lack of a government entity responsible for maintaining a national population register;
- Data privacy and confidentiality issues;
- Lack of a clear vision and cooperation between competing government entities; and
- Lack of a government-wide integration and interoperability framework

With the aforementioned challenges identified in addition to many other factors, such as the recent economic downturn, many countries are facing a challenge to drive the notion of a connected 24-hour government.



3. The UAE National Identity Management Infrastructure

As a result of the rapid growth of the economy as well as the population over the past few years in the United Arab Emirates (UAE), the government has expressed strong determination to enhance the performance of public departments and increase efficiency in a bid to improve the coordination of and citizens' access to public services.

Among the most strategic initiatives in the UAE is the national identity management infrastructure development program launched in 2003. As part of the program, all citizens and legal residents are issued unique identification numbers and smart cards that are linked with their personal information and biometric details.

The smart identity card provides a single secure identification document. It is envisioned that the new card will further assist in streamlining and simplifying government procedures and enable the country's citizens to use the new identity card as a travel document within the GCC countries.

The smart identity card has the following characteristics:

- One card type for nationals and residents with personal profile information;
- All cards are PKI-enabled (digital certificate);
- Biometric data on card with “match on card” feature;

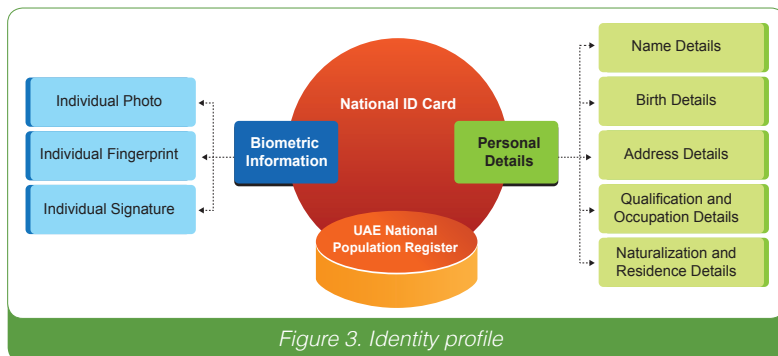


Figure 3. Identity profile

- Multiple security features (anti-fraud) built into the card; and
- Multi-factor authentication mechanisms for identity verification.

The validity of an identity card for residents is linked to the period of the residency visa permit; i.e., the expiry date as it appears on the card would be equal to the expiry date of the visa. To enhance the value and use of the new national identity card, the government is working on using it with PKI-enabled services.

The UAE government recently announced a comprehensive Federal e-Government Strategy to promote connecting the different government entities at the federal and local levels. It sets a strategic objective of having a connected government serving the entire population, where the new identity management infrastructure is envisioned to play a fundamental role.

By adopting cutting-edge and innovative technologies in this promising national program, the government is keen to make it play an active and central role in supporting the development initiatives of the country. Among the primary contributions of this program is the development of a business intelligence system around population demographics to support decision-making and strategic planning in the country. Another strategic objective aims to develop and improve existing service delivery models through advanced identity authentication capabilities and facilitating e-government and e-commerce.

3.1 The Need for Enterprise Integration

With the core identity management infrastructure in place and the UAE population fully enrolled in the Population Register, the following challenges were identified in maintaining an up-to-date and accurate national population register:

- Keeping the ID card and the personal profile information updated per the life events in the citizen/resident life cycle;
- Managing the card life cycle in synchronization with the identity life cycle; and

- Keeping the population register updated in near real time.

The primary reasons behind these challenges were seen to be twofold:

- Clear identification of the sources of information, and
- Lack of integration between the different government entities and the ID-issuing authority.

Considering these challenges, the government commissioned a comprehensive study to address these challenges, focusing on the development of an enterprise integration strategy bringing together the different sources of information.

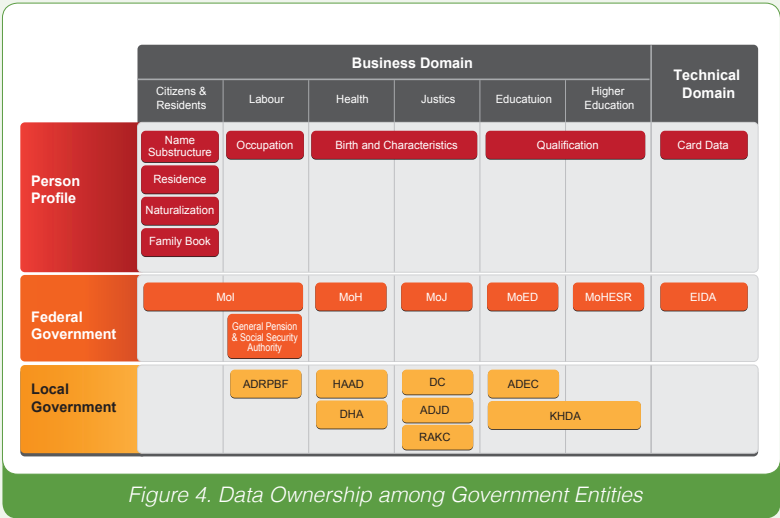
3.2 The State of Person Profile Information in the UAE

The UAE government has categorized the personal profile information into six key domains:

- **Core Identity:** Citizens' and residents' core identity information, such as name, residence and naturalization status, biometric data, digital certificates, and ID card numbers
- **Employment:** Data providing information about current occupation and employment status
- **Health:** Life information, including birth details
- **Academic:** Education details of schooling and higher education and related information
- **Legal:** Judicial information, including marital status

Based on the aforementioned key domains, it was essential to hold workshops with over 20 federal and government entities from the seven emirates to understand their role in maintaining such information, the business processes in relation to the feasibility of adoption of the national ID, and the technology used to maintain and store such information.

The outcome of this exercise was a detailed study in the integration of these government entities for managing the personal profile information in the National Population Register managed by the ID-issuing authority. The following diagram shows the mapping of the person information to the federal and/or emirate government entities:



4. Integration Strategy Overview

With the results of the study highlighting the different data sources for person profile information, the government has formulated a comprehensive approach to develop an enterprise integration strategy and meet its strategic objectives.

The enterprise integration strategy was designed to be in complete alignment with the overall identity-issuing authority's business strategy and objectives. The integration strategy formulated the integration strategic objectives and outlined the priorities of the integration components.

A comprehensive enterprise integration strategic framework was also developed to define the key components to develop an agile and practical integration strategy that will have an overarching contributinal impact on the identity-issuing authority's overall business strategy.

This integration strategy led to a set of initiatives covering the people, process, technology, and on-boarding of government entities into the enterprise integration initiative. Each of the initiatives was prioritized and used to define an enterprise integration roadmap that was actionable and executable. The following diagram depicts the methodology adoption for the integration strategy development.

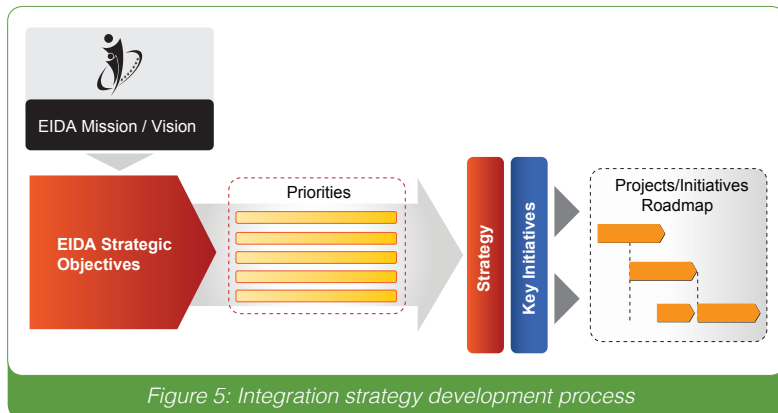


Figure 5: Integration strategy development process

4.1 Integration Strategy Objectives and Priorities

The enterprise integration strategy was architected to achieve the strategic objective of implementing an integrated and up-to-date secure national population register and deliver ID management services to UAE federal and local government entities through a flexible and adaptable service-oriented architecture.

The enterprise integration strategy was thus stated with the following objectives:

- 1) Provide a secure, scalable, and flexible business platform that supports the enterprise integration of the national population register, ID validation, and federated identity services based on the Emirates ID card and enterprise applications.
- 2) Provide proactive life events services enabling identified data owners to update and propagate person profile changes to update the national population register.
- 3) Provide person profile data services to e-government programs across different Emirates, authorized government entities, and authorized businesses.
- 4) Provide population register data replica services to authorized government entities and security organizations; provide statistics data to Department of Statistics for population statistics reports.
- 5) Provide effective Web-based dashboard and management capability for monitoring and managing the business enterprise integration.

To achieve the above objectives, the following priorities were identified:

- Ensure that the enterprise integration strategy and roadmap defines end-to-end architecture and solution implementation with minimal dependency and risks to achieve a successful implementation.
- Build an enterprise integration function that enables capability building for planning, management, operations, and support of enterprise integration.
- Consider leading enterprise integration patterns from leading vendors available in the market to implement the complete enterprise integration that can be modular and scalable.
- Leverage existing IT systems, IT infrastructure and security, and data center as well as other existing systems from other stakeholders effectively.



- Adopt an appropriate approach to implementing and operating the required enterprise integration and its platform through qualified and experienced system integrators and solution providers to deliver.

Based on these objectives, an integration framework has been designed and adopted to achieve effective integration, which is discussed next.

5. Integration Framework

The framework for the enterprise integration strategy was based on the identity-issuing authority's corporate business strategy and objectives as the main drivers with consideration for enterprise integration best practices, enterprise integration technologies, and on-boarding external and internal entities on the proposed integration platform. Also, the framework ensured alignment with the internal ICT department initiatives and current environment. The resulting enterprise integration strategic objectives and priorities were defined across a number of enterprise integration strategic components, as shown in Figure 6 below.

The enterprise integration strategic framework components were defined as follows:

- **Integration Models:** Defines the multiple integration models to government entities to access the services provided by the enterprise integration platform.
- **Integration Services:** Defines the business services providing integration capabilities to the national population register required to maintain an up-to-date national population register and services where government entities and potentially business to access the register. The technical services facilitate the platform and application services and the internal and external integration at the identity-issuing authority.

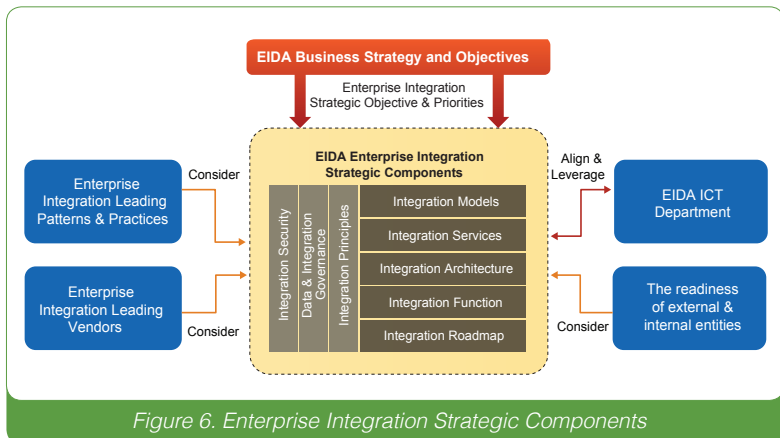


Figure 6. Enterprise Integration Strategic Components

- **Integration Architecture:** Defines the required technology architecture including the needed applications, integration, data, infrastructure, and security to fulfill enterprise integration needs.
- **Integration Function:** Defines the required enterprise integration organization and structure to support the roll-out of the enterprise integration strategy.
- **Integration Roadmap:** Defines the detailed roadmap to implement the enterprise integration strategy covering the people, process, technology, and government on-boarding initiatives.
- **Integration Security:** Defines the security requirements for state-of-the-art security measures covering integration services access and authorization, data encryption, and secure transport.
- **Data & Integration Governance:** Defines the service, data, and security governance measures to support the enterprise integration unit and its function.
- **Integration Principles:** Defines the general integration principles that are the rules and guidelines for the integration, platform standards, change management, and others.

5.1 Integration Models

Various integration models needed to be supported by the integration platform to meet possible business and functional requirements and to provide various options for external entities to connect through the four distinct models of integration that were developed for the implementation of the integration strategy. See Figure 7.

5.2 Integration Services

The enterprise integration needed to be supported by a series of business integration services that allow external entities to integrate with the national population register systems. The business services taxonomy was organized into several service groups to provide integration capabilities to the national population register. These services were mainly post-issuance services, i.e., services that could be provided after a national ID number and ID card were issued. Figure 8 shows the various business integration services groups:



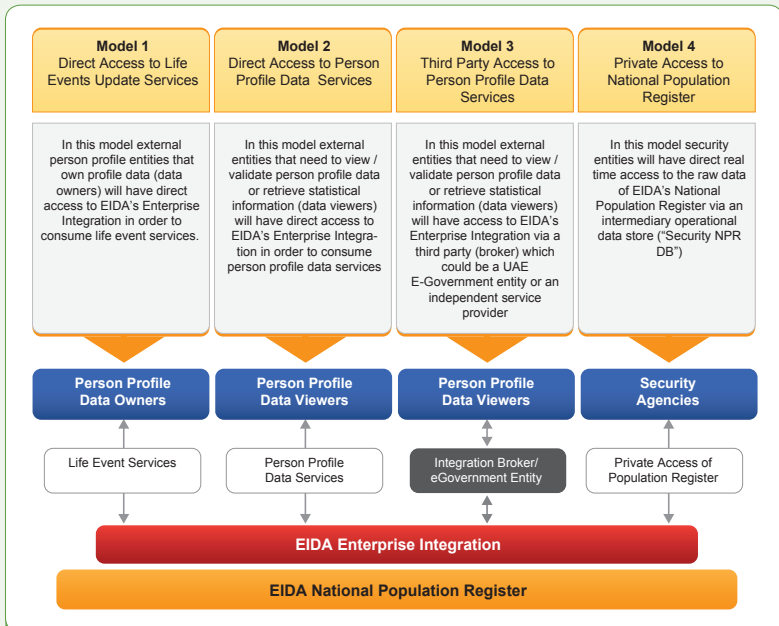


Figure 7: The four integration models

Service Group	Group Description	Service Types
Life Event Services	These are the core services used to update the population register information	Higher Education Services, Education Services, Labour Services, Judiciary Services, Health Services, Citizen & Residence Services
Retrieval Services	These are the core services used to view or validate the population register information	Inquiry Services, Verification Services, Matching Services
Statistical Services	These are the core services used to obtain statistical information from the population register	Population Demographics, Life Event Reports, Family Links Analysis
Special Services	These are the core services used to process any special operation that are required by individual entities	Tailored Reports, Raw Data Access Services
Person Profile Services	These are a lower level of services used to facilitate access to the data in each of the Person Profile Substructures.	Create Services, Read Services, Update Services, Deactivate Services, Historic Read Services

Figure 8. Business integration service groups

5.3 Integration Architecture

To enable seamless, secure, and flexible integration within the internal environment and between the external entities, a standards-based and an SOA-based enterprise integration were seen as important to implement to enable the functionality of the integration platform. A reference architecture was developed as depicted in Figure 9 below.

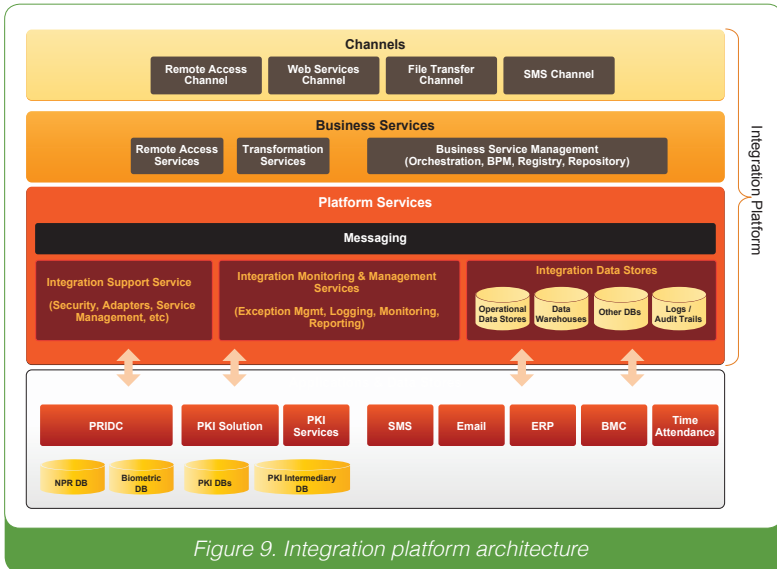


Figure 9. Integration platform architecture

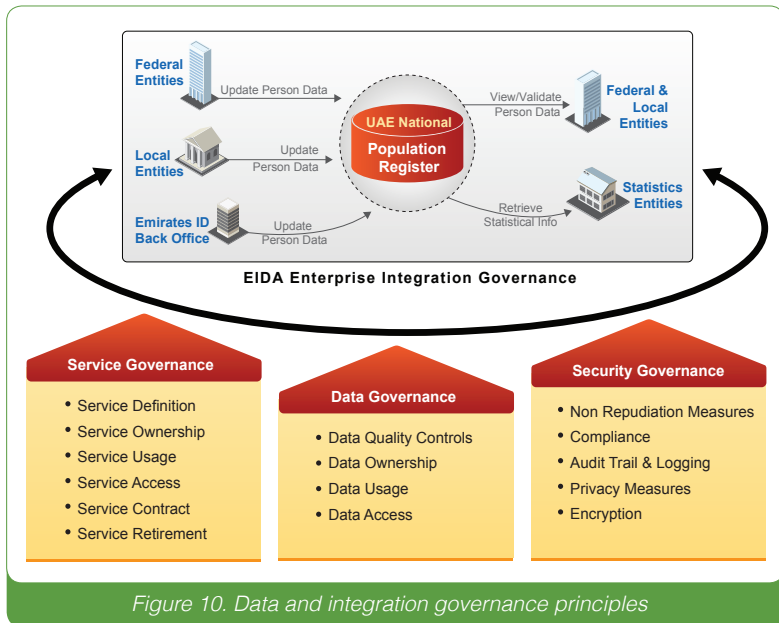
Each of the four reference architecture layers is described in Table 1.

Table 1. Reference Architecture Layers

Layer	Description
Channels	This layer is the presentation layer of the enterprise integration. It allows external entities to use the identity authority's services through various channels such as Web services, file transfer (FTP), and remote access.
Business Services	This layer provides the functionality for service modeling, service orchestration, SOA governance, transformation, and remote access (needed for special security operations) where all services provided to government entities are defined and maintained
Platform Services	This layer is the key enabler of SOA-based enterprise integration. It provides messaging capabilities, integration services (adapters, APIs, etc.), monitoring and management services, and data services (ODSs, DWs, and DBs) to facilitate internal and external integration.
Applications & Data Stores	This layer is not considered a part of the enterprise integration to be implemented. This layer contains applications and data stores that will be integrated with each other via the enterprise integration, as well as facilitating external entities' integration for the purpose of accessing the population register.

5.4 Integration Governance

The enterprise integration governance model was needed to ensure control over the life cycle of services exposed through the platform and consumed by the different stakeholders. Enterprise integration governance defines and enforces policies related to service contracts, data quality, data and information privacy protection, authorized access to services, non-repudiation, and logging. For the successful implementation and operation of enterprise integration, these governance principles needed to be adhered to. The diagram below illustrates the data and integration governance principles that needed to be defined and enforced to control access to the enterprise integration platform.



5.5 On-Boarding of Government Entities

To ensure a structured deployment process, a comprehensive approach needed to be defined that will clarify the process of on-boarding government entities and confirming their readiness, service development, service testing, and launching of the integrated services. See also Figure 11.

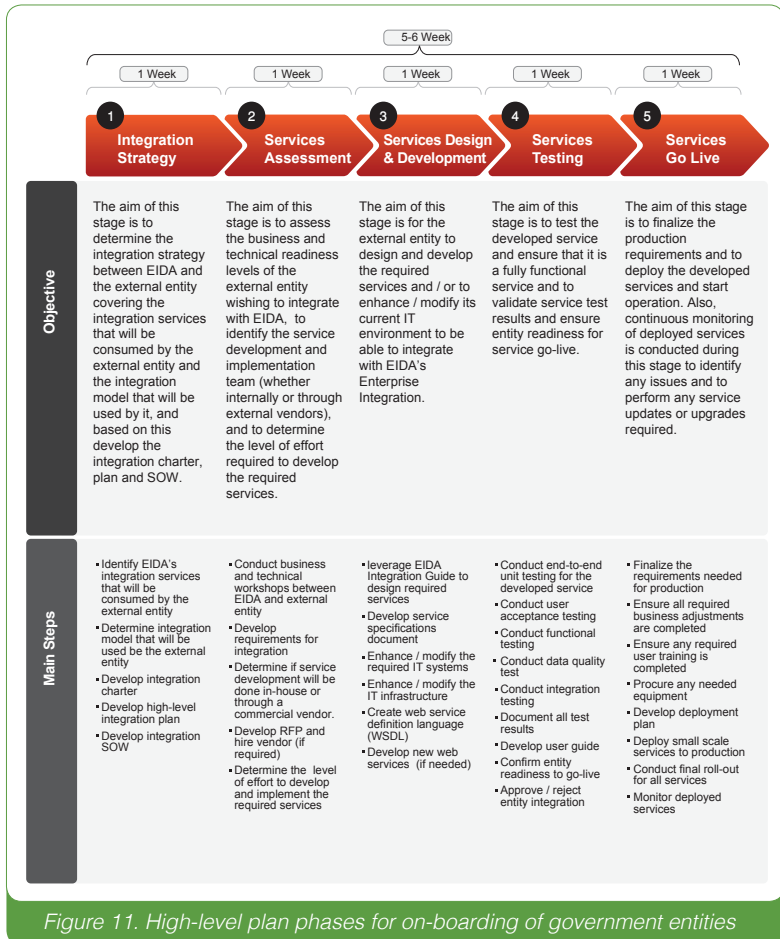
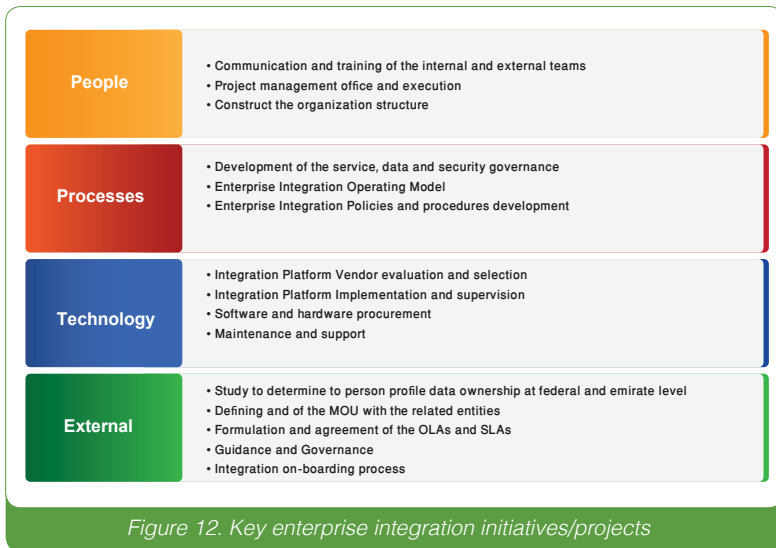


Figure 11. High-level plan phases for on-boarding of government entities

5.6 Integration Strategy Key Projects and Initiatives

The successful implementation of the integration strategy required the project team to undertake a number of initiatives/projects across four key domains: people, processes, technology, and external entities. Below are the identified key enterprise integration implementation initiatives/projects.

Each of the above initiatives and projects has been defined, highlighting the needed resource requirements, estimated duration, and interdependencies.



5.7 Integration Strategy Roadmap

With the enterprise integration strategy set to be executed over a three-year period, a comprehensive enterprise integration implementation roadmap was crafted to execute the defined initiatives/projects with the following key objectives to be achieved in each year:

- **Year 1:** Evaluate and select the right technology vendor to implement the integration platform and define the integration function requirements to support its implementation.
- **Year 2:** Implement the necessary strategy initiatives to kick-start the integration platform and on-boarding of government entities while setting up the necessary integration function to support its implementation.
- **Year 3:** Focus on adding more government entities as part of the integration strategy and provide the necessary support to operate, maintain, and support the integration platform.

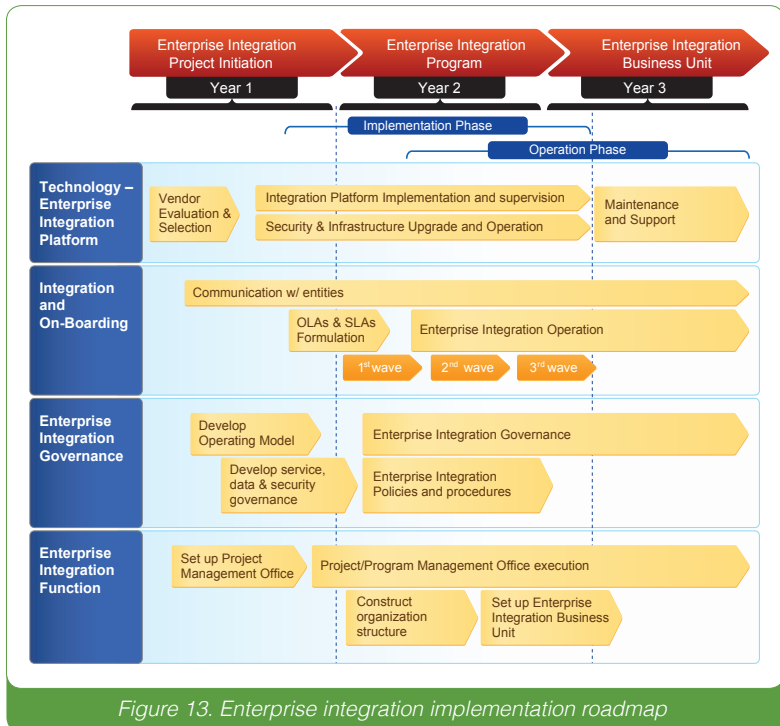


Figure 13. Enterprise integration implementation roadmap

6. Key Success Factors

To achieve a successful implementation of the enterprise integration strategy, the government identified the following key success factors that needed to be dealt with vigilantly:

- **Promotion** of the integration strategy to UAE federal and local government entities through the adoption of a well-defined communication plan and awareness campaigns.
- **Adoption** of the new smart ID card by government entities/ citizens/residents by requiring the presentation of an ID card when requesting services.
- **Adoption** of an ID number as part of person profile by data owners would support and enable integration between the identity-issuing authority and the government entities.
- **Provide comprehensive services** to UAE federal and local government entities.
- **Ensure secure access** to the national population register to promote confidence and adhere to data privacy and confidentiality best practices.
- Robust **integration on-boarding approach** and **dedicated on-boarding team** to help and support government entities in integrating with the national identity management system.

7. Summary and Discussion

A national identity management program is characterized by the scope of the identity profile of an individual. One of the key factors to establish a successful identity management infrastructure is the level of integration between the different government entities (e.g., data owners) and the entity responsible for managing identities (e.g., Identity Authority).

In the case of the UAE, the early work of integration was handled at a system level where the primary focus was on identifying what data is needed for creating the identity profile. The integration focus at the time primarily dealt with how to collect information from a single system (i.e., the Ministry of Interior). The integration was more of a point-to-point integration pattern between the Interior and the Identity Authority.

Over the past years and prior to setting up the new integration strategy in the UAE, the number of systems that needed to be connected with (i.e., data owners), has grown exponentially, and thereby adding more point-to-point integration interface requirements. This has led to complex integration implementations. On the other hand, the maintenance of such interfaces presented the identity authority with additional costs, limited flexibility in addressing new requirements and related risks. This in turn led the UAE to study different topologies of integration such as hub-based integration and bus-based integration.

As explained earlier in section 2, in hub-based integration, government entities can connect to a central or federated hub. This connectivity enables stakeholders to send and receive data securely through reusable messaging and integration interfaces to a centralized data hub. On the other hand, bus-based integration introduced the concept of decentralized messaging between different applications by sending and receiving data akin to a television broadcast. This respects the fact that different stakeholders have their own databases and services, but need to share data in delivering their services effectively.



The UAE integration strategy recognized that integration is the key to not just providing an identity to an individual but also to create a complete identity profile and more importantly manage this identity profile for its currency. It is in this context that a new integration strategy has been drawn up.

The primary consideration of the UAE integration strategy is that different stakeholders (e.g., government entities) can connect and send information that can be received by one or many government entities without the need to physically connect to the individual infrastructure of the government entity. This is envisaged to provide a level of flexibility for sending data sets to multiple government entities using a single message similar to a broadcast, albeit securely. This is the basis of the UAE's new integration strategy.

It is also recognized in the UAE that the identity profile created in the national population register spans the life-events of an individual and that life-events need to be updated in real time in the population register. Accordingly, the program has identified different sources (i.e., data owners) that contribute to the personal profile (e.g., Ministry of Interior, Ministry of Justice, Ministry of Education, to name a few). The new integration strategy envisages going beyond point-to-point connectivity by providing business process integration in addition to the technical integration with respect to data update.

The UAE integration strategy implementation is based on integrating systems for updating the population register in real-time as per the occurrence of the life-events. In the first phase of integration, there will be integration at systems level for updating the population register in real-time as life-events occur. In the second phase of the implementation, the infrastructure will provide the required business process integration to ensure the validation of the data updates coming from the identified sources of information (data owners). This will bring in the much required

data governance needs and the business rules for validating the automatic data update in the national population register.

The third phase of the integration strategy implementation envisages the data subscription and data sharing services on account of an up to date population register. This will ensure that the nation as a whole is served by the current population register and will enable efficient delivery of services to the citizens from the government, securing in the knowledge that the service is being delivered to the individual who he or she claims he or she is.

8. Conclusion

This article has attempted to provide some practical insights into a government integration strategy design and architecture that aims to improve identity life cycle management. The explored initiative is believed by the UAE government to propel the country to a leading position in providing integrated identity management solution and support its strategic 2021 vision of being among the top ten countries in the world. The innovative integration strategy outlined in this article is also envisioned to enable the UAE federal government and local Emirates' strategy to achieve their objective of being a 24-hour connected government. This is likely to contribute to the UAE's prosperity and economy, providing effective, efficient, and secure government services to its citizens and residents.

A key contribution of this article is that it explores and describes the strategy from within a government setting. In light of the lack of existing research to cover this topic until now, we hope that the presented work supports the fields of both research and practice. The single case and the qualitative nature of this study are considered an obvious limitation. Therefore, more quantitative research that sheds light on wider implementations is seen as an opportunity for further research and exploration of the practices to provide a more holistic picture of the given subject.

Finally, the rapid technological advancements will put more pressure in the days to come on governments to adapt and become connected governments. This will raise the bar in the public sector to reduce costs, improve relationships, become more efficient and effective, and, most importantly, user-centric (see, for example, Noveck, 2009; OECD, 2009; Shareef et al., 2012). Similar to the private sector, governments will have hard times ahead as they will seek ruthlessly to strengthen their international competitive advantage and cope with the new digital world order.

References

Al-Khouri, A.M. (2012a). Population Growth and Government Modernisation Efforts. *International Journal of Research in Management & Technology*, 2(1), pp. 1-8.

Al-Khouri, A.M. (2012b). PKI in Government Digital Identity Management Systems. *Surviving in the Digital eID World*, *European Journal of ePractice*, 4, pp. 4-21.

Al-Khouri, A.M. (2012c). eGovernment Strategies: The Case of the United Arab Emirates. *European Journal of ePractice*, 17, pp. 126-150.

Backman, J. (2009). Beyond Silos: Cross-boundary Internet Service Portals'. *Government Finance Review* [Online]. Retrieved from: <http://www.highbeam.com/doc/1G1-195266688.html>, [10 December 2012].

Bertino, E. and Takahashi, K. (2010). *Identity Management: Concepts, Technologies, and Systems*, Artech House Publishing.

Chappell, D. (2004). *Enterprise Service Bus: Theory in Practice*, O'Reilly Media.

Daigneau, R. (2011). *Service Design Patterns: Fundamental Design Solutions for SOAP/WSDL and RESTful Web Services*, Addison-Wesley Professional.

Dunleavy, P., Margetts, H., Bastow, S. and Tinkler, J. (2008). *Digital Era Governance: IT Corporations, the State, and e-Government*, Oxford University Press, USA.

Gottschalk, P. and Solli-Saether, H. (2009). *E-Government Interoperability and Information Resource Integration: Frameworks for Aligned Development*. Information Science Reference.

Kubicek, H., Cimander, R. and Scholl, H.J. (2011). *Organizational Interoperability in E-Government: Lessons from 77 European Good-Practice Cases*, Springer.

Li, S., Hu, Y., Xie, Q. and Yang, G. (2009). Heterogeneous Information System Integration Based on HUB-SOA Model. *Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCST '09)*. Huangshan, P. R. China, 26-28, Dec. 2009, pp. 239-242, [Online], Retrieved from: <http://www.academypublisher.com/proc/iscst09/papers/iscst09p239.pdf>, [6 December 2012].

Noveck, B.S. (2009). *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*. Brookings Institution Press.

O'Brien, A. (2012). *Business Strategy: From Silos to Smart Government – SOA in Human Services*, IDC.

OECD (2009). e-Government Studies Rethinking e-Government Services: User-Centred Approaches. Organisation for Economic Co-operation and Development, OECD Publishing.

OECD (2011). The Call for Innovative and Open Government: An Overview of Country Initiatives. Organisation for Economic Co-operation and Development, OECD Publishing.

Pollock, J.T. and Hodgson, R. (2004). Adaptive Information: Improving Business through Semantic Interoperability, Grid Computing, and Enterprise Integration. Wiley-Interscience.

Ross, J.W., Weill, P., Robertson, D. (2006). Enterprise Architecture as Strategy: Creating a Foundation for Business Execution, Harvard Business Review Press.

Saha, P. (2012). Enterprise Architecture for Connected E-Government: Practices and Innovations, IGI Global.

Shareef, M.A., Archer, N., Dwivedi, Y.K., Mishra, A., Pandey, S.K. (Eds.) (2012). Transformational Government Through eGov Practice: Socioeconomic, Cultural, and Technological Issues, Emerald Group Publishing Limited.

UNPAN (2008). United Nations e-Government Survey 2008: From e-Government to Connected Governance, United Nations, New York, [Online], Retrieved from: <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf> [6 December 2012].

UNPAP (2012). United Nations E-Government Survey 2012: E-Government for the People, United Nations, [Online], Retrieved from: <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf> [6 December 2012].

Watson, H.J. and Ariyachandra, T. (2005). Data Warehouse Architectures: Factors in the Selection: Decision and the Success of the Architectures, [Online], Retrieved from: http://www.terry.uga.edu/~hwatson/DW_Architecture_Report.pdf [6 December 2012].

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

Windley, P.J. (2005). Digital Identity, O'Reilly Media.

Wu, R, C-Y. (2007). Enterprise integration in e-government, Transforming Government: People. Process and Policy, 1(1), pp.89-99.



4

5

6

Digital Identity

- 4 - Digital Identity: Transforming GCC Economies
- 5 - Federated e-Identity Management across the Gulf Cooperation Council
- 6 - Identity Management in the Age of Mobilificaiton



Digital Identity: Transforming GCC Economies¹

Abstract

Governments and businesses alike are coming to understand that national and global economies should use the Internet as a medium for innovation and economic growth. A critical component that has been left to service providers to establish and manage is that of digital identities of online clients and customers. Lack of regulation and effective methods of management has resulted in greater concerns over privacy, security, and productivity in online environments, thus hindering the development and use of the full potential of the Internet. This paper attempts to explore the role of a government initiated digital identity management system in supporting the creation of a stronger digital economy. The author provides an overview of the identity management infrastructure development initiatives in Gulf Cooperation Council (GCC) countries and briefly examines their potential to revolutionize and transform existing economic models. The author argues that the new smart identity cards produced in these countries may serve as secure tokens that connect digital and physical identity, create trustworthy environments, and strengthen confidence in online transactions critical to the growth of the digital economy.

Keywords: *digital identity, identity management; e-government, e-business, e-commerce, digital economy.*

¹ Please quote this article as follows:
Al-Khoury, A.M. (2014) "Digital Identity: Transforming GCC Economies", Research, Innovation and Entrepreneurship Reforms in Gulf Cooperation Council (GCC) Countries, *Journal of Innovation: Management, Policy & Practice*, Vol. 16, No. 2, pp. 3594-3617.

1. Introduction

The world has been undergoing transformation over the last twenty years, due to the advent of breakthrough technologies converting our societies from analog to digital models. Copper technology has given way to optical fiber, and we now have information flowing at the speed of light. We live in an interconnected world of instant access. However, in this interconnected digital world with a multitude of content domains, dissemination of information remains a challenge (OECD, 2009). Essentially, it is not so much a challenge of the medium of dissemination as the challenge of verification of the identity of online individuals, one of ensuring that the information is reaching the right seeker. Is the service beneficiary the intended one? (Al-Khouri, 2012a; 2012b). Rifkin (2010) argues that economic shifts over the last several decades have given rise to a regime where anonymous transactions are almost impossible. In a service-based economy where delivery has come to depend upon digital networks, businesses and governments alike need reliable, secure, and private means for creating, storing, transferring, and using digital identities (ibid.).

Conventional identity documents fall short of meeting today's digital world needs (Al-Khouri, 2012b; Baym, 2010; Sullivan, 2011). There is a need for digital identity profiles by trusted identity service providers. Such identity providers would fill the void of trust. Providing secure digital identification credentials would enable many faceless transactions on the web, cutting across the different electronic access channels such as Internet portals, kiosk machines, mobile phones, and contact centers.

Nonetheless, the management of digital identity has many facets – technical, economic, social, and cultural – and is a complex area of practice (Backhouse, 2006; Camp, 2004; Fish, 2009; ITU, 2006; Neubauer & Heurix, 2010; OECD, 2011). In the digital world, the challenge is how to translate the mechanisms through which service providers and clients trust each other when initiating online transactions.

According to a recent report published by Boston Consulting Group, the economic value of applications built on the use of digital identity for both public and private sector organizations is expected to reach €330 billion in Europe alone by 2020, representing a 22% annual growth rate (Liberty Global, 2012). That report also estimates that the consumer benefit will far exceed the organizational value, reaching €670 billion annually by 2020, mainly stemming from reduced prices through data-driven cost synergies, time savings through self-service transactions, and the high value that individuals place on free online services and mobile apps, supported at least in part by the sharing of their personal data. Another finding of the report indicates that two-thirds of potential value generation, €440 billion in 2020, at risk if stakeholders fail to establish trust in secure flow of data.

The existing literature is full of studies and reports that argue that management of digital identity does not seem to have reached the level of maturity that would enable the full realization of the digital economy (see, for example: ITU, 2006; OECD, 2009; OECD, 2011). The argument is based on the fact that online interactions carry a high level of risk, yet the level of security that existing digital identity management practices provide is not high enough for users to trust engagement in such transactions (Bertino et al., 2009; Cavoukian, 2008; Fish, 2009; Koops & Leenes, 2006; Thompson, 2010; Windley, 2003). Comprehending this critical need, many governments around the world have initiated programs at the national level to provide verifiable digital identification credentials to their citizens (Al-Khouri, 2012c).

The aim of this article is to explore the role of government initiated digital identity management systems in supporting the creation of a stronger digital economy. It uses the example of GCC countries, which have led the world by issuing digital credentials to all of their citizens. These credentials are based on advanced and integrated technologies such as biometrics, public key infrastructure, and smart cards. The article will briefly discuss the potential benefits of setting up a government-owned validation authority to provide online identity verification and authentication

services to both public and private sectors. This is argued to contribute to the creation of trustworthy environments and strengthen confidence in online activities critical to growth of the digital economy.

The article is structured as follows: Section 2 sets the argument for smart identity cards and their beneficial economic impact in GCC countries, and presents a simplified model of the role of government as an identity service provider. Section 3 provides an overview of identity management infrastructure programs in GCC countries. Section 4 presents a benefit accrual model and business transformation opportunities based on the application of the smart identity card. Section 5 explores the application of smart identity cards with their multiple factor authentication capacities for remote transactions. Section 6 highlights the possible opportunities for entrepreneurs to develop and offer value-based solutions for service providers that can use the smart identity card capacities. Section 7 draws on some similarities and differences in the digital ID implementation approach between GCC and European Union (EU) countries. Section 8 concludes the article.



2. The Smart Identity Hypothesis

“Identity is precisely the beaming light that guides the economic system and eventually determines the path to development.”(Djafar, 2009).

Though the context of the above statement is about a country's social identity, our hypothesis is related to the fact that a digital identity may act as a beaming light to guide new frontiers of economic and development models. As such, modern identity management infrastructure implemented by governments is expected to change the way business is transacted and open up previously unknown avenues, contributing to overall economic growth. The use of smart card-based digital identity profiles is expected to transform the way services and benefits are delivered (Al-Khouri, 2007; Forget & Stervinou, 2007).

Figure 1 illustrates a government-owned identity management infrastructure providing identification and authentication services in a trusted chain established by government. The certification and registration authorities represent the enrolment and issuing processes. The use of smart identity cards and the associated verifiable credentials (e.g. digital certificates, biometrics, digital signatures, and time-stamps) provide strong authentication and non-repudiation mechanisms. Service providers in e-government or e-commerce environments can rely on government-issued identities to offer their online services and deliver them remotely. Such a service paves the way to new opportunities that were previously hindered because of concerns regarding online identities. Such a model is likely to open up previously unavailable channels for service and benefit delivery, thus contributing to increased economic activity.



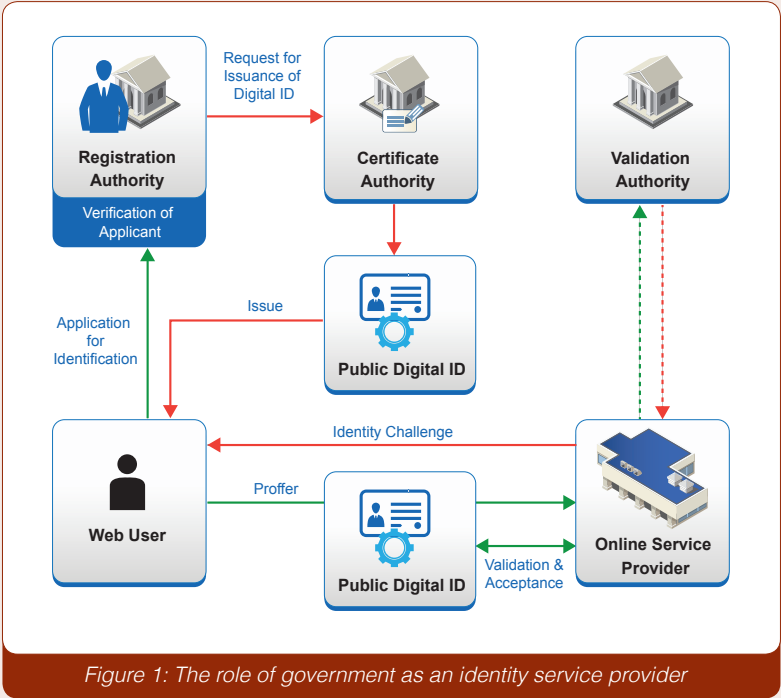


Figure 1: The role of government as an identity service provider

3. Digital ID and Economics– The GCC Context

GCC governments have launched national identity management infrastructure development programs to modernize their existing population databases (Al-Khouri, 2012c). These schemes attempt to enroll the entire population. They add a new dimension to the identification process represented by the capture of biometrics. All GCC countries have established either independent government entities or departments within their Ministries of the Interior to act as registration authorities and as the countries' digital identity providers.

With a clear mandate for population enrollment, these entities have also taken on the role of a certification authority to generate a complete digital profile of every resident and citizen in their respective countries. To date, GCC countries have issued more than 20 million digital identities that are based on various biometrics and advanced cryptographic technologies, packaged in secure smart cards. See also Figure 2.

CC smart identity cards serve as secure documents that uniquely identify individuals and link personal data to their own biological features, such as fingerprints and facial recognition. The smart card with its micro-chip includes a unique identity number, ICAO-compliant photograph, cardholder's electronic and digital signatures, a set of fingerprints, and a pair of digital certificates issued by the population certification authority (CA) secured by a PIN, as well as the personal data provided at the time of enrollment. This constitutes a complete identity profile packaged securely in a compact card, with little variation from one country to another. With multi-factor authentication and online validation capabilities, GCC countries are now poised to provide a range of identity-related services to both the public and private sectors. These services are expected to change the way that business is conducted online.



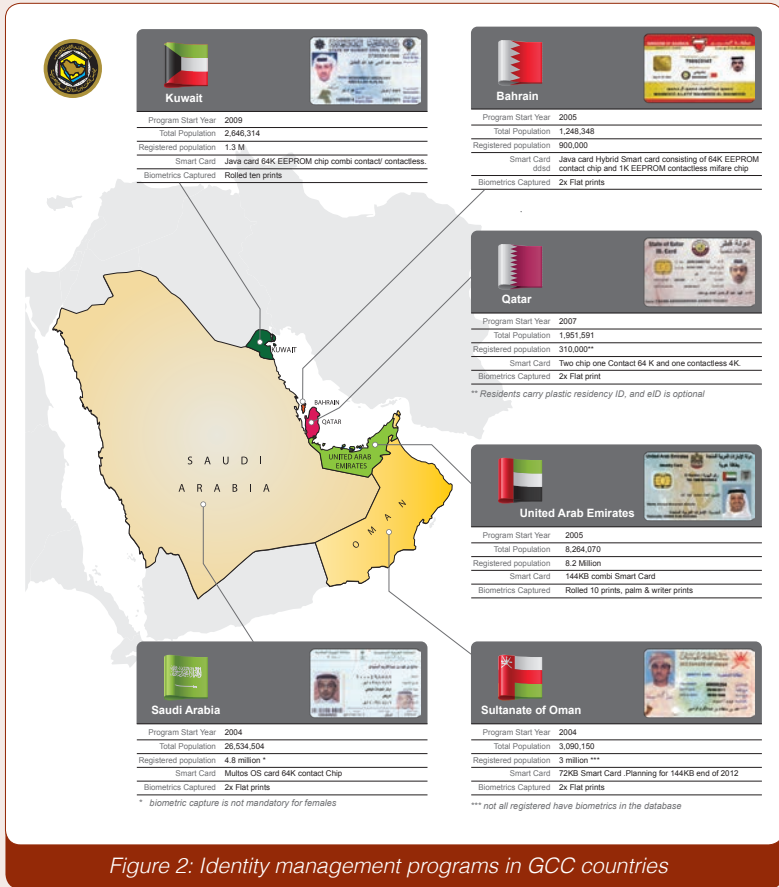


Figure 2: Identity management programs in GCC countries

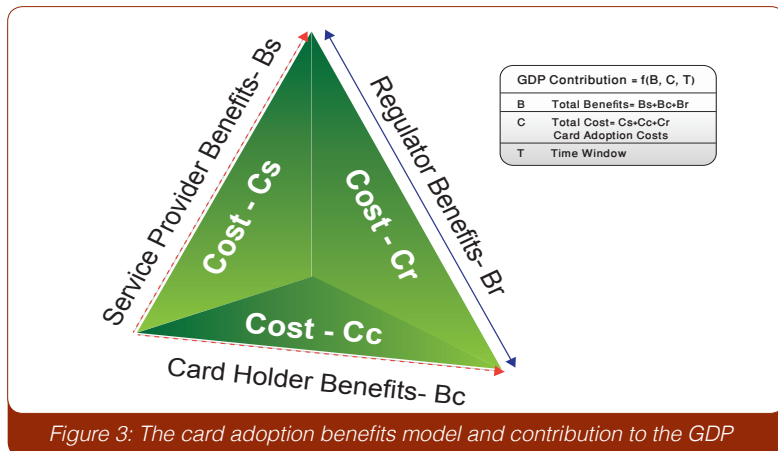
4. The National ID Card and Business Transformation

With such identity credentials issued to individuals, many interesting avenues are opened for new business practices. We will first examine a potential business transformation and its projected economic impact in the context of the United Arab Emirates (UAE).

The new smart identity card is now mandatory in the UAE. It must be produced to receive any benefit or service from a government department anywhere in the country. The government is currently working to improve promptness of access by service providers to information from the new identity card before extending its use from the public to the private sector. As the acceptance of the new identity card becomes more widespread, service providers will gradually begin accruing benefits in various forms. The Benefit Accrual Model for smart identity card usage can basically be constructed with three major stakeholders:

1. The service providers;
2. The card holder (service seeker); and
3. The regulator (government).

See also Figure 3.



The apparent economic benefits would far outweigh the adoption costs. Investment in establishment and adoption processes would benefit solution providers that would enable the integration of the identity card into service systems, thus opening up new business avenues for entrepreneurs. The hypothesis here is that benefit realization is a function of the cost. Costs incurred by one entity are revenues for another entity within the economy, thus contributing overall to GDP.

An internal study that we carried out in the banking sector in the UAE during the preparation of this article showed that nearly twenty minutes of data entry time was saved when opening a customer account using the smart identity card. So if the same bank opens 10,000 accounts per year nationwide, the time savings are estimated to be nearly 200,000 minutes. This is a saving of nearly two person-years of labor!

One can only imagine the increase in productivity and the opportunities that this time saving could provide to the institution. The following table provides an overview of further areas of benefit to the three stakeholders.

Table 1: Stakeholders' benefits

Service Providers	Card Holders	Regulators
ID theft reduction- less fraud	ID theft reduction- more protection	Less arbitration
Paper document reduction- less storage costs	Paper document reduction- less costs of holding	Green environment
Data integrity- increased data integrity resulting in quicker transactions	Data integrity- transaction assurance	Ease of audit- reduced time for verification
Saving in identity management systems	Saving in carrying multiple identities	Unified identity management
Resource reduction-increasing productivity and reducing costs by deploying e-services	Ease of access and convenience of access to services	Resource productive redeployment
Lower space requirements- reduced costs of office holdings by e-offerings	Convenience of access to services- 24-hour availability	24-hour authority
Increased security in transactions	Assured delivery of services	Reduced carbon foot print



There are many other direct benefits that can be added to the above list when effects on space, time, and productivity are considered. While customer self-service and process automation may currently be the major applications of digital identity, we expect that this focus will shift towards innovative new services and enhanced user experience (Liberty Global, 2012). Figure 4 depicts three evolutionary stages of digital identity value creation. The digital identity intensity of use increases over time and depends on a number of prerequisites. The first stage involves the use of basic digital identity capabilities to securely authenticate individuals for basic digital services and/or products. Stage two focuses on internal enhancements and process optimization leveraging with advanced digital identity capabilities. Stage three envisages an ecosystem in which individuals, businesses, and other organizations enjoy greater trust and security as they conduct sensitive transactions online.

Services provided by both public and private sectors are still at the very beginning of the path. Many organizations in these sectors are only now starting to embrace digitalization—such as government agencies and health care providers moving to electronic records and setting up processes that move this data along the value chain. The availability of a government-owned, trusted identity management system with an online validation service has the potential to fuel substantial opportunities for economic growth.

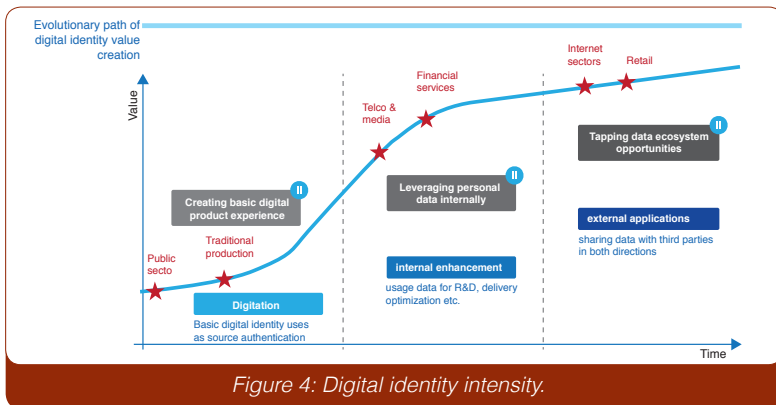


Figure 4: Digital identity intensity.

Source: Liberty Global, 2012

5. Smart Identity Card and Remote Transactions

The new smart identity card bridges and bonds the “digital” and the “physical” identity. The use of smart identity cards, public key infrastructure, and biometrics allows the connection between the digital and physical identity to be made (Al-Khouri, 2007; Barral, 2010; Kathrine & Kirubakaran, 2011; Khan et al., 2010). The public key infrastructure (PKI) components and controlled biometric authentication enable service providers to enhance their remote and e-service offerings. No longer are transactions required to be carried out in person for trust to be established. The identity card provides the necessary basis for trust that enables remote transactions on the internet, at kiosk machines, and from mobile phones.

Land registration departments could make it possible for contracts to be signed by the lessor and the lessee using their smart identity cards, leaving a clear audit trail and enabling remote registration of property transactions. The courts could also archive their legal documents and judgments digitally signed by judges and preserved in electronic vaults.

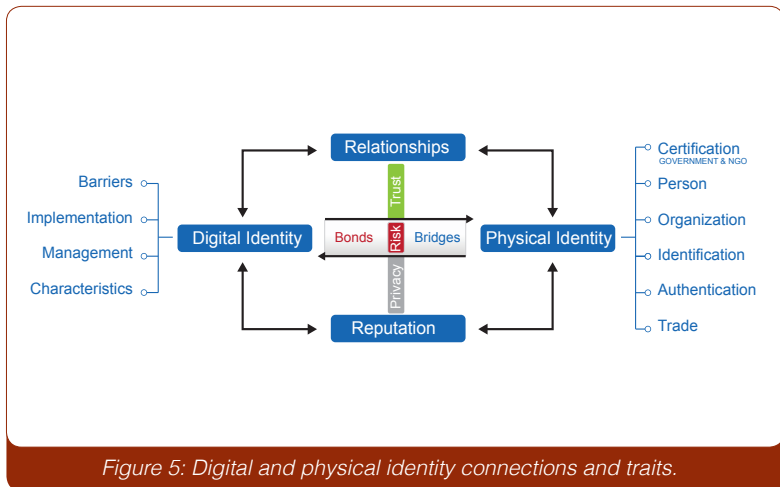


Figure 5: Digital and physical identity connections and traits.

Source: Fish, 2009

Banks are already poised to provision new customers and allow them to open accounts remotely in the basis of knowing that the identity card presented for authentication on the Web portal is genuine and verified by government. Micro-payments would be possible using the smart identity card enabling online transactions and reducing the burden of small change on the national treasury. These are but some of the critical transactions that would be made possible using the new smart identity card and some examples of the benefits that GCC countries would experience once appropriate strategies and roadmaps for the use of these services were put in place. Certainly, these innovations could provide huge economic benefits.

6. The National ID Card and Entrepreneurship

The possibilities outlined in this article are preliminary models for some of the new service industries that could be launched, based on the smart identity card system. Provision of identity services and integration of smart card identity systems into current systems will require critical and innovative thinking to develop value-based solutions for service providers. Use of technologies such as near field communication (NFC), could be driven by smart phone usage enabled by identity cards. Such innovation would create attractive opportunities for entrepreneurial solution providers. A new wave of technology implementation is coming.

While the new smart identity cards provide identity security, cross-border travel would become easier, due to similar initiatives across the region. New opportunities for collaboration between providers of border security services would arise. Adoption and implementation of the identity card is still in its nascent stages. While this is so, opportunities for entrepreneurs abound.

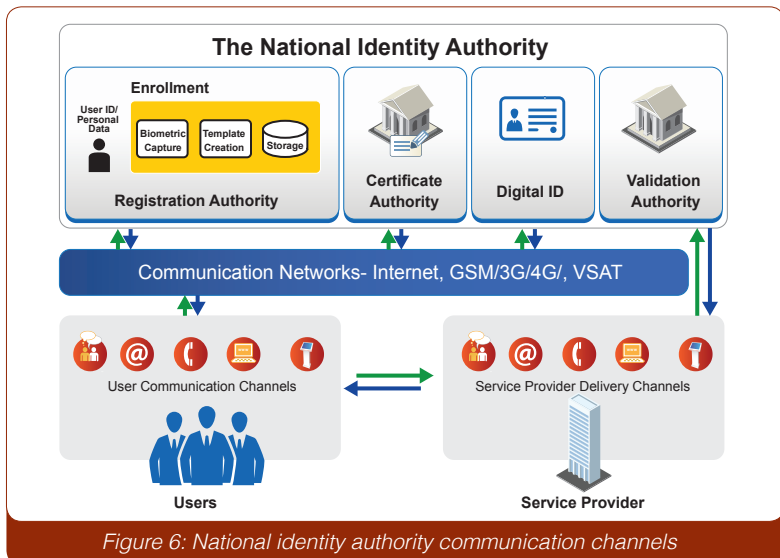


Figure 6: National identity authority communication channels

7. Digital Identity in GCC & EU Countries

There are interesting comparisons that can be drawn between digital identity implementation in GCC countries and the processes in European Union (EU) countries. Although there are some similarities, differences exist in the approaches adopted.

An important difference is in the basis for the provision of the digital identity. While GCC countries are issuing digital identities as part of a national ID program, EU countries seem to distinguish between national ID programs and the digital identity, although both serve the same purpose.

EU countries are driving the digital identity initiative with a clear goal of promoting the development of the digital economy. They are taking conscious steps in the achievement of this goal. Their steps are based on detailed scientific studies that show how the digital economy is growing at seven times the rate of the conventional economy, may improve economical sustainability and offers social benefits.

The Digital Agenda for Europe (DAE) was formally constituted, with a vision for 2020 and 101 targets to achieve in the propelling European economy's 2010-2020 growth strategy (European Union, 2012). See also Figure 6 in the Annex. Full implementation of this digital agenda is projected to increase European GDP by 5%, or 1500€ per person, over the next eight years, by increasing investment in information and communication technology (ICT), improving eSkills levels in the labor force, enabling public sector innovation, and reforming the framework conditions for the internet economy. In terms of jobs, up to 3.8 million new jobs could thus be created in the long term.

Security requirements and consequent identity verification requirements are considered the chief issues driving the need for digital ID profiles of EU citizens. Thus, EU countries seem to have sufficient confidence in PKI technology to use it to enable secure digital transactions and identity verification. Personal information privacy and data protection are major

topics on the discussion tables of policy makers in EU countries that could be barriers to larger scale implementation of digital IDs in EU. Adoption of biometrics technology in digital ID profiles seems to face resistance for privacy reasons.

In contrast, the digital ID initiatives in GCC countries are driven by security needs at a national level, given that these economies are largely served by a workforce, the majority of whom are expatriates. Biometric verification thus assumes a greater significance in the establishment of personal identity. UAE and Saudi Arabia stand out as countries with a clear PKI program agenda complementing the personal identity profile.

The economic importance of the digital ID profile is not ignored by the GCC countries. There are several initiatives, within individual countries and at the GCC level, to set up collaborative operational standards like those prevailing within the EU bloc (Al-Khouri and Bechlaghem, 2011). As economic activity becomes transformed by the use of the national digital identity profiles, issues of data protection and privacy are bound to arise. It is expected that these issues will be addressed in agreements between the service providers and the beneficiaries.

In this context, it is important to note the demographic composition of the GCC countries. While EU and GCC economies are each impacted by expatriate populations, the contrast the level of such impact is stark. The EU's member countries mainly contend with expatriate workers from within the bloc, while GCC countries employ expatriates from around the world. Herein lies the main difference.

GCC countries also employ a largely transient expatriate population whose average residency is shorter, compared to the migratory nature of the expatriate workers in the EU, who are nonetheless mostly EU citizens. This transience, coupled with large outbound remittances, brings challenges to economic activity in the GCC. This represents another difference in the implementation approach of the digital identity profiles and their usage in securing remote transactions.

In UAE, the digital identity profiles are linked to the residency permits for the expatriates and automatically expire when the residency expires. When the residency is renewed so does the digital ID profile. While the national identity number remains perpetual, the digital identity profile consisting of digital certificates from the Population Certificate Authority are reissued and biometric data revalidated. This key process brings an added element of security, enhancing the basis for trust that the national ID brings to economic activity.

7. Conclusion

Digital identity management is a critical pillar for the development of the digital economy. However, many of the prevalent digital identity management practices currently in use around the world are not robust enough to support the development of higher-value online services. Such online services normally carry a higher level of risk related to security, privacy, and trust. The complexity of credential management and limitations of existing approaches are considered decisive impediments to the progress and development of the digital economy. Government intervention in setting up the right supporting conditions is critical for development of trust and for promotion of innovation across the public and private sectors. Such developments should help provide a critical mass of high-value online services complemented with an infrastructure to manage assurance of credentials in digital spheres.

The argument presented in this paper depends on a scenario of great economic activity surrounding the adoption of smart identity cards in GCC countries. With GCC countries taking giant leaps in technology adoption and infrastructure investment, it is beyond doubt that an economy based on digital identity will endure and flourish. As more transactions are based on the new smart identity card, more services are likely to be rolled out using its advanced features, such as biometrics, digital signatures and time-stamps. Governments are on the path of e-transformation into 24-hour authorities, with social benefits to be delivered remotely, using the new smart identity card.

We are likely to witness transformation of business practice from the traditional personal delivery mode to a secure virtual and remote mode. This will take shape with the confidence that the new smart identity card will provide the same basis for trust as one would expect in a personal transaction. This should also open up new opportunities for innovation in both service delivery and business models. A clearly formulated national strategy for digital identity management is fundamental to the further movement of existing offline economic and social services into the digital

world, to the creation of innovative online public and private services, and to the continued development of the digital economy (Al-Khouri, 2012d; Al-Khouri, 2012e; Hornung, 2004; OECD, 2011).

References

- 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*, 3(5), 361-367.
- 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), 30-49.
- Al-Khouri, A. M. (2012a). eGovernment Strategies: The Case of the United Arab Emirates. *European Journal of ePractice*, 17, 126-150.
- Al-Khouri, A. M. (2012b). PKI in Government Digital Identity Management Systems. *European Journal of ePractice*, 4, 4-21.
- Al-Khouri, A. M. (2012c). Population Growth and Government Modernisation Efforts. *International Journal of Research in Management & Technology*, 2(1), 1-8.
- Al-Khouri, A. M. (2012d). Emerging Markets and Digital Economy: Building Trust in the Virtual World. *International Journal of Innovation in the Digital Economy*, 3(2), 57-69.
- Al-Khouri, A. M. (2012e). 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*, 3(4), 1-28.
- Backhouse, J. (2006). Interoperability of identity and identity management systems. *Data Protection and Data Security*, 30(9), 568-570.
- Barral, C. (2010). *Biometrics & Security: Combining Fingerprints, Smart Cards and Cryptography*. Retrieved from: http://biblion.epfl.ch/EPFL/theses/2010/4748/EPFL_TH4748.pdf
- Baym, N. K. (2010). *Personal connections in the digital age*. Malden, MA: Polity Press.
- Bertino, E., Paci, F., Ferrini, R. & Shang, N. (2009). Privacy-preserving Digital Identity Management for Cloud Computing. *Computer*, 32, 21–27, Retrieved from <ftp://ftp.research.microsoft.com/pub/debull/A09mar/bertino.pdf>
- Camp, L. J. (2004). Digital Identity. *IEEE Technology & Society*, 23(3), 34-41 Retrieved from http://social.cs.uiuc.edu/class/cs598kgk-04/papers/digital_identity.pdf
- Cavoukian, A. (2008). *Privacy in the Clouds*. White Paper on Privacy and Digital

Identity: Implications for the Internet. Retrieved from <http://www.cloudhosting.co.uk/files/PrivacyintheClouds.pdf>

Djafar, B. A. (2009). National identity, prerequisite for growth, The Jakarta Post. Retrieved from <http://www.thejakartapost.com/news/2009/09/24/national-identity-prerequisite-growth.html>

European Union (2012). Digital Agenda for Europe, Retrieved from <https://ec.europa.eu/digital-agenda/en>

Fish, T. (2009). My Digital Footprint: A two-sided digital business model where your privacy will be someone else's business! London: FutureText.

Forget, G. & Stervinou, A. (2007). The virtual smart card. *Card Technology Today*, 19, 7-8.

Hornung, G. (2004). Biometric Identity Cards: Technical, Legal, and Policy Issues, in S. Paulus, N., Pohlmann, and H. Reimer, (Eds), *Securing Electronic Business Processes* (pp. 47-57). Vieweg, Wiesbaden. Retrieved from http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/Hornung_Buch_ISSE_2004.pdf

ITU (2006). Digital Life. Retrieved from International Telecommunication Union (ITU), Geneva website: <http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf>

Kathrine, G. J. W. & Kirubakaran, E. (2011). Biometric Authentication and Authorization System for Grid Security, *International Journal of Hybrid Information Technology*, 4(4), 43-58. Retrieved from http://www.sersc.org/journals/IJHIT/vol4_no4_2011/4.pdf

Khan, B., Khan, M. K. & Alghathbar, K. S. (2010). Biometrics and identity management for homeland security applications in Saudi Arabia. *African Journal of Business Management*, 4(15), 3296-3306. Retrieved from <http://www.academicjournals.org/ajbm/pdf/pdf2010/4Nov/Khan20et20al.pdf>

Koops, B. & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime, *Data Protection and Data Security*, 30(9), 553-559.

Liberty Global (2012). The Value of Our Digital Identity, Retrieved from Liberty Global website: <http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>

Neubauer, T. & Heurix, J. (2010). A Roadmap for personal identity management, 2010 Fifth International Conference on Systems, Retrieved from Publication Database of the Vienna University of Technology website: http://publik.tuwien.ac.at/files/PubDat_192118.pdf

OCED (2011). Digital Identity Management: Enabling Innovation and Trust in the Internet Economy, Retrieved from The Organisation for Economic Co-operation and Development (OECD) website: <http://www.oecd.org/internet/interneteconomy/49338380.pdf>

OECD (2009). The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. Digital Economy Papers, No. 160. OECD Publishing. Retrieved from The Organisation for Economic Co-operation and Development (OECD) website: <http://dx.doi.org/10.1787/222134375767>

Rifkin, J. (2001). The Age of Access: The New Culture of Hypercapitalism, Where all of Life is a Paid-For Experience, New York: J.P. Tarcher/Putnam.

Sullivan, C. (2011). Digital Identity. Retrieved from The University of Adelaide

Adelaide, South Australia website: http://www.adelaide.edu.au/press/titles/digital-identity/Digital_Identity_Ebook.pdf

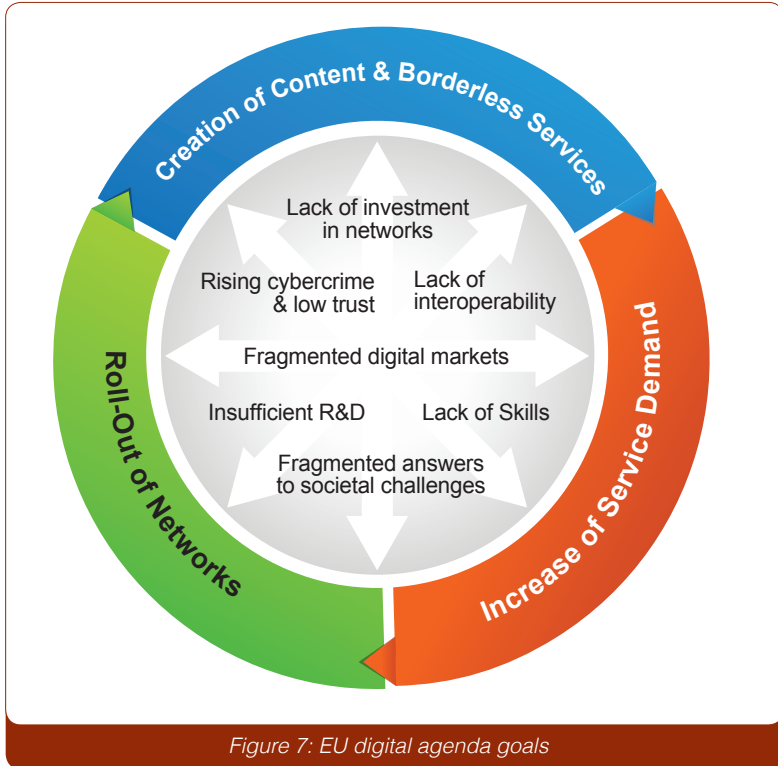
Thompson, P. (2004). Cognitive Hacking and Digital Government: Digital Identity. Journal of Systemics, Cybernetics and Informatics, 2(2), 9-12.

Windley, P. J. (2003). Understanding Digital Identity Management. Retrieved from Windley's Technometria website: <http://www.windley.com/docs/DigitalIdentity.pdf>

Annex: EU Digital Agenda Goals

Source: http://europa.eu/rapid/press-release_IP-10-581_en.htm

Figure 6 depicts the EU digital agenda goals. Below is a brief explanation of each of the seven goals.



A new Single Market to deliver the benefits of the digital era

Citizens should be able to enjoy commercial services and cultural entertainment across borders. But EU online markets are still separated by barriers which hamper access to pan-European telecoms services, digital services and content. Today there are four times as many music downloads in the US as in the EU because of the lack of legal offers and fragmented markets. The Commission intends to open up access to legal online content by simplifying copyright clearance, management and cross-border licensing. Other actions include making electronic payments and invoicing easier and simplifying online dispute resolution.

Improve ICT standard-setting and interoperability

To allow people to create, combine and innovate we need ICT products and services to be open and interoperable.

Enhance trust and security

Europeans will not embrace technology they do not trust - they need to feel confident and safe online. A better coordinated European response to cyber-attacks and reinforced rules on personal data protection are part of the solution. Actions could also potentially oblige website operators to inform their users about security breaches affecting their personal data.

Increase Europeans' access to fast and ultra fast internet

The 2020 target is internet speeds of 30 Mbps or above for all European citizens, with half European households subscribing to connections of 100Mbps or higher. Today only 1% of Europeans have a fast fibre-based internet connection, compared to 12% of Japanese and 15% of South Koreans (see table below). Very fast internet is essential for the economy to grow strongly, to create jobs and prosperity, and to ensure citizens can access the content and services they want. The Commission will inter alia explore how to attract investment in broadband through credit enhancement mechanisms and will give guidance on how to encourage investments in fibre-based networks.

Boost cutting-edge research and innovation in ICT

Europe must invest more in R&D and ensure our best ideas reach the market. The Agenda aims to inter alia leverage private investments with European regional funding and increasing EU research funding to ensure that Europe keeps up with and even surpasses its competition. EU investment in ICT research is less than half US levels (€37 billion compared to €88 billion in 2007).

Empower all Europeans with digital skills and accessible online services

Over half of Europeans (250 million) use the internet every day, but another 30% have never used it. Everyone, young and old, irrespective of social background, is entitled to the knowledge and skills they need to be part of the digital era since commerce, public, social and health services, learning and political life is increasingly moving online.

Unleash the potential of ICT to benefit society

We need to invest in smart use of technology and the exploitation of information to seek solutions to reduce energy consumption, support ageing citizens, empower patients and improve online access for people with disabilities. One aim would be that by 2015 patients could have access to their online medical records wherever they were in the EU. The Agenda will also boost energy saving ICT technologies like Solid State Lighting technology (SSL) that use 70% less energy than standard lighting systems.

5

Federated e-Identity Management across the Gulf Cooperation Council¹

Abstract

The concept of federated e-identity is gaining attention worldwide in light of evolving identity management challenges to streamlining access control and providing quality and convenient online services. In a federated system, participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to online resources. The article provides insight into the ongoing federated e-Identity initiative in GCC countries. The aim of the initiative is to develop a trusted and secure cross-border infrastructure to authenticate and validate citizens' identities across GCC borders. Such an interoperability platform then can be used to facilitate citizens' mobility and stand as the basis for digital economy development. Current literature does not include any information about the work going on in GCC countries in relation to the GCC eID platform. This article thus contributes to developing a better understanding of such practices, triggers debate and discussion, opens the door to reflection, and guides international efforts in this eminent domain of practice.

Keywords: *identity federation; federated identity management, electronic identity, eID interoperability, citizen mobility; GCC countries*

¹ Please quote this article as follows:
Al-Khoury, A.M. (2013) "Federated e-Identity Management Across the Gulf Cooperation Council", *International Journal of Public Information Systems*, Vol. 9, No. 1, pp. 20-44..

1. Introduction

The field of identity management systems has been evolving rapidly over the last two decades (Al-Khouri, 2012). With this development, countless modern systems have been introduced, many of which are innovative and are based on breakthrough sciences (Bertino and Takahashi, 2010; Williamson et al., 2009). The technological evolution, associated with increasing customer expectation in relation to service quality and convenience, has created higher demand for more integration between such systems (Bhargavan et al., 2008; Cabarcos, 2013; Camenisch and Pfitzmann, 2007; Novell, 2011). Concepts such as service oriented architecture, online government, and new public sector management are pushing the field of practice to establish digitally trusted and federated identities for individuals that can be used across borders by service providers in electronic environments (Buecker et al., 2005; Chadwick, 2009; Goodrich et al., 2008).

On a global scale, the field of identity management has witnessed a significant number of initiatives to address this requirement, often referred to as federated identity management systems (Baldoni, 2012). These initiatives have been grappling with providing services like single sign on and identity verification capabilities to enable seamless identity management solutions. These implementations vary in terms of the frameworks they follow and the trust mechanisms they use.

Governments have been realizing the need to develop interoperable federated identity management platforms to support citizens' mobility cross-borders (Bruegger, 2007; Fleurus et al., 2011; Langenhove et al., 2011; Porter, 2008). The European Commission is implementing a project to develop an interoperable electronic identification (eID) platform to provide single, secure, and cross-border infrastructure for the authentication of legal and natural persons across Europe (STORK, 2013). GCC countries are also working on a similar platform development to facilitate GCC citizens' mobility and enhance economic cooperation between the six member states. Both projects aim to allow citizens to

access cross-border services securely by using eID credentials issued by their home countries.

The objective of this article is to provide a high level overview of how GCC countries intend to develop an interoperable identity federation across their countries. The existing literature does not include any information about this subject, and this study will attempt to fill in some fundamental knowledge gaps in the existing body of knowledge. This should in turn trigger debate and discussion, open the door for reflection, and subsequently guide international efforts in this eminent domain of practice.

The article is structured as follows. In section 2, we present the various dimensions of federated identity management systems and the platform on which such systems are designed. In Section 3, we elaborate on the identity federation and present the critical role of an identity provider in the overall federation ecosystem. In section 4, we present the current conceptual and agreed design of how identity federation across GCC countries will operate. In Section 5, we reflect on the differences between the GCC interoperability framework and the European STORK 2.0 project. We also reflect on the need to address and meet the needs and expectations of the customer spectrum to increase the chances of success of such large and mission-critical endeavors. The article is then concluded in section 6.

2. Federated Identity Management Landscape

Sharing Identity information and enabling access to different resources has always been an issue in multi-service, single channel delivery environments. If we consider the Internet to be the channel of service delivery, we find multiple service providers and content providers. These providers use their individual user management and identity management systems to enable user access to the services, resulting in multiple logins and multiple identities for users. This is not only inconvenient but also inefficient. This is far more complex as compared to an enterprise in which the organization accords a singular identity.

Managing and handling identities in a typical Web model is more complex on account of multiple domains as opposed to a single domain in the enterprise. Identity federation provides just the right and effective mechanism for handling these issues. Federation literally means “united in an alliance.” “Identity Federation” thus is the mechanism by which a group of members who form a union collaborate on identity information.

Identity federation describes the technologies, standards, and use-cases that serve to enable the portability of identity information across otherwise autonomous security domains (CNIPA, 2008). The ultimate goal of the identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly and without the need for completely redundant user administration (ibid.).

The use of an identity federation has the potential to reduce costs, enhance security, and lower risk by leveraging stronger credentials to enable an organization to identify and authenticate a user once and then use that same identity information across multiple systems, including external partner systems (Manish and Sharman, 2008). It can arguably improve privacy compliance through identity authentication and authorization controls and drastically enhance citizen experience by eliminating the need for multiple registrations through automatic «federated provisioning» (Blakley, 2010).

The term «identity federation» is by design a generic term and does not refer to or imply any specific implementation technology. Identity federation can be implemented in any number of ways. Liberty Alliance, WS-Federation, and Shibboleth are examples of different frameworks and initiatives leading to trust establishment between different service providers. It addresses various identity verification and authentication development capabilities. See also Annex-1 for more elaboration on these frameworks. On the whole, many current systems are based on open standards and specifications, but there are many other frameworks and approaches in existence that are proprietary.

On the other hand, there are also many technical vocabularies and terms commonly used in every identity federation discussion. The general components that make up any federated identity management systems are depicted in Figure 1. The next section elaborates on the components.

2.1 Identity Provider (IdP)

An IdP is an entity that issues an identity to an individual or an entity and manages user authentication and user identity relevant information. It plays a key role in not only providing a digital identity but also authenticating the user and storing attributes about the user. Potentially, an identity provider offers the following:

1. Identification and authentication data: This can be used to inform the service provider who the user is, and the identity provider guarantees that it is really that user.

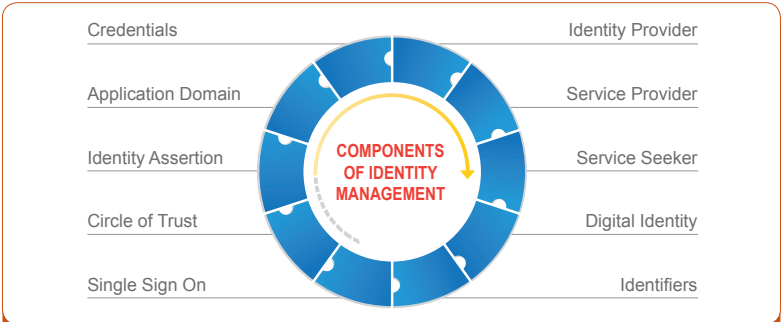


Figure 1: Identity Federation Consideration

2. Authorization data: This is meant to ensure that the user is allowed to perform a specified operation.
3. Personal profile details of the entity: If the identity holder permits it, this is based on a request from a service provider.

2.2 Service Provider (SP)

An SP (also referred to as relying parties) is an entity that offers services to users who seek any services based on the eligibility and provision of the services for users/service seekers. It basically provides services to the user and relies on the identity provider to perform user authentication.

2.3 Service Seeker

A service seeker is an identity holder and an entity that seeks services for individual or group consumption from a service provider. This could be a person, a group of people, an organization, a process, or even a device—i.e., any subject that is able to make a transaction (servers, network devices, people). The user interacts by using agents such as a browser with a service provider's online application and seeks a service.

2.4 Digital Identity

This is the electronic representation of the identity of an individual or an entity within a given applicable domain. This identity is generally a combination of different identifiers and credentials packaged for use in electronic transactions.

2.5 Identifiers

Identifiers are different attributes of a given digital identity. These compose the metadata related to a digital identity and constitute an identity profile (e.g., unique identity number, certificates, name, date of birth, address, or employment details).

2.6 Credentials

Credentials are a set of objects/elements that serve to authenticate an identity by means of the validation of its identifiers. This follows the (1) What does one know? (2) What does one have? (3) What is one's identity?

For example, credentials can be a password or a valid response to a challenge, constituting what the individual knows. A credential could be a digital certificate constituting what the individual has. Finally, a credential could be an inherent characteristic of the entity, such as a fingerprint, eyes, or voice. This defines what the individual is.

2.7 Domain of Application

This is the application scope in which the digital identity has validity (e.g., a government department, company, hospital, club, university, or the Internet). An individual may have several identities/roles within the same domain of the application. For instance, a doctor could become a patient in the same hospital where he/she works. A doctoral research student could double up as a lecturer in a University.

2.8 Circle of Trust

This is a trust relationship between involved stakeholders. Organizations that have built trust relationships to exchange digital identity information in a safe way preserve the integrity and confidentiality of the user's personal information.

2.9 Single Sign-On (SSO)

This allows users to authenticate with an identity provider and then gain access to different services provided by several service providers with no extra authentication.

2.10 Assertion

This is a piece of data produced by a security assertion markup language (SAML) authority that refers to an act of authentication performed on a user along with personal profile data as required. This assertion completes the circle of trust.

Having described the components of federated identity management, the next section presents the fundamental role of an identity provider in the overall federation ecosystem.

3. The Role of Identity Provider in the Federation Ecosystem

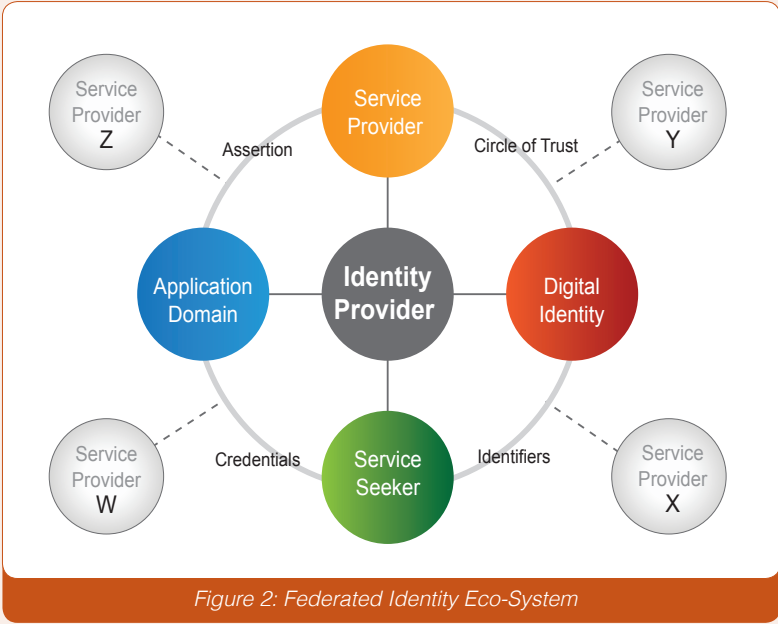
An identity provider plays a pivotal and key role in the overall identity management process (see also Figure 2). In the context of multi-organizations, the identity provider's role then becomes more crucial. For the overall ecosystem to operate successfully, trust must be established between service providers and the identity provider, both of which need to reach an agreement on the trust mechanisms enabled by the latter in relation to offered identification and authentication capabilities. Cross-domain identity management systems, by design, delegate the identification and authentication role to the identity provider. Service providers typically manage their own identity management systems, which determine the eligibility, accessible privileges, and the overall authorization functionality. Figure 3 illustrates how on a high level, identity federation and its management fit into this scheme.

An identity provider typically follows three processes that establish the identity of an entity (human or machine). These are as follows:

1. Enrollment Process: Registration of the entity, collecting various identifiers, and storing them for later verification and validation.
2. Digital Identity and Credentials Issuance: Credential generation, packaging the identifiers and credentials, and issuing the Identity for Assertion.
3. Authentication Capabilities: Verification and Validation of credentials and identifiers and establishment of the identity of an entity.

Identity federation management focuses on rationalizing these three processes with respect to managing the identity lifecycle, such as creation, update management, usage, revocation, and facilitation of the unification, sharing, or linking the digital identities of the users among different service providers across different application domains.

From a legal standpoint, governments have long been the de facto identity providers through the issuance of identity documents to their citizens and



IDENTITY ESTABLISHMENT	IDENTITY FEDERATION
Enrollment. Registration of the entity, collecting various identifiers and storing them for verification and validation later.	Rationalizing these Identity Establishment processes
Issuance. Credential generation, Packaging the identifiers and credentials and issuing the Identity for Assertion	Managing the ID Lifecycle
Authentication. Verification and Validation of credentials and identifiers and establish the identity of an entity	Facilitate the unification , sharing, or linking the digital identities of the users among different service providers across different application domains.

Figure 3: Roles of Identity Providers



residents—e.g., passports, ID cards, driving licenses, voter registration cards, and more. With the advancement of the Internet and remote service delivery, trust and identity assertion in the digital environment has become the need of the hour. Coping with such pressing needs, governments the world over have realized the need to modernize their identity management systems and initiate technologically-driven, digital identification infrastructure development programs that create digital identity profiles along with various electronic identifiers and credentials.

If we consider this to be the basis for identity federation, interoperability should be an easier exercise. Modern government identity programs in GCC countries fully fit these requirements and are compliant to all the design requirements of an interoperable and federated identity that can be used across borders. We further elaborate on this in the next section.

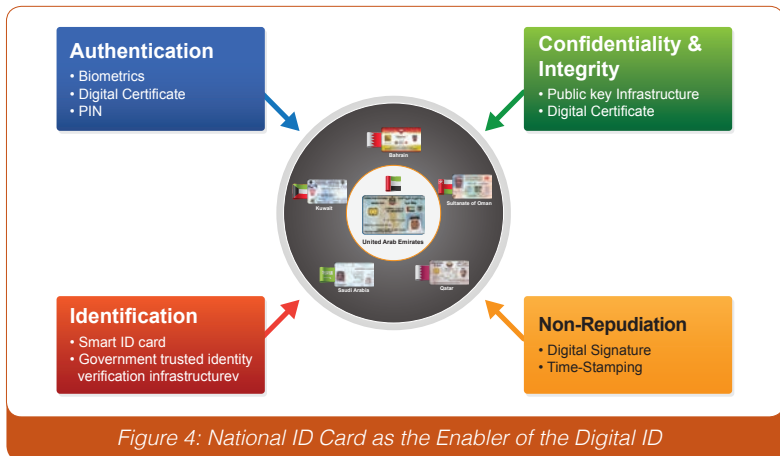
4. Identity Federation in GCC

All GCC countries have initiated modern national identity management programs in the last ten years. Each country issues smart chip-based identity cards that are associated with advanced technologies of public key infrastructure and biometrics (e.g., fingerprints, iris scan, and facial recognition). Identity management systems in GCC countries are backed by independent national identity legal frameworks.

Technologies and systems that constitute the digital identity in GCC countries are similar and are based on a similar set of identifiers and credentials. Figure 4 depicts the advanced capabilities provided by the smart identity cards in GCC countries.

In addition, smart cards in GCC countries are equipped with advanced functionalities that address digital transformation requirements, which include the following features:

1. Provided with identification parameters stored securely in the smart chip.
2. Establish a person's identity on-site, remotely allowing secure and trusted transactions.



3. Multi-factor authentication capabilities provide both match-on-card and match-off-card features and facilitate validation, verification, and authentication of an Identity.
4. The cardholder is accorded all identity services-validation, verification, authentication, and assertion of identity-from the respective national identity providers.

This indeed serves as a reliable platform to establish trust between different entities cutting across borders. Figure 5 depicts a generic framework adopted for digital identity issuance, identity services, and overall identity lifecycle management in GCC countries. It depicts the different layers that compose the current national identity management framework in each of the GCC countries.

The government is at the heart of the framework—the first, innermost layer—because GCC governments have realized the need to own the development of their digital economies through the development of digital identities. This is also based on the belief that a government-issued digital identity is likely to provide higher levels of trust and assurances, and would positively impact the uptake and usage by service providers. Each of the GCC countries has established independent entities and departments to act as an identity authority (identity provider), which provides the second layer of the framework. These entities and departments are responsible for the development of the infrastructure and provision of identity services (i.e., authentication and validation services). These are layers three and four. Service providers and citizens make up the fifth and sixth layers, respectively, as beneficiaries and users of the identity services. Identity lifecycle management creates the seventh layer and represents the integration platform with other government organizations to maintain automated data updation in case of changes to personal data .

In 2012, GCC governments initiated a large-scale project to make their national identity cards recognizable—digitally—across borders. Technically speaking, this should not be a difficult endeavor. The building blocks for an interoperability platform between GCC countries already exist in their national digital identity systems as they are based on common international standards and quite similar technologies.

Each of the GCC countries has set up a national validation gateway to provide authentication and validation services to both public and private sector organizations in their own countries. These gateways are designed to provide a federated identity for government-to-government and government-to-citizen transactions. For instance, when a user moves from one service provider to another, the assertion token is released to the second service provider, who trusts the authentication token generated

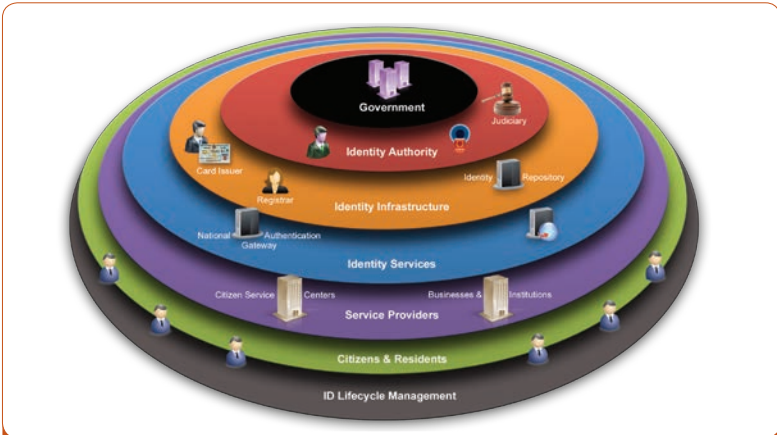


Figure 5: National Digital Identity—the GCC Context

5

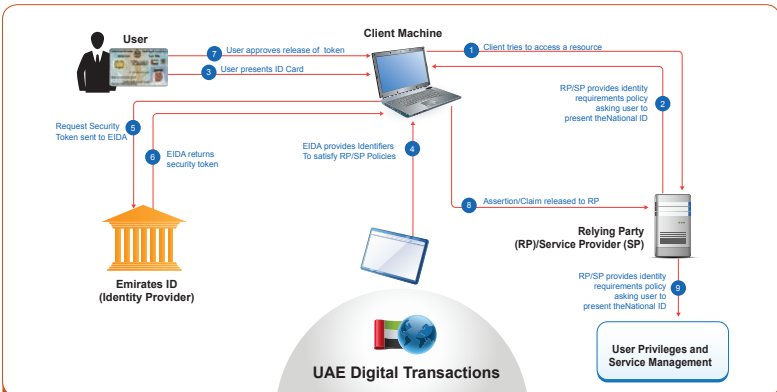


Figure 6: National ID Card and Federated Identity



in the first place. This ensures that across multiple service providers, the same authentication token can be used to trust the service seeker/ user without the need for the user to login or self-authenticate multiple times. In the e-government context, this token could be handed over to the e-government portal, and the e-government entity acts as the identity proxy. Figure 6 depicts how the national validation gateway has been set up in the UAE.

The GCC federated identity management concept is based on extending the services provided by national identity providers to the GCC bloc, where each identity provider will act as a proxy for each other. This will serve to bridge the identity providers in a seamless bind for individual digital identity holders across the identity providers. An authentication carried out by an identity provider in the UAE, for example, can be passed on as a “token” to the identity provider in Oman. The national validation gateway in Oman will then determine whether to grant or revoke access to the service or resource. See also Figure 7.

It is here in this context of interoperability that identity federation in the GCC countries becomes a crucial cog in the interoperability wheel. When this is extended to the GCC, the identity providers in other countries are accorded with the “Assertion” token (which is essentially an SAML token) from the home country (e.g., the UAE identity provider). See also Figure 8.

Efforts are already underway, and GCC countries have conducted multiple workshops on interoperability. Pilots are in the planning stage to ensure “recognition” of the ID cards using Web services. In fact, a common API was developed in 2011 to read public data, in offline mode, from the GCC smart identity cards, and is implemented at borders (airports and land and sea ports) in each of the six countries. The current working phase links the national validation gateway systems in all countries to provide online validation and verification services across borders. Figure 9 depicts a high level, tentative implementation plan of GCC eID interoperability project.



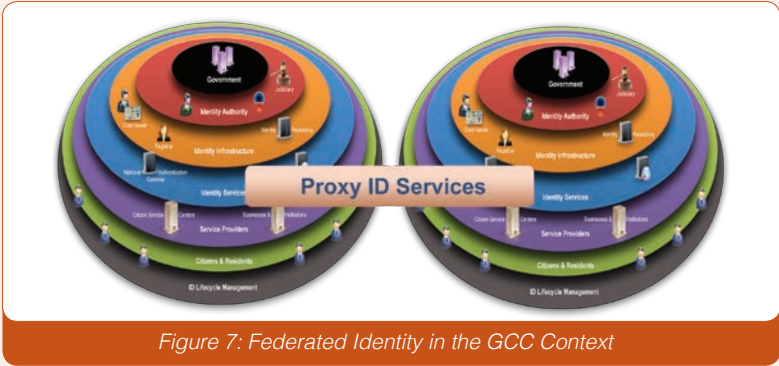


Figure 7: Federated Identity in the GCC Context

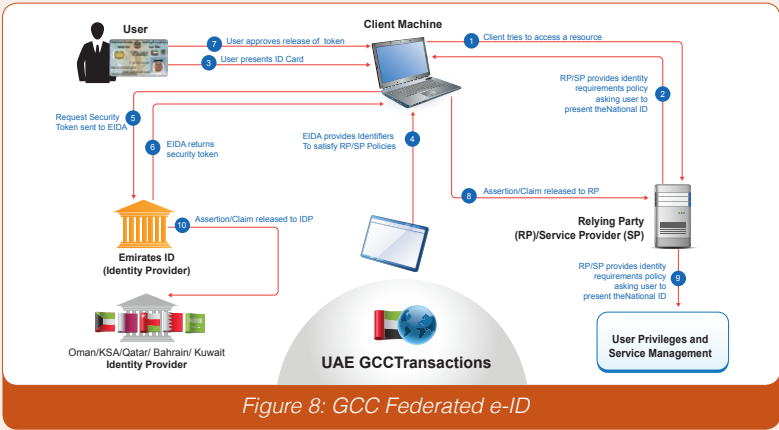


Figure 8: GCC Federated e-ID

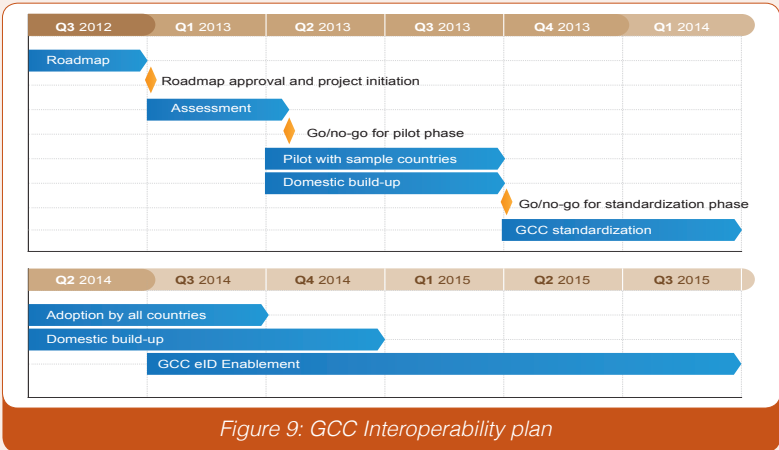


Figure 9: GCC Interoperability plan

5. Reflection

5.1 GCC e-ID Interoperability Platform vs. European STORK2.0

If we disregard the fact that there is still no formal charter document for GCC e-ID interoperability, the main difference from the European STORK and STORK 2.0 is in the current approach to interoperability. The federated eID is highly dependent on the existing national identity systems in GCC countries, through which identity validation is performed across borders. In essence, the overall objectives are the same as the STORK and STORK 2 objectives. Figure 10 depicts these objectives.

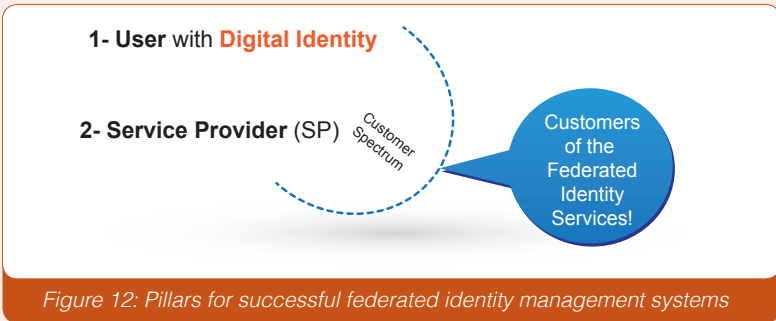
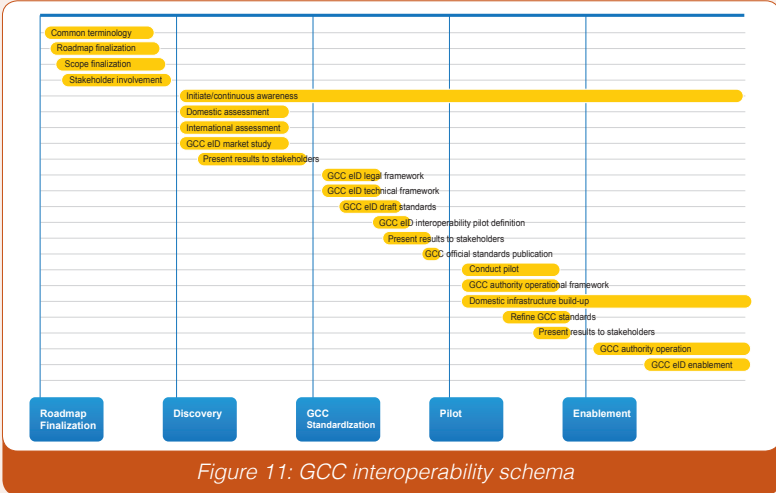
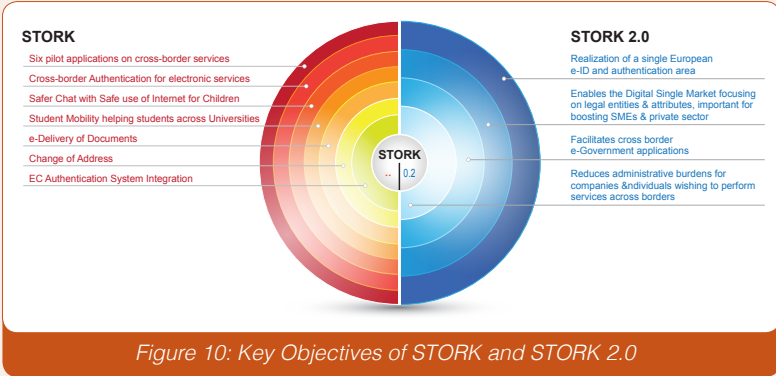
From a technical perspective, the GCC interoperability initiative is conceptually the same as the European initiative. The main differences lie in the approach and implementation. See also Figure 11.

GCC eID interoperability is driven by national identity management systems, from a vision that identification and credentials issued by governments are central to interoperability. However, the current GCC project scope is still narrow and focuses on cross-border identification and credential verification as principle priorities.

This prompts us to recommend that GCC governments broaden their visions on how such an interoperable eID platform will address more strategic future opportunities and how it can support the overall transformation of GCC countries and the development of sustainable digital economies.

5.2 Addressing the User Spectrum

Key to the development of a workable federated identity management system is meeting the needs and expectations of the customer spectrum—i.e., users and service providers, the ultimate beneficiaries of such systems. One of the creative yet simple models that we recommend is Kano's Model, also depicted in Figure 13. The main objective of this model is to help organizations understand three categories of customer needs and attributes so that new products or services are launched



successfully. The model classifies product attributes based on how they are perceived by customers and their effect on customer satisfaction (Kano et al., 1996). These classifications are useful for guiding design decisions in that they indicate when good is good enough, and when more is better (ibid.).

In principle, the model addresses three quality categories (also called Critical To Quality Characteristics (CTQs)):

- Dissatisfier – Must have – This is the absolute basic requirement that the product/service must meet. Without this, the customer will surely be dissatisfied.
- Satisfier – More is better – This defines improvization in the basic requirements or better performance in the basic requirement. These factors will enable the customer to be satisfied.
- Delighter – Meeting the latent need – These factors are differentiators. They bring delight, or the “wow” factor to the customer.

See also Figure 14.

The identity federation needs to be designed on such a quality basis. In a federated identity management project, it is imperative to define the service specifications based on the needs and expectations of our citizens and reach out to the delight levels of both ends of the customer spectrum. Governments need to focus on creating added value. Federated identity can bring significant value and can enhance online education systems, healthcare management (eHealth), government and public services, and overall IT infrastructure transformation. See also Annex-2.

The potential value of an Interoperable eID between countries is enormous. If designed with clear and concrete milestones and measurable outcomes, GCC countries will not only enhance their national security but will take giant steps toward the development of a true knowledge-based, digital economy (Al-Khouri, 2012; Landau and Moore, 2011).



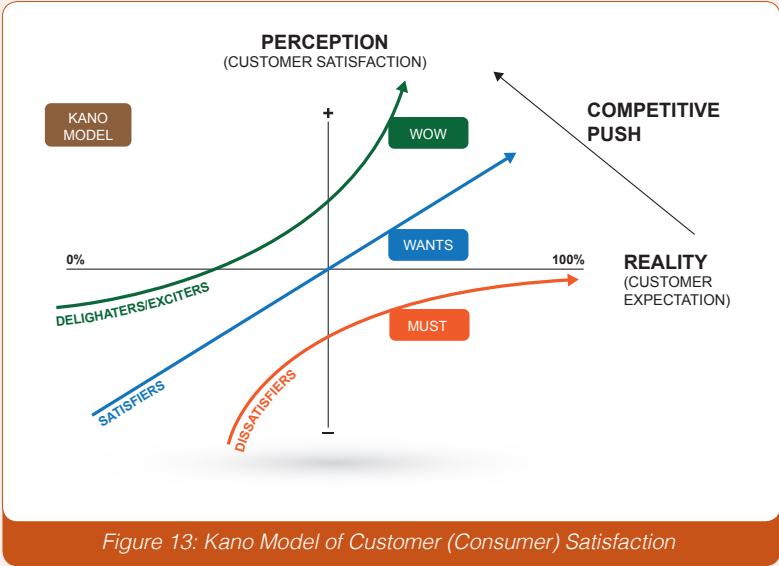


Figure 13: Kano Model of Customer (Consumer) Satisfaction

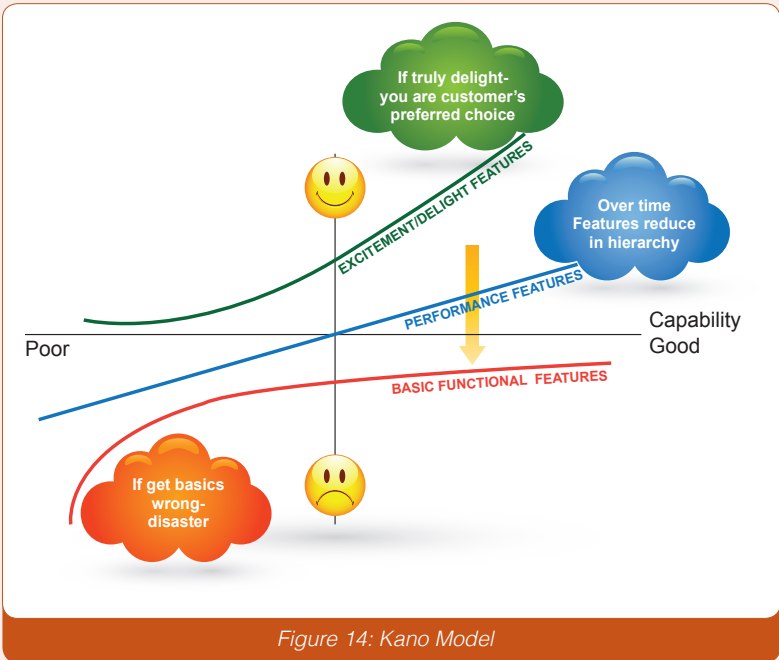


Figure 14: Kano Model

6. Conclusion

As indicated, it is certain that the benefits of a single PAN GCC digital identification and authentication area scheme are legion and will require the current economic cooperation between GCC countries to reach new and higher levels. A GCC eID interoperability platform should allow citizens to establish and conduct e-transactions across borders, just by presenting their national eID issued to them from their own home countries. Cross border user authentication has the potential to create benefits in different sectors and enhance access to education resources, commercial transactions, and banking transactions. The possibilities are endless.

GCC governments still need to work with each other to formulate a legal framework that sets the rules and defines how identity providers, service providers, and users will interact, and the overall framework in which identity verification and validation services will operate. They will need to broaden their visions and collaborate more closely to address future challenges and opportunities. An interoperable eID platform can indeed put GCC countries at the forefront in the digital economies arena and global competitiveness.

As a final note, interoperability will certainly become a precondition backbone for future development efforts at all levels. As the world gets smaller and more ubiquitously connected (with landscape geography having no meaning), countries and governments will need to act as one entity. A global eID platform will be an attractive objective in the near future. In fact, in the years to come, interoperability will become more associated with global sustainability; they will be two sides of the same coin. This will be a conundrum many seek to solve for years to come.

Acknowledgment

The content of this article was presented at World e-ID Congress: Identity Services for Government Mobility and Enterprise Conference, Sept 25-27, 2013, Nice, French Riviera, France.

References

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. 3, No. 2, pp. 57-69.

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.

Baldoni, R. (2012) Federated Identity Management Systems in e-Government: the Case of Italy, *Electronic Government International Journal*, vol. 8, no. 1, pp. 64–84. <http://www.dis.uniroma1.it/~midlab/articoli/EG6642.pdf>

Bertino, E. and Takahashi, K. (2010) *Identity Management: Concepts, Technologies, and Systems*. Boston, MA: Artech House Publishers.

Bhargavan, K., Fournet, C., Gordon, A.D. and Swamy, N. (2008) Verified Implementations of the Information Card Federated Identity-Management Protocol. Proc. of ASIACCS '08, Akihabara Convention Hall, Tokyo, ACM, pp.123–135. <http://prosecco.gforge.inria.fr/personal/karthik/pubs/verified-implementations-of-cardspace-asiaccs08.pdf>

Blakley, B. (2010) *The Emerging Architecture of Identity Management*. Gartner. http://www.ciosummits.com/media/pdf/solution_spotlight/gartner_emerging_architecture.pdf

Bruegger, B.P., Hühnlein, D. and Kreutzer, M. (2007) Towards global eID-Interoperability. *Biometrics and Electronic Signatures - BIOSIG*, pp. 127-140. <http://subs.emis.de/LNI/Proceedings/Proceedings108/gi-proc-108-012.pdf>

Buecker, A., Filip, W., Hinton, H., Hippenstiel, H.P., Hollin, M., Neucom, R., Weeden, S. and Westman, J. (2005) *Federated Identity Management and Web Services Security*. <http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf>

Cabarcos, P.A. (2013) *Dynamic Infrastructure for Federated Identity Management in Open Environments*. Doctoral Thesis. http://e-archivo.uc3m.es/bitstream/handle/10016/17202/tesis_patricia_arias_cabarcos_2013.pdf;jsessionid=020B2984187D0863B77F4090EEB1FD2A?sequence=1

Camenisch, J. and Pfitzmann, B. (2007) «Federated Identity Management», in Petkovic, M. and Jonker, W. (eds.) Security, Privacy, and Trust in Modern Data Management, Springer, Berlin / Heidelberg. <http://idemix.files.wordpress.com/2009/08/campfi06.pdf>

Chadwick, D. (2009) «Federated identity management», in Aldini, A.& Barthe, G.& Gorrieri, R. (Eds.), Foundations of Security Analysis and Design V, Lecture Notes in Computer Science, vol. vol. 5705, p.96-120.

CNIPA (2008) D2.3 Overall European Regulations and Standardisation. European Civil Registry Network. http://www.ecrn.eu/docs/standard_repository.pdf

Dalakian, G. (2012) 25 Essential Stats on E-Commerce in the Middle East. <http://www.wamda.com/2012/10/25-essential-stats-on-e-commerce-in-the-middle-east-stats>

Digitome (2011) Telemedicine. <http://digito.me/telemedicine/>

European Commission (2005) Study of the e-learning suppliers' "market" in Europe, Directorate-General for Education and Culture. http://ec.europa.eu/education/archive/elearning/doc/studies/market_study_en.pdf

Fleurus, C., Peijl, S., Zuuren, E., Wauters, P. and Whitehouse, D. (2011) Towards a Trusted and Sustainable European Federated eID system. European Commission. <http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/smart2010-0068.pdf>

Gartner (2013) Cloud Services Market In The Middle East And Northern Africa Region To Reach \$462.3 Million in 2013. <http://www.gartner.com/newsroom/id/2333517>

Goodrich, M.T., Tamassia, R. and Yao, D. (2008) Notarized Federated Identity Management for Web Services, Journal of Computer Security, 16(4), pp. 399-418. <http://cs.brown.edu/cgc/stms/papers/notarizedFIM.pdf>

Gupta, M. and Sharman, R. (2008) Dimensions of Identity Federation: A Case Study in Financial Services, Journal of Information Assurance and Security, 3, pp. 244-256. <http://www.softcomputing.net/jias/manish.pdf>

Kano, N., Seraku, N., Takahashi, F., and Tsuji, S. (1996), "Attractive Quality and Must-Be Quality", The Best Quality, IAQ Book Series Vol. 7, ASQC Quality Press, 165 - 186.

Kapoor, R. (2011) MIDDLE EAST: Online education is vital for the region. University World News. <http://www.universityworldnews.com/article.php?story=20110507091849885>

Landau, S. and Moore, T. (2011) Economic Tussles in Federated Identity

Management. In: 10th Workshop on the Economics of Information Security, June 14{15, 2011, Fairfax, VA. <http://weis2011.econinfosec.org/papers/EconomicTusslesinFederatedIdentityManagement.pdf>

Langenhove, P., Dirx, M. and Decreus, K. (2011) EUROPEAN INTEROPERABILITY ARCHITECTURE (EIA). European Commission- Interoperability Solutions for European Public Administrations Work Programme. http://www.difi.no/filearchive/eu-common-vision-for-an-eeia-final_1.pdf

Linkous, J. (2009) Telemedicine and Telehealth Outcomes Research, American Telemedicine Association. <http://www.capsil.org/files/TelemedicineandTelehealthOutcomesResearch.pdf>

Novell (2011) Staying Ahead of the Access Management Game with Federated Identity Technology. http://www.novell.com/docrep/2011/07/novell_access_management_federated_identity_technology_whitepaper_en.pdf

Porter, C. (2008) Achieving Full eID Mobility across Federated Political Domains: a Case for Mobile Identity with Operator and ME/SIM Platform Independence. European eID Card Conference, Leuven, Belgium. <http://www.cisforum.com/wp-content/uploads/2010/09/eIDCrossBorderInterop030308.pdf>

Rorissa, A., Potnis, D. and Demissie, D. (2010) A Comparative Study of Contents of E-government Service Websites of Middle East and North African (MENA) Countries. In C.G. Reddick (ed.), Comparative E-Government, Integrated Series in Information Systems, Springer, New York, pp. 49-69.

STORK (2013) What is STORK 2.0?. <https://www.eid-stork2.eu>

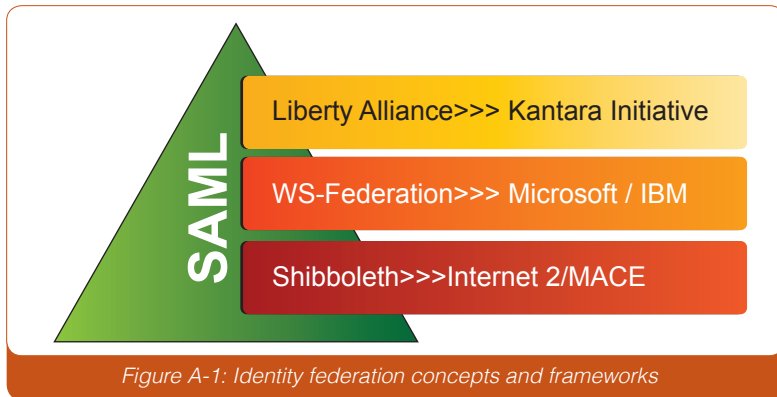
Whittake, Z. (2013) Gartner: Public cloud services to total \$131B by 2017. ZDNet. <http://www.zdnet.com/gartner-public-cloud-services-to-total-131b-by-2017-7000011958/>

Williamson, G., Yip, D., Sharoni, I. and Spaulding, K. (2009) Identity Management: A Primer. Big. Sandy, TX, USA: McPress.

World Health Organisation (2010) Telemedicine Opportunities and Developments in Member States: Report on the Second Global Survey on eHealth. http://www.who.int/goe/publications/goe_telemedicine_2010.pdf

Zwahr, T, Rossel, P, Finger, M (2005) Towards Electronic Governance - Gaining Evidence for a paradigm shift in Governance from Federated Identity Management. In Transactions of the ECEG, the 5th European Conference on E-Government (pp. 1-10). Antwerpen: s.n. <http://infoscience.epfl.ch/record/55874/files/e-gov.pdf>

Annex-1: Identity Management Frameworks



Liberty Alliance, WS-Federation, and Shibboleth are three well known ID management frameworks based on this principle of collaboration and sharing of identity information. Their initiatives are aimed at establishing trust between different service providers (relying parties). All of them utilize the identity verification/authentication methods based on open standards and use SAML Assertion. The following is a brief on each of the three frameworks.

- SAML is the foundation for all of the current identity federation mechanisms. It has gone through three releases: 1.0, 1.1, and (the most recently ratified) 2.0. SAML 2.0 is seen as a point of convergence as it incorporates Liberty Alliance's ID-FF 1.1 and 1.2 specifications as well as Shibboleth version 2 functionalities.
- Shibboleth is a «single-sign in» or logging-in system for computer networks and the Internet. Shibboleth is a project of Internet2/ MACE and seeks to develop the architecture, policy structures, technologies, and open source implementation, to support inter-institutional sharing of Web resources. This is of course subject to business rules and access controls that will allow inter-operation. This initiative seeks to provide peer-to-peer collaboration using a federated identity infrastructure based on SAML. Shibboleth has been largely adopted by university and research communities

around the world. Shibboleth 2.0, which was released in March 2008, is based on SAML 2.0.

- The Liberty Alliance is an organization of vendors and enterprises that is largely perceived as having formed in response to Microsoft's Passport efforts. Since that beginning, the Liberty Alliance has written several protocols that enable both browser-based identity federation as well as Web services identity federation. The Liberty Alliance protocols include the identity federation framework (ID-FF) and identity Web services framework (ID-WSF). Their ID-FF work, which originally resulted in two versions of the ID-FF specification, has now been incorporated into SAML 2.0. Liberty Alliance has also taken on the role of certifying conformance and interoperability of vendor products to federation standards. They provide testing services for SAML 2.0 as well as their own protocols.

The Liberty Alliance project has released its specifications for Identity Federation as open technology standards and guidelines for federated identity management. The guidelines include privacy protection and describe the requirements for handling identity information. The Liberty Alliance specifications include Identity Federation Framework specification for single sign-on, federated account linking, identity provider introduction, and global logout. It also defines messages and protocols for securing Simple Object Access Protocol (SOAP).

- The WS-* Federation started as a proposal from IBM and Microsoft to define how companies could share user and machine identities across corporate boundaries and across domain authentication and authorization systems. It defines a security framework for Web services and has developed a full suite of specifications driven by a collaborative effort among Microsoft, IBM, VeriSign, RSA Security, Ping Identity, and others.

Some of these protocols, such as WS-Security, have been submitted to and ratified by existing standards organizations, such as Organization for the Advancement of Structured Information Standards (OASIS). WS-* can be thought of as a suite of specifications for enabling secure Web services. This

collection of specifications, including WS-Trust, WS-Federation, and WS-Policy, is an evolving set of mechanisms for layering authentication, authorization, and policy across both single and multiple security domains.

Open ID

OpenID is a newer, “open, decentralized, free framework for user-centric digital identity” 3. OpenID is designed for users who want a single login for several applications on the Internet. The framework is driven by the needs of Web 2.0 applications such as blogs and wikis. OpenID has a much more lightweight nature and is not based on several layers of XML schemas, WS-* standards, or a variety of data formats and communication channels.

Whereas these latter specifications amount to several hundred pages, the OpenID specification is only 14 pages long. One could say that the other specifications satisfy an organization’s wish to provide advanced functionality and fine-grained control. Instead of using SAML to create identity assertions, OpenID uses the eXtensible Resource Descriptor Sequence. This metadata format utilizes eXtensible Resource Identifiers (XRIs) to identify users. After authenticating with an OpenID Provider (OP), the XRIs are validated by the OpenID Relying Partners(RP) before permitting access. Typically, the RP will host an authentication service that refers the user back to the selected OPs when first accessing the Web site. In essence, the OpenID mechanism does not appear to be much different from an SAML or WS-Federation use case.

Annex-2: Examples of the potential impact of an international, interoperable eID on different sectors.

- **Healthcare Management:** Providing access to healthcare services and insurance with a single identification and authentication. Healthcare has huge potential when viewed in terms of electronic health (e-Health) (World Health Organisation, 2010; see also Linkous, 2009). Telemedicine as a concept necessitates remote access and authentication. This is virtually non-existent today. Major healthcare centers, such as existing government hospitals in GCC countries, can potentially associate with the American/European partners in providing telemedicine facilities that can be driven by the identification and federated authentication of the patients (e.g., in accessing patient records). The global growth rate in telemedicine is estimated at 19% (Digitome, 2011). A population of over 380 million in the MENA region in 2013 (two thirds of which is rural) at a cost of \$385 per patient per year translates to \$97.5 billion. We take only 10% of this population for telemedicine—it works out to nearly \$10 billion. There are many other economic impacts that Telemedicine could create: e.g., saving on transportation costs, time, and manpower. None of these were considered in the calculations. Telemedicine will be extremely useful and cost effective when applied to the correctional institutions for the inmates. In terms of security, no transportation means no potential jail breaks, and secure identity ensures the prevention of fraud in health. There are many advantages.
- **Online Education:** Enhancing access to educational materials for students across universities. Online education is expected to grow at a healthy rate of 26% annually (at a conservative level). Considering the growth in population and the skill sets required, we have very few universities available. Online education is even lower as of today. If we consider that the Middle East needs 55 million skilled employees in the next 10 years, even if we cater to just half of them, the current education facilities will fall short. The opportunity window here is huge in terms of providing quality education online, and this needs strong identity management—specifically, identity federation—so that students gain access to

worldwide resources. So American universities, for example, can provide access to the learning material based on enrollment at local universities (see, e.g., European Commission, 2005; Kapoor, 2011).

- **Government Services:** Improve access to government services. Digital signature services for remote transactions are expected to exceed \$15 billion in the immediate future (with land deals and property transactions and e-enabled goods and services). Regarding e-Government services, just between the UAE and KSA, the e-Government payment transactions were published at a value of 4.7 billion AED and 2.8 billion SAR for 2012 and 2011 (Dalakian, 2012; Rorissa et al., 2010). Estimates of G2G, G2B, and G2C can be facilitated by using the national ID card. The potential is huge.
- **IT Transformation:** Identity As A Service (IdAAS) will be the cornerstone of IT transformation across the region, enabling the migration of conventional IT systems to cloud computing. The value of this transformation in pure economic terms is estimated at \$5 billion globally in the next five years. Cloud services are on the rise in the Middle East. As per market estimates, cloud services are valued at a staggering \$462 million in 2013 in the MENA region and are estimated to grow at 18% annually (Gartner, 2013). The world market today is estimated at \$131 billion (Whittake, 2013).

6

Identity Management in the Age of Mobilification¹

Abstract

In light of the staggering evolution of mobile technologies, the concept of mobility is gaining more attention worldwide. Recent statistics demonstrate mobile channels' increasing significance in outreach and service delivery. However, governments and businesses face a challenge in reaping the benefits of mobile platforms: how to confirm the authenticity of mobile users and transactions. Mobile devices, by design, are well suited for enabling authentication and digital signing services, similar to traditional PC and laptop environments. But although various implementations support different authentication schemes, they still do not instill sufficient levels of trust and confidence. In this article we explore the practice of mobile identity management. We provide an overview of how EU countries tackle mobile identity. The main part of the article sheds light on the solution framework adopted in the United Arab Emirates (UAE) to address, recently launched mobile government transformation initiatives. Taking into account the newness of the topic, the content of this article should fuel the current limited knowledge base and trigger debate around the presented approaches.

Keywords: *mobile identity, e-identity, mobility, m-government, e-government.*

¹ Please quote this article as follows:

Al-Khoury, A.M. (2014) "Identity Management in the Age of Mobilification", *Internet Technologies and Applications Research*, Vol. 2, No. 1, pp. 1-15.

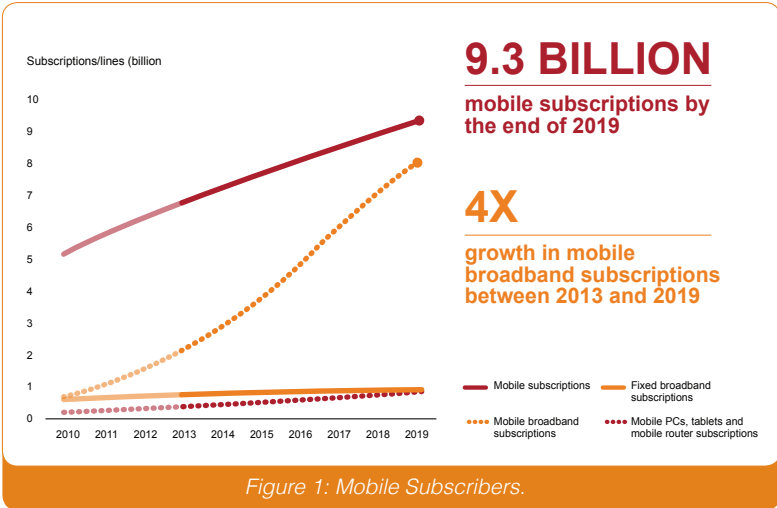
1. Introduction

The snowballing of mobile phones and smart devices has brought the concept of user mobility to the tables of policy makers and practitioners in government and private sectors. Today's citizens are unique, demanding, and participative (Jacobson 2001). Innovations in mobile devices and apps, directional and location-aware capabilities, personalization and cross-link experiences, all give citizens more control over where, when and how they engage with organizations. Mobile self-service business models are compelling niches into which organizations in all industries are moving (Macciola 2013).

User mobility means a single user's use of the same or similar telecommunication services at different places, with services following him or her (Sørensen 2011). Having recognized the opportunity, the mobile industry has been developing at explosive rates. Almost half the world population now uses mobile communications. According to the World Bank, global mobile penetration reached 91% in Q3 2013, with nearly 7 billion mobile subscriptions worldwide (Ericsson 2013; Fitchard 2013; ITU 2013; Portio Research 2013). See also Figure 1.

The mobile market is expected to grow even more strongly on the dimension of connections over the next five years, with 3 billion additional connections expected by 2017, representing annual growth of 7.6% (Atkearney 2013). In 2019, there will be 9.4 billion mobile subscriptions around the world, and 5.6 billion of them, or 60 percent, will be linked to a smartphone (Fitchard 2013).

In general, such constant increase in penetration means growth in the mobile app market as well. According to a recent study, 102 billion apps will be downloaded from mobile app stores in 2013, nearly 40 billion more than in 2012 (Gartner 2013). Total revenue of app downloads is also expected to increase from \$18 billion last year to \$26 billion by the end of 2013 (ibid.). See also Table 1.



Source: Fitchard 2013.

Table 1: Mobile App Store Downloads, Worldwide 2010-2016 (Millions of Downloads).

Region	2012	2013	2014	2015	2016	2017
Free Downloads	57,331	92,876	127,704	167,054	211,313	253,914
Paid-for-Downloads	6,654	9,186	11,105	12,574	13,488	14,778
Total Downloads	63,985	102,062	138,809	179,628	224,801	268,692
Free Downloads %	89.6	91.0	92.0	93.0	94.0	94.5

Source: Gartner (September 2013)

Although the mobile industry is growing at an incredible speed and pace as illustrated above, the business world has not yet taken full advantage of this platform. Among other challenges, identity management in mobile environments hinders progress. The foundation of any service delivery platform is the ability to verify identities. Mobile identity management practices are very fuzzy and confusing. No standard solution exists that may confirm the authenticity of the identity of mobile device user and of the transaction as well.



In this article we attempt to address this topic more pragmatically. We explore how governments are trying to handle identity management in mobile environments. To do so, we review practices in European countries, and also provide some detailed insights into developments in one of the emerging mobile markets, the United Arab Emirates. The UAE's solution, based on its national identity management infrastructure, is considered a practical case that may help practitioners understand how some foundational concepts of identity management can address challenging system requirements. Since no articles on the topic take a government perspective, this article should enlighten existing literature of what governments' role may look like in the mobile age.

It is structured as follows. In section 2, we provide statistical data around the growing mobile industry. In section 3, we attempt to define and correlate electronic identity and mobile identity, aiming to pinpoint the basic questions about authentication requirements. In section 4, we review a study on mobile identity management practices in Europe. In section 5, we present the case of the UAE, and show how the government is trying to leverage its existing national identity management infrastructure to support a mobile transformation of government services. In section 6, the article concludes with reflections and thoughts for further research.



2. The Age of Digital Mobility

Mobile telephony meant that instead of calling a place you could call a person. Similarly, having long been seen as a separate place, accessed through the portal of a PC screen, the internet is fast becoming an extra layer overlaid on reality, accessed by a device that is always with you (and may eventually be part of you). In the coming years, that will be the most profound change of all (Standage 2013).

Digital mobility is perhaps the most important trend emerging from exponential advances in computing and mobile revolution. Digital mobility is not only driving new growth opportunities, but also dramatically changing how business is conducted and customers reach out. While it took AOL 9 years and Facebook 9 months to reach one million users, it took less than 10 days for online gaming tools such as Draw Something and Line Pop to reach a million-user milestone. This is largely attributed to the high penetration rates witnessed by the globally growing enhanced and Internet-capable mobile devices in the last few years. As such, mobilification, the conversion of existing content for use on mobile devices has become the new buzz word.

For quite some time, access to the Internet came only through PCs and laptops, or perhaps through a mobile app, but as mobile devices have become more popular and more capable, they have become a far more promising platform (Standage 2013). By 2014, mobile Internet usage is envisaged to overtake desktop usage (ibid.). See also Figure 2.

The rise of the mobile internet is also foreseen to transform governments and major businesses. Forrester predicts mobile commerce to reach \$31 billion by 2016 (Mulpuru et al. 2011). Other statistics show mobile payments² are considered by far the greatest opportunity for market growth (Kumar and Venkata 2011). According to Juniper Research, the sector should grow from \$170 billion in 2010 to \$630 billion in 2014, due to the increase in use of smartphones and traffic through app stores (Wilcox 2010).

² M-payments can be defined as any payment transactions, whether in close proximity or remote, executed on mobile devices, except for Internet payments made through mobile phones.

Then again, while most organizations in public and private sectors are aware of the rising importance of mobile channels to their customers and their businesses, many struggle to understand how to use this platform to serve and support their customers (Accenture 2010). Their visibility is obstructed by technology's evolving and disruptive nature. Their greatest challenge, though, remains identity management.

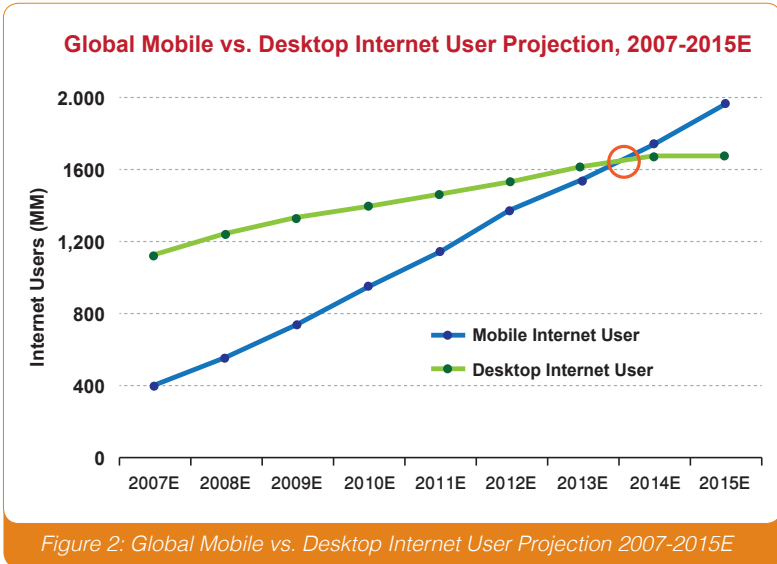


Figure 2: Global Mobile vs. Desktop Internet User Projection 2007-2015E

3. Electronic Identity

Definitions of digital identity vary with regulatory contexts (Lenco 2013). For example, the European Commission's proposed regulation defines electronic ID as "the process of using personal identification data in electronic form unambiguously representing a natural or legal person" (European Commission 2012). As depicted in Figure 3, electronic identity serves as a proxy for real identity, be it for an individual or an organization, and complements the real identity. It then becomes a representation of a set of credentials submitted by an entity to another entity to assert and confirm the identity. Mobile identity is essentially an extension of electronic (digital) identity provided via mobile networks and devices.

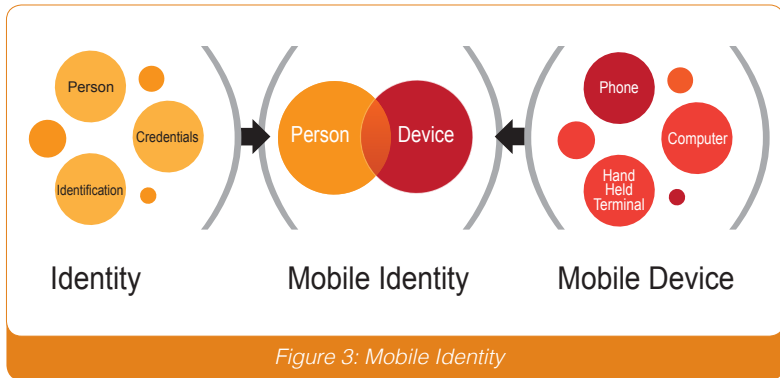
Statistics above suggest billions of identities are accessing millions of mobile applications, trillions of times a day. Here lies the criticality of identity and the need for an authentic digital proxy to for the real identity. This in turn leads us to the two dimensions of mobile identity, and prompts us to address a principal question: should we identify the mobile device, or mobilify the identity?

Mobilifying identity is extending a given digital identity to the mobile ecosystem. Mobile identity used to relate only to mobile telephony. Users could be identified by mobile phones through SIM cards and phone numbers. Telecom operators managed identity and access. But as mobile devices evolved from mere voice communication and simple data transfer tools to Internet-capable mini-computers, existing mechanisms failed to be a secure platform for business transactions and service delivery. Mobile devices could be used by anyone, so how could we ascertain that a SIM card is in the hands of the rightful owner? Could telecom operators solve this issue on their own? Will such solutions provide the necessary assurances and address potential misuse concerns and share liabilities? Although solution providers and consultants may come up with shinning answers, existing solutions have yet to convince policy-makers in the government.

In other words, many existing authentication solutions are insecure or inconvenient, and do not holistically address data security and privacy threats. Other challenges also relate to:

- Commercial feasibility: cost and scalability of the solution, clarity of the stakeholders' roles, number of concrete customer references;
- Technological feasibility: availability of standards, handset support and platform interoperability;
- Overall security levels: resistance to man-in-the-middle and phishing attacks, strength of data protection; and
- Usability of the solution in enrollment, activation and usage processes.

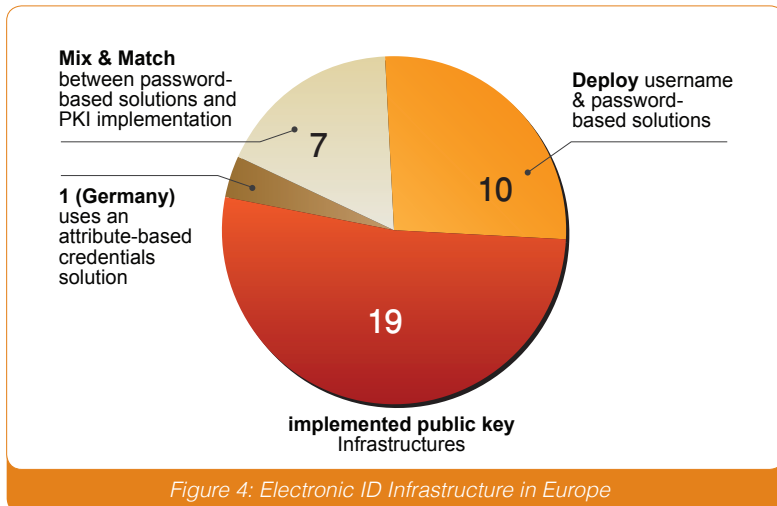
Key issues are device and user authenticity. In business terms, the typical default status we have in mobile environments is an “unauthorized device” (UD) with an “unauthenticated user” (UU). So the primary question left to answer is, how can we identify that the mobile device is authorized by its rightful owner? European countries have addressed this issue.



4. Mobile Identity Practices in Europe

European countries have deeply probed the full impact of digital technologies on their societies (BCG 2012). They have hosted substantial work in the field of identity management, which contributes to the expansion of theory and practice. EU countries are recognized for their notable progress in the field of digital authentication platform development (See Annex 1 and 2). Mobile authentication, although not as thoroughly addressed, but are included in part of generic themes. Practices widely vary from one country to another (See Annex 3). Figure 4 summarizes the mobile authentication solutions and citizen e-signature schemes adopted in 37 European countries.

Nordic and Baltic countries use a multitude of both password-based systems and PKIs. These systems are run collaboratively with banks and mobile network operators. The majority of the password-based systems are one-time-password (OTP), largely used to logon to online banking sites. Only in two Nordic countries, Denmark and Norway, do public authorities institute mobile identities based on OTPs.



Nordic countries are early adopters of mobile PKI solutions in Europe, but mainly run by private parties. Telecom companies and banks have, for instance, developed and operated SIM-based mobile BankID in Finland, Latvia, Norway, Sweden, and Lithuania. The only exception is Estonia, where the success of the national eID card encouraged the government to introduce its mobile version, Mobiil-ID.

Germany uses an attribute-based credentials solution. Pre-pilots are underway to test mobile authentication with German eID-cards and NFC-enabled smartphone. Politicians are as yet undecided.

In general, mobile identity solutions used in Europe and applicable worldwide come in one or more of five forms:

1. Username and password authentication;
2. MSISDN (phone number)-based authentication solutions;
3. Simple one-time-password (OTP), generated locally or remotely and sent by SMS;
4. Mobile PKI solutions (SIM-based and server-based); and
5. Smart card with NFC-based approach: using either mobile device to act as a reader and secure element, or through using NFC-enabled SIM.

Although the last two approaches listed above boost security, the earlier three are fraught with drawbacks because their overall security depends on that of the GSM network and their authentication process is local to the phone and can be defrauded.

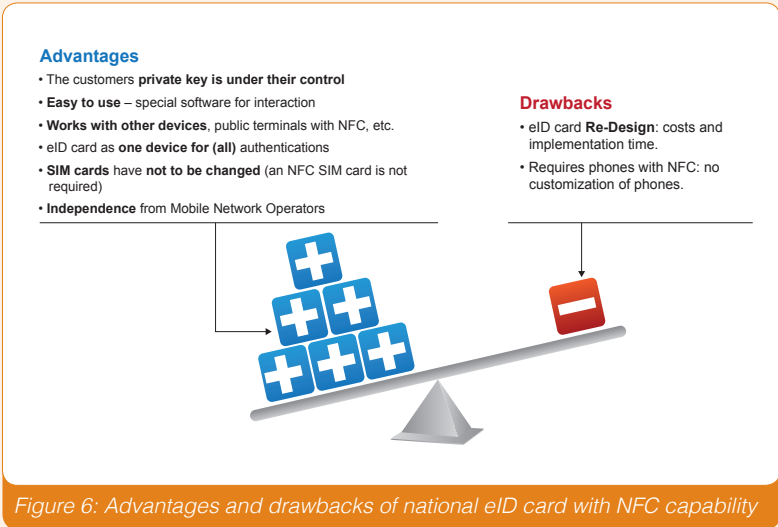
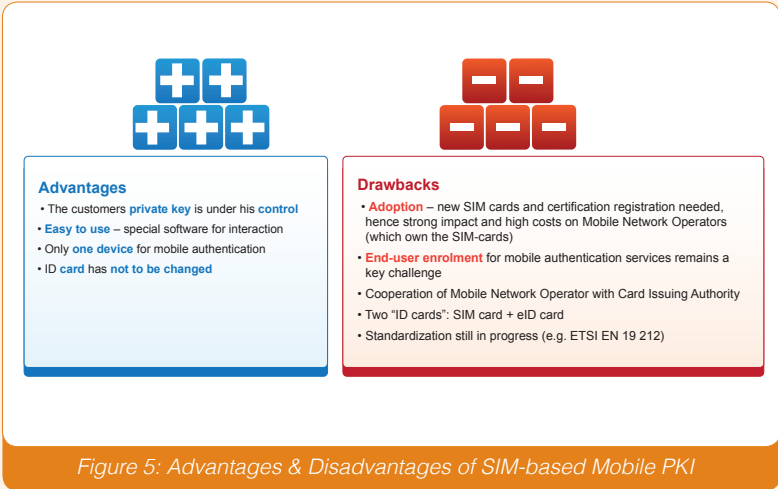
Two of the best authentication mechanisms for providing high levels of security are digital certificates (PKI credentials) and one-time passwords (OTPs). Cloud computing and mobile technology has paved the way for PKI to flourish in Europe and become an IT security game-changer. Turkey, Estonia, and Finland use mobile PKI with special SIM cards. SIM cards come with keys and signature algorithms, where the SIM becomes a “signature creation device.” Figure 5 depicts the advantages and disadvantages of SIM-based mobile PKI solutions.



However, the fifth solution listed above—eID smart card with NFC—is an approach few governments are trying but one that heightens security assurances. The approach relies on mobile devices with NFC capabilities as an ID card reader. The contactless feature of the eID card establishes communication between the card and the phone. The major challenge facing governments is the limitation of existing eID infrastructures to enable PKI communication in contactless mode. Most existing national ID card designs restrict PKI access to only be established in contact mode; ID card need to be inserted into a smart card reader. Figure 6 lists the pros and cons of the approach.

Attempting to explain this latter approach in more detail, the next section will survey its use in one of the world's renowned identity management infrastructures; UAE.





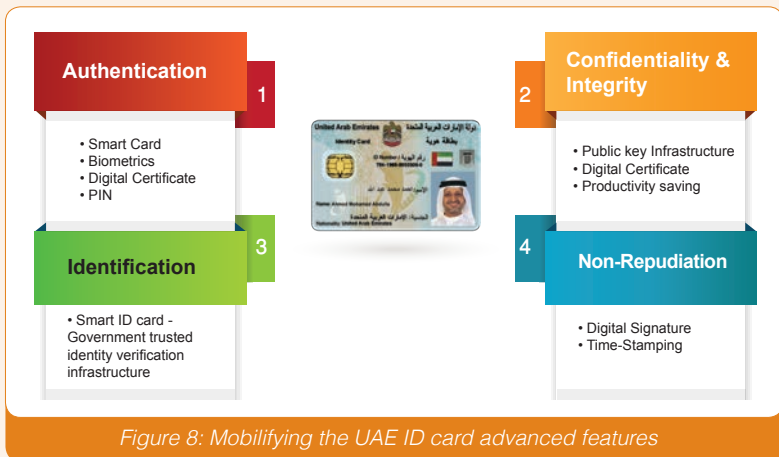
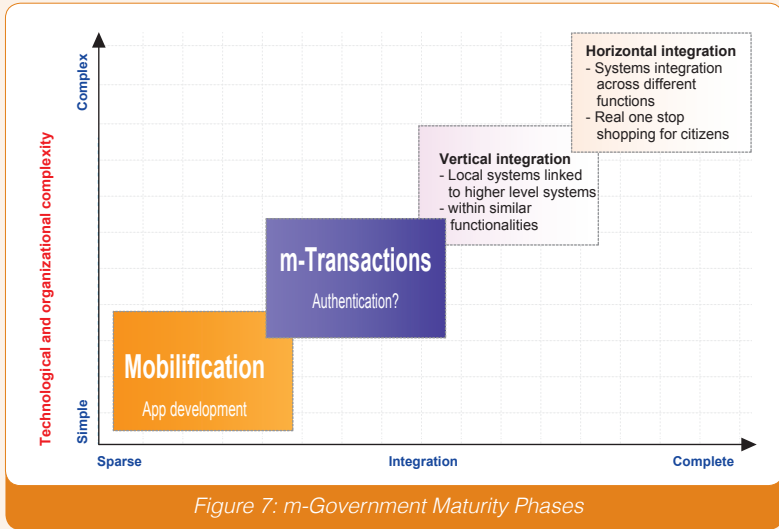
5. UAE Smart Government Initiative

The UAE announced recently its intention to deliver all government services through smartphones and devices under a scheme named “Smart Government.” The scheme is an extension of the e-Transformation path of government services that work twenty-four hours and operate as a “one mobile stop shop.” All government agencies are now mobilizing, developing mobile apps and enabling mobile payments to process government fees. See also Figure 7. However, the biggest challenge government agencies face remains the identification and authentication of individuals in mobile environments.

The current and widely used authentication approach is still based on usernames and passwords. All mobile phone users in the UAE need to register their SIM cards with National IDs under scheme called “My Number, My Identity” (TRA 2013). This registration transforms a default “unauthorized device” into a registered authorized device. Mobile phone and smart device users are prompted to set a PIN during the registration process for logon. Although the basis of “Authorized-Device-Authenticated-User” (AUAD) has been met, the overall approach is still not considered robust in digital security.

The UAE is therefore using its existing identity management infrastructure to heighten the security levels in mobile platforms. That infrastructure is based on sophisticated technologies such as NFC-enabled smart cards, biometrics, and public key infrastructure (Al-Khouri 2011; 2012a). The infrastructure is designed to support both national security and digital economy development (Al-Khouri 2012b).

As such, the UAE smart identity card comes with a complete digital identity profile, and current infrastructure supports digital identification and authentication of identities through desktops and laptops equipped with smart card readers. The government is now mobilizing its existing identity card features by extending the digital profile to the mobile ecosystem. Figure 8 illustrates the advanced features of UAE identity



cards. All these features—the use of multi-factor authentication with mobile phones, and PKI-enabled security levels of confidentiality, integrity, and non-repudiation—have yielded successful test results.

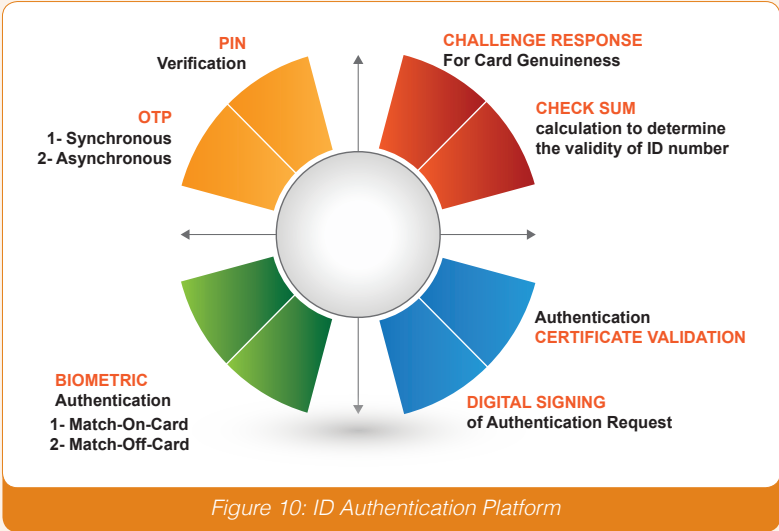
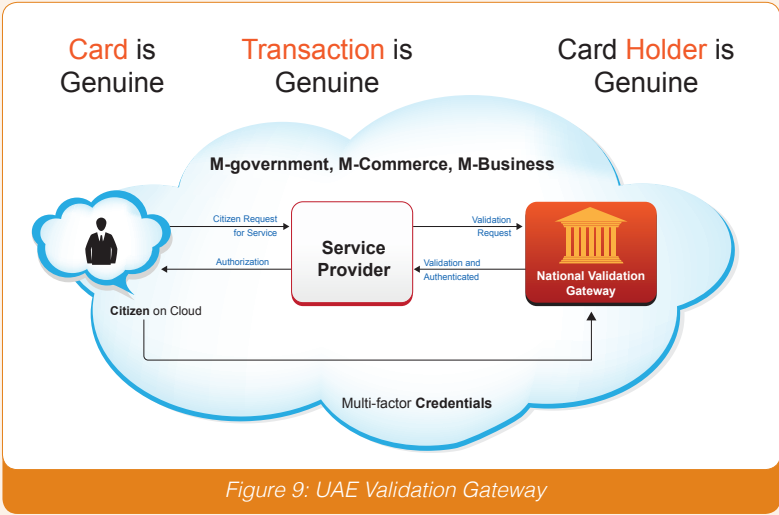
Besides, the UAE has set up a national validation gateway to provide online, real-time identification and authentication services to ID card-based transactions (Al-Khoury 2012c). So in principle, the digital and mobile identity involves the use of a national gateway to provide more secure, online, real-time validation, verification and authentication of credentials: card, transaction, and holder genuineness. See Figure 9.

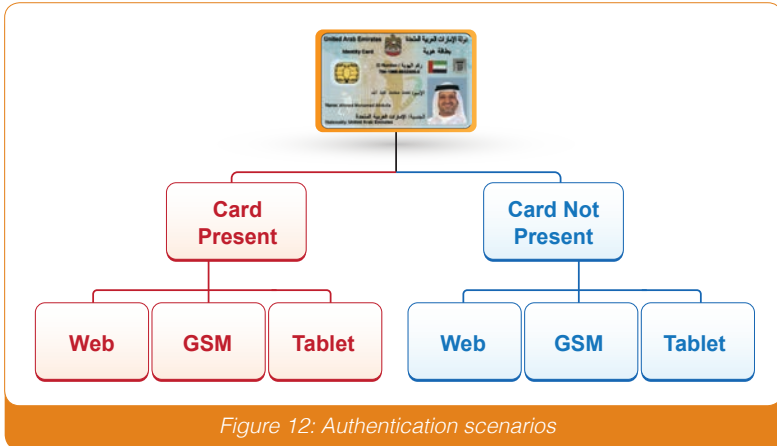
In the “card present” scenario, the digital ID credentials provide the perfect identification and authentication tools for both in-band and out-of-band modes. A mobile device can read the card using contact or contactless interfaces. Thus, whether the device is a phone, tablet, mobile PC, or handheld terminal, if it can read the card, the gateway validates online ID.

This does not thus warrant any further identity or device registration process in the future. The “card genuine” check and data integrity authenticates identity, and provides the authentication response to the service provider with the Government Issuing Authority’s digital signature. The digital signature certificates in the card, accessible by PIN, allow any transaction. The validation gateway thus provides multiple authentication mechanisms. Figure 10 depicts the range of them.

In simple terms, and as depicted in Figure 11, users typically need to download onto their smartphones or mobile devices a government mobile app with NFC reading capability—either built-in or as external plug-in hardware. Users will need to tap their card only when authentication is required, and the phone will act as a secure element that will interface with the validation gateway.

The above design supports the “card present” scenario and provides maximum trust for mobile identities. See also Figure 12. However, the government comprehends that in the “card not present” scenario, ID





services need to be just as strong and secure. Subsequently, an identity authentication platform that accords these services using the national identity management infrastructure brings true mobilification of the digital identity.

In the case of the ID card's absence, the challenge is to find additional proxies that serve the real ID as efficiently and effectively. Considering that true mobility goes beyond phones with SIM cards, the ID authentication platform should be able to provide the ID verification and authentication services independent of the devices.

A mobile phone of course serves the purpose of a secure mobile digital ID proxy if the SIM/ UICC³ registration is done in conjunction with the national ID card. Thus for every SIM issued, there needs to be at least a one-to-one (1:1) correlation of the SIM with the national ID card. It could then be extended to accord an n:1 correlation of the SIM with the national ID card (with multiple SIM cards issued to a given national ID).

The national ID credentials set is planned to further expand to provide:

1. IVR credentials, by enabling a national ID cardholder to register the ID card with a T-PIN (Telephone PIN);
2. An SMS-based credential set, by enabling the registration to an SMS-based challenge-response with a registered phone;
3. A USSD-based credential set by enabling the registration to an SMS-based challenge-response with a registered phone;
4. Biometric credentials, including voice and face recognition; and
5. A call-in (call-back) facility for ID verification and authentication.

Major new developments in electronic ID regulation are also taking place in the UAE. Digital identity and electronic signature (e-Identification, eAuthentication and eSignature) framework is under review by a federal committee. The legal framework is designed to support building trust in digital environments and interactions, and support the transformation of government services through leveraging the national identity management infrastructure. That structure will play a critical role in enabling secure and seamless electronic transactions between businesses, citizens, and administrations, thereby improving public and private electronic services, e-business and e-commerce.

Additionally, the overall framework provides cross-border interoperability of stronger forms of identification and authentication, such as eID. All in all, its e-authentication platform and legal framework show the UAE government plans on more stringent rules for service providers, in terms of security, data protection, and overall trust requirements.

³ SIM (Subscriber Identity Module) has given way to UICC (Universal Integrated Circuit Card). UICC is the same as the smart chip used in national smart ID cards today and will support mobility as per the GSM Association of mobile operators. UICC is expected to help identify user and application. It has on-board processing capabilities and thus can carry applets and run algorithms. It can communicate using Internet Protocol (IP), the same standard used in the Internet and the new generation of wireless networks. It also can support multiple PIN codes, which better protect one's digital profile and personal information.

6. Concluding Remarks

Although technological advances may substantially improve some aspect of an agency's operations, be it a government or a business, they can also create their own set of challenges that must be addressed to achieve the intended benefits. As such, they are double-edged swords (Accenture 2010).

The ever-changing expectations of communication options with government agencies and businesses will continue to create need for more tightly integrated experience across various heterogeneous digital channels. Emerging mobile technologies, access, and capabilities will regenerate citizens' expectations for immediate and self-service experiences.

Amid all this, governments need to develop digital mobility strategies and put in place action plans to ensure that they are not left behind. Indeed, the future impact of mobile devices on fields such as insurance, banking, education, training, and healthcare can only be guessed (Jacobson 2001).

Establishing trust should be the heart of such plans. Trust is crucial to electronic interactions between users, governments, and the private sector. Governments need to work beyond simple username/password schemes, and provide stronger authentication methods that support security, privacy, and safety in online environments (Lecon 2013). Building trust in online and mobile environments is critical to the growth of digital identity services and digital economies as a whole, and should become a preoccupation of governments and regulators around the world (*ibid*).

Governments need to understand that today's digital ecosystem is dramatically different from what it was few years ago. To protect citizens in cyberspace, all players—governments, network operators, device manufacturers and application/content developers—must work together (Juniper Networks 2012).

Identification and authentication issues will, in our opinion, remain a barrier, hindering the full potential of the digital (mobile) economy. Unless we have complete ID authentication architecture, it is practically impossible to prevent masquerades and identity thefts, abuse of the digital ID proxy and fraudulent transactions. Two basic questions will always need to be asked when evaluating any mobile ID solution:

1. How do we ensure that the identity is authentic?
2. How do we prove that the transaction is genuine?

The UAE's national validation gateway extension is fundamental for true m-government transformation. The UAE mobile identity authentication architecture provides robust and reliable mechanisms to authenticate mobile identities and pave the way for revolutionary mobilified business models.

We foresee modern national identity programs, becoming more prevalent around the world, would serve the purpose of mobile identity best. Governments have been working eagerly to address cyberspace's challenges and exploit its potential, but success is very limited. To make a true quantum leap, practitioners need to move out of their comfort zones, to examine digital transformation needs. Such examination should take into account overall political, economic, societal, technical, legal and environmental dimensions.

The content of this article aimed to fuel and trigger thoughts in this crucial embryonic field. Subsequent qualitative research could show how governments and businesses worldwide are addressing mobile identity in more detail and attempt to provide a feedback mechanism to understand current efforts and plan for future ones. Further research could also determine the best collaboration models between governments and business organizations in addressing mobile identity aspects. As mobility will likely remain the driving paradigm of technology and computing, research is needed to look at the ecosystem in more universal terms, critically evaluate threats and examine vulnerabilities. This research should guide and enlighten practices, and avoid jumping to "solutions" without understanding the problem!

References

Accenture (2010) Mobility and Customer Service: Tapping into an Increasingly Powerful Channel. http://www.accenture-blogpodium.nl/site/wp-content/uploads/2011/03/Mobility_in_Service_PoV.pdf

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.

Al-Khouri, A.M. (2012a) «PKI in Government Digital Identity Management Systems», *Surviving in the Digital eID World*, *European Journal of ePractice*, No. 4, pp. 4-21.

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

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

AT&T (2013) The Mobile Economy 2013. <http://www.gsma-mobileeconomy.com/GSMA%20Mobile%20Economy%202013.pdf>

BCG (2012) The Value of Our Digital Identity. Boston Consulting Group. <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>

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

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

Daniels, Matt (September 23, 2010). «Businesses need to get in the game». *Marketing Week*. <http://www.marketingweek.co.uk/disciplines/market-research/opinion/businesses-need-to-get-in-the-game/3018554.article>

Ericsson (2013) Ericsson Mobility Report: On the Pulse of the Networked Society. <http://www.ericsson.com/res/docs/2013/emr-august-2013.pdf>

European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Council of the European Union. <http://register.consilium.europa.eu/pdf/en/12/st17/st17269.en12.pdf>

Fitchard, K. (2013) Ericsson: Global smartphone penetration will reach 60% in 2019. <http://gigaom.com/2013/11/11/ericsson-global-smartphone-penetration-will-reach-60-in-2019/>

Gartner (2013) Forecast: Mobile App Stores, Worldwide, 2013 Update. <http://www.gartner.com/newsroom/id/2592315>

Global Finance (2013) <http://www.gfmag.com/tools/global-database/ne-data/11942-internet-users.html#axzz2lShDnnKF>

Guillen, M. F., & Suárez, S. L. (2005). Explaining the global digital divide: Economic, political and sociological drivers of cross-national internet use. *Social Forces*, 84(2), 681-708.

Herger, Mario (May. 21, 2012). «Gamification Facts & Figures». Enterprise-Gamification.com.

Huotari, Kai; Hamari, Juho (2012). «Defining Gamification - A Service Marketing Perspective». *Proceedings of the 16th International Academic MindTrek Conference 2012, Tampere, Finland, October 3-5*. http://www.hiit.fi/u/hamari/Defining_Gamification-A_Service_Marketing_Perspective.pdf

Internet World Stats (2013) <http://www.internetworldstats.com/stats.htm>

ITU (2013) ICT Facts and Figures. ITU World Telecommunication. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>

Jacobson, D. (2011) Digital mobility drives you – You drive digital mobility. PwC Technology Consulting Services. http://www.pwc.com/en_CA/ca/technology-consulting/technology-advisory/publications/digital-mobility-white-paper-2011-11-en.pdf

Juniper Networks (2012) 2011 Mobile Threats Report. <http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf>

Kumar, S. and Venkata, V.P.S. (2011) Mobile Payments: How Can Banks Seize the Opportunity? An Approach for Financial Services Institutions. Capgemini Consulting. http://www.capgemini.com/sites/default/files/resource/pdf/Mobile_Payments__How_Can_Banks_Seize_the_Opportunity_.pdf

Layne, K, Lee, Jungwoo (2001), Developing Fully Functional E-government: A four-stage model, *Government information quarterly* 18(2): 122-136.

Lenco, M. (2013) Mobile Identity: A Regulatory Overview. GSMA. <http://www.gsma.com/mobileidentity/wp-content/uploads/2013/03/Mobile-Identity-A-Regulatory-Overview-FINAL-Feb2013.pdf>

Lim, I., Coolidge, E.C. and Hourani, P. (2013) *Securing Cloud and Mobility: A Practitioner's Guide*. Auerbach Publications.

Macciola, A. (2013) How Mobile Apps Can Customize Customer Service. CIO Network. <http://www.forbes.com/sites/ciocentral/2013/01/14/how-mobile-apps-can-customize-customer-service/>

Mossberger, Karen, Carolina J. Tolbert, and Michele Gilbert. 2006. Race, Place, and Information Technology (IT). *Urban Affairs Review*. 41:583-620. retrieved from <http://uar.sagepub.com/content/41/5/583>

Mulpuru, S., Evans, P.F., Sehgal, V., Ask, J.A. and Roberge, D. (2011) *Mobile Commerce Forecast: 2011 To 2016*. Forrester Research <http://www.forrester.com/Mobile+Commerce+Forecast+2011+To+2016/fulltext/-/RES58616?objectId=RES58616>

O'Brien, Chris (October 24, 2010). «Get ready for the decade of gamification». San Jose Mercury News. http://www.mercurynews.com/ci_16401223

Portio Research (2013) *Portio Research Mobile Factbook 2013*. <http://www.portioresearch.com/media/3986/Portio%20Research%20Mobile%20Factbook%202013.pdf>

Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke (2011). «From game design elements to gamefulness: Defining «gamification»». *Proceedings of the 15th International Academic MindTrek Conference*. pp. 9–15.

Sørensen, C. (2011) *Enterprise Mobility: Tiny Technology with Global Impact on Work (Technology, Work, and Globalization)*. Palgrave Macmillan.

Standage, T. (2013) *Live and unplugged*, *The Economist*. <http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/>

TRA (2013) *My Number My Identity*. Telecommunication Regulatory Authority. <http://www.tra.gov.ae/mynumber.php>

Whitehouse (2012) *Digital Government: Building a 21st Century Platform to Better Serve the American People*. <http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf>

Wilcox, H. (2010) *Mobile Payment Markets - Strategies & Forecasts 2010-2014*. Juniper Research. http://www.juniperresearch.com/reports/mobile_payment_markets

Wilson, III. E.J. (2004). *The Information Revolution and Developing Countries*. Cambridge, MA: The MIT Press.

Zichermann, Gabe; Cunningham, Christopher (August 2011). «Introduction». *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps* (1st ed.). Sebastopol, California: O'Reilly Media. p. xiv. ISBN 1449315399. Retrieved 2012-12-10.

Annex 1: EUROPEAN E-ID SOLUTIONS CONNECTING CITIZENS TO PUBLIC AUTHORITIES

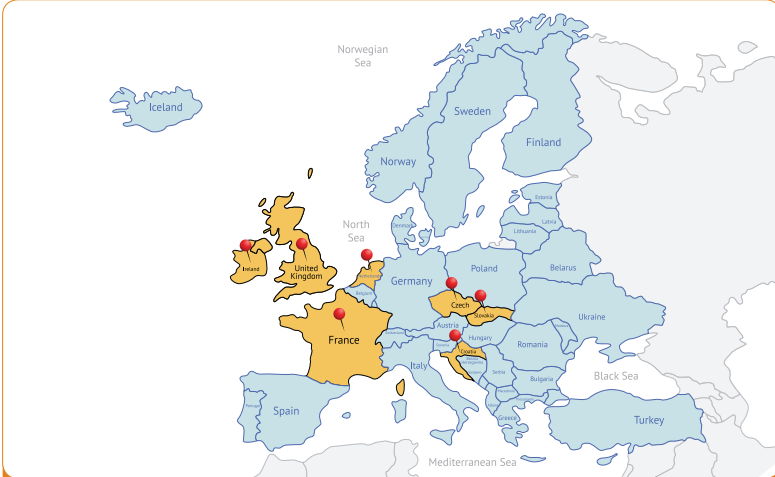


Figure A-1: eID-solutions based on username-passwords in Europe

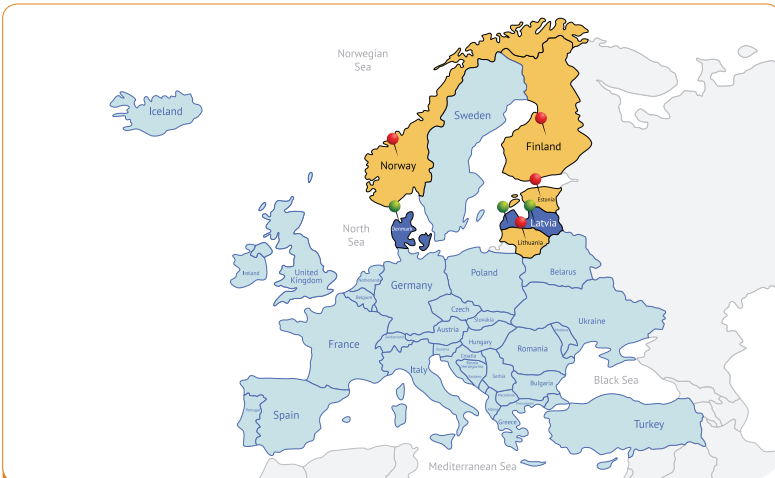


Figure A-2: eID-solutions based on OTP lists in Europe

(Note: The green pin is used to mark that the OTP is used for authentication only)

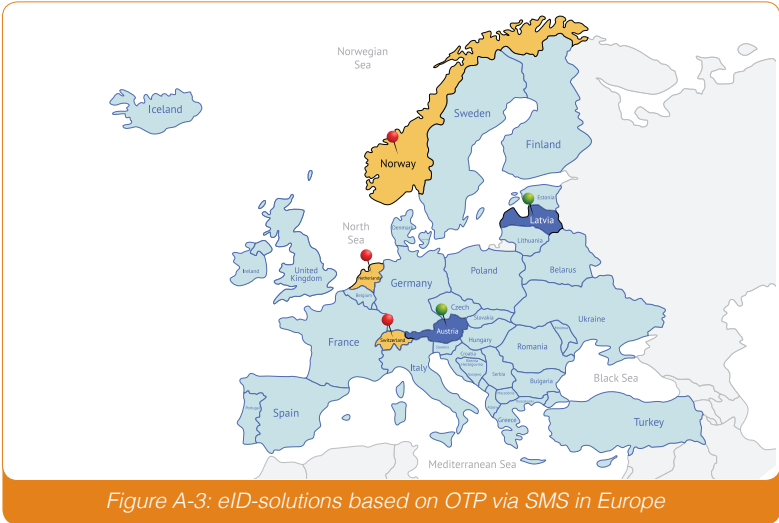


Figure A-3: eID-solutions based on OTP via SMS in Europe

(Note: The green pin is used to mark that the OTP is used for authentication only)

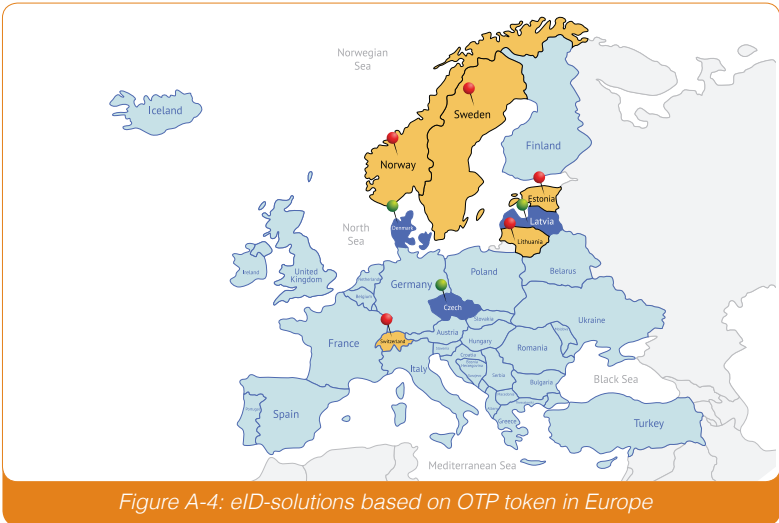


Figure A-4: eID-solutions based on OTP token in Europe

(Note: The green pin is used to mark that the OTP is used for authentication only)

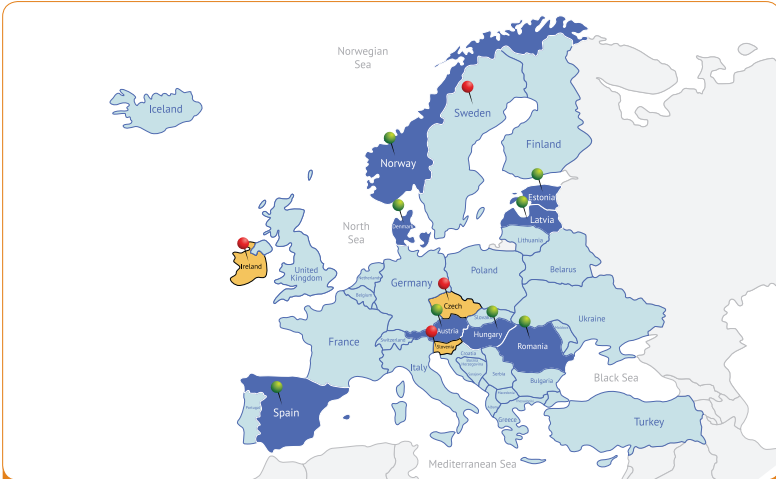


Figure A-5: eID-solutions based on soft certificates in Europe

(Note: The green pin is used to mark that the solution is used for electronic signatures only)

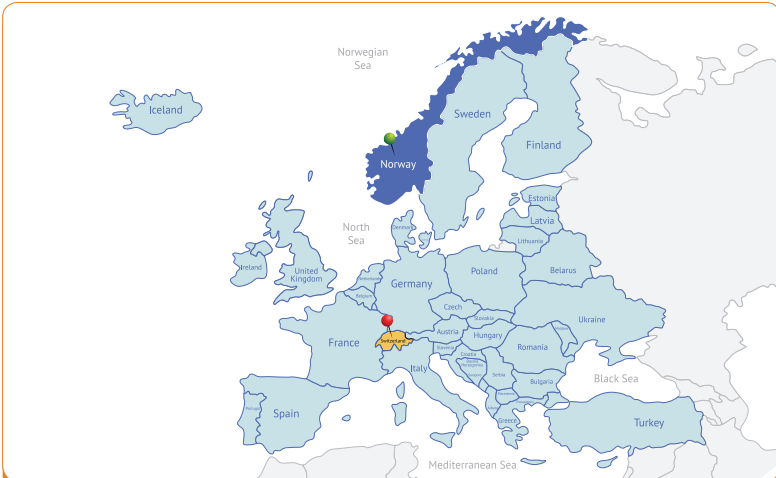


Figure A-6: eID-solutions based on PKI Token in Europe

(Note: The green pin is used to mark that the solution is used for electronic signatures only)

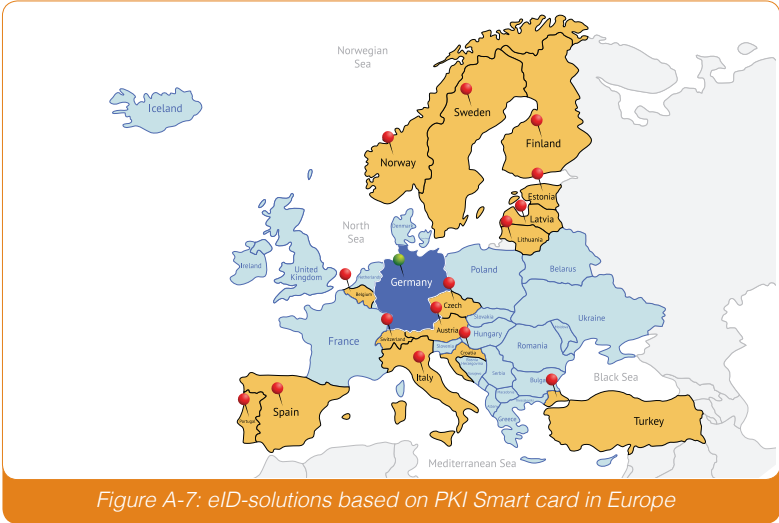


Figure A-7: eID-solutions based on PKI Smart card in Europe

(Note: Solution in Germany is Attribute Based Credentials solution; probably NFC based mobile solution)

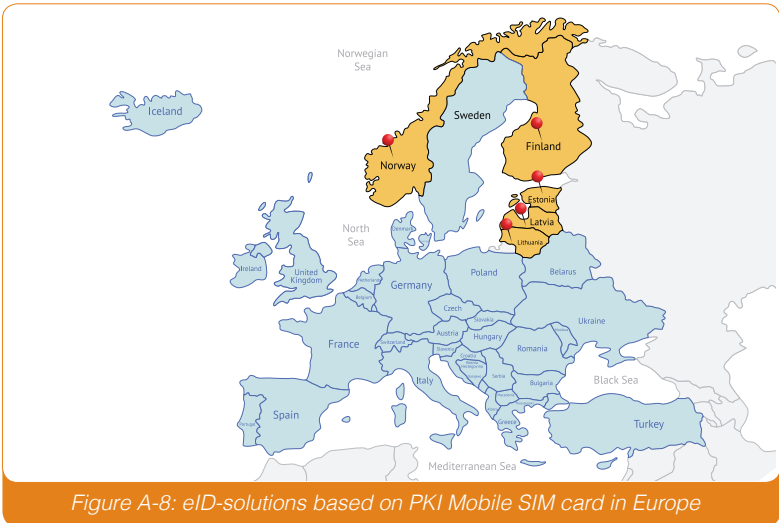


Figure A-8: eID-solutions based on PKI Mobile SIM card in Europe

Annex-2: eID by Governments in Europe (eID functionality on the national ID cards based on PKI)

First wave: Finland, Estonia, Italy, Belgium, Spain and Portugal.

Although Finland was the first European country to actually implement a PKI on national cards, these were never mandatory and Finnish citizens were better used to other authentication and digital signing mechanisms (e.g. bank OTP), which remained in use even after the introduction of the PKI FINeID card. The same applies to Italy.

A new wave: PKI cards are prepared to be launched in Central and Eastern Europe: Bulgaria, Greece, Poland, Romania, Slovakia, Slovenia and Russia. Latvia and the Czech Republic already introduced PKI smart cards in 2012. Germany uses its German eID card with attribute based credentials solution (using PKI).

eID by Public Authorities (not on the national ID card): There are also cases of specially issued cards bearing the eID functionality only, issued both by public authorities (in Sweden – TaxCard, in Italy – National Services Card, in Latvia – eSignature card) and private parties (in Switzerland – cards issued by three different parties, in Norway – the BuyPass card).

Annex-3: M-Government applications and mobile authentication – Examples OECD 2011/12

Table 1.

Country	Application
Canada	- Wireless Portal of the Government of Canada
Turkey	- E-Government Gateway
The Republic of Korea	- Mobile Portal of the Government of the Republic of Korea - Cafe of Invention - Comprehensive Tax Services - e-People: The People's Online Petition & Discussion Portal - Internet Civil Services - Single Window for Business Support Services
Spain	- Information service on government offices - National Tax Agency sends SMS - Payment gateway for services in the Basque region - Ticket payment online - Booking medical appointments - Open government - M-Signature for civil servants
Italy	MiaPA: your voice to enhance PA - Vivifacile: services for school and motoring - Trenitalia mobile - ScuolaMia – Convening substitute teachers
Singapore	- MyeCitizen SMS Alerts - TradeNet – a nation-wide Electronic Data Interchange (EDI) System
China	- Use of SMS to deliver tax information to citizens
Hungary	- SMS with exam results, scholarship decisions, etc.
Finland	- SMS Public Transport Tickets
UK	- Voting through the use of text messaging using mobile phones

Country	Application
Malta	- "M-Government Initiative" in Malta - Using mobile devices to file complaints
India	- Lokvani – "The Voice of the people" – an innovative model of Citizen Service Centers (CSCs) - SMS based services for Challan status enquiry
USA	- Electronic Benefits Transfer (EBT)
Malawi	- Dowa Emergency Cash Transfer Project (DECT)
Sweden	- Access Public Services via Mobile Digital Signatures
Austria	- Mobile phone signature "Handy Signatur"
Estonia	- M- government @ m- city - Mobile Voting
Republic of Azerbaijan	- Certificate Services Centre on E-signature and Asan Imza (Mobile ID)
Canary Islands Government	- Electronic Signatures Agenda from smartphones and tablets
Republic of Moldova	- M-Pass - m-ID



7

8

9

Identity Applications

- 7 - Privacy in the Age of Big Data:
Exploring the Role of Modern Identity Management Systems
- 8 - Identity Management in the Retail Industry: The Ladder to Move to the Next Level in the Internet Economy
- 9 - Environment Sustainability in the Age of Digital Revolution: A Review of the Field



Privacy in the Age of Big Data: Exploring the Role of Modern Identity Management Systems¹

Abstract

In today's digital world, our ability to better understand data is seen as fundamental to addressing complex economical and societal challenges. The massive amounts of digital data that governments and businesses collect as well as the technological tools they use for analyzing disparate data are referred to as big data. These advances in data collection and analysis have raised concerns about individuals' rights to privacy. In this article, we attempt to provide a short overview of big data and explore the role of modern identity management systems in providing higher levels of security and privacy in online environments. The article also makes reference to one of the most advanced identity management systems in the world, namely the United Arab Emirates' (UAE) identity management infrastructure, and how the government has designed its systems to support privacy and security in e-government and e-commerce scenarios.

Keywords: *big data, privacy, identity management.*

¹ Please quote this article as follows:

Al-Khoury, A.M. (2014) "Privacy in the Age of Big Data: Exploring the Role of Modern Identity Management Systems". *World Journal of Social Science*, Vol. 1, No. 1, pp. 37-47.

1. Introduction: The Age of Big Data

The proliferation of modern technologies and smart devices in addition to the popularity of social networking is generating unprecedented amounts of data, both in structured and unstructured forms, whether it be text, audio, video, or other forms (Mayer-Schonberger and Cukier, 2013). Data as a term and concept has become ubiquitous in today's digital landscape. In fact, data is rather becoming multi-form, multi-source, and multi-scale (Sathi, 2013).

The sheer number of bytes that is generated daily is mind-boggling! According to a recent report published by IBM, 2.5 quintillion (2.5×10^{18}) bytes of data are created every day (IBM, 2010). According to the same report, 90% of the data in the world today has been created during the past two years. Experts indicate that the world is in a digital explosion era (Liebowitz, 2013; Marz and Warren, 2013; Minelli et al., 2013; Smolan and Erwit, 2012). This phenomenon is referred to as big data.

“Big data” refers to a conglomerate of datasets whose size is beyond typical database software's ability to capture, store, manage, and analyze (Manyika et al., 2011). As depicted in Figure 1, all computer hard drives in the world equaled 160 exabytes in 2006. The total storage systems did not reach one zetabyte of information in 2012. One Zetabyte equals to 1,000,000,000,000,000,000 bytes, or 1000 exabytes. By 2020, the expected growth rate is forecasted to reach 112 zetabytes of data, representing almost 75% annual growth rate.

Big data is generated from practically everywhere; i.e., social media sites (Facebook, Twitter, Linked-in), digital pictures and videos, e-mails, purchase transaction records, cell phone, global positioning system (GPS) signals, geo-stationary satellites, and meteorological sensors, to name a few. See also Figure 2. Billions of posts in social networks, blogs, commerce sites, e-mails, text messages, and utility payments are being “piggy-backed” to result in patterns of the digital interactions and individual behavior patterns that are then constructed from there.

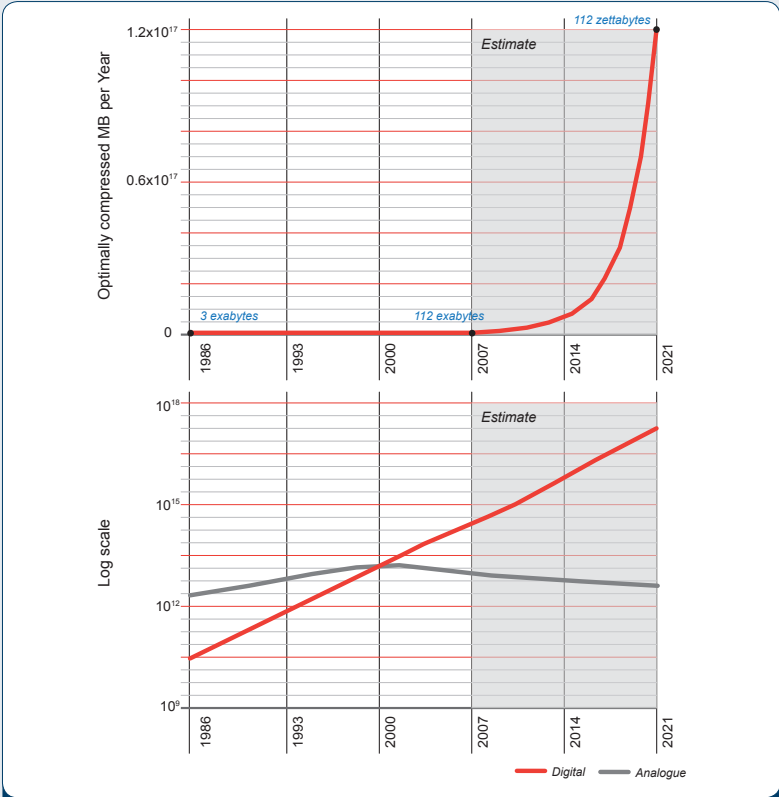


Figure 1. Global Growth of Digital Storage Capacity

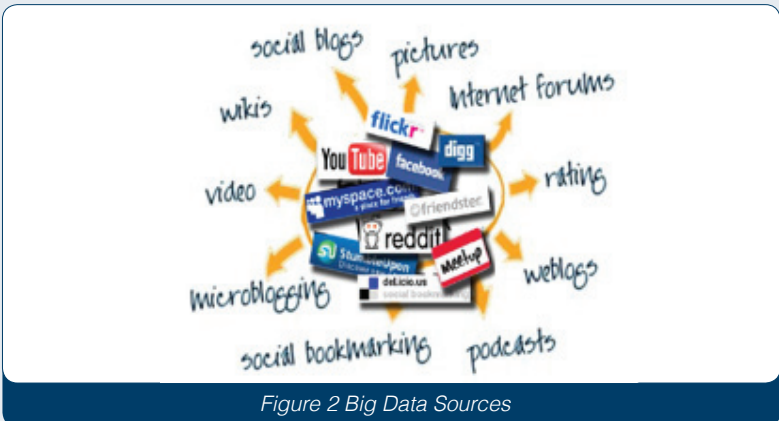


Figure 2 Big Data Sources

Data growth is being enabled by innovative software and analysis tools as well as inexpensive storage and a proliferation of sensor and data capture technology, thus increasing connections to information via the cloud and virtualized storage infrastructures (Gantz and Reinsel, 2011). A study that IDC conducted in 2011 showed that new technologies are driving down the cost of creating, capturing, managing, and storing information to one-sixth of the cost in 2005 (ibid.). See also Figure 3. The same study also indicated that consumers will create almost 68% of unstructured data in 2015.

All in all, the amount of data is continuing to grow at an exponential rate. As it grows, this collection of data is seen as creating a new layer in the economy by turning information into revenue and accelerating growth in the global economy by creating jobs (Gartner, 2012).

This article's purpose is to explain this phenomenon and to view it from an individual's privacy perspective. The article mainly attempts to shed light on modern identity management systems' role in protecting individuals' privacy rights in online environments. We use the example of the United Arab Emirates (UAE) and its identity management infrastructure in this regard.

The article is structured as follows. In section 2, we explain the characteristics that constitute big data. In section 3, we provide some thoughts regarding how identities can be constructed from online and digital behaviors. In section 4, we illustrate how government identity management systems can provide higher security and protection levels in online environments. We also demonstrate how the UAE's government has addressed the privacy and security concerns of its citizens and residents in online e-government and e-commerce transactions. The article is then concluded in section 5.

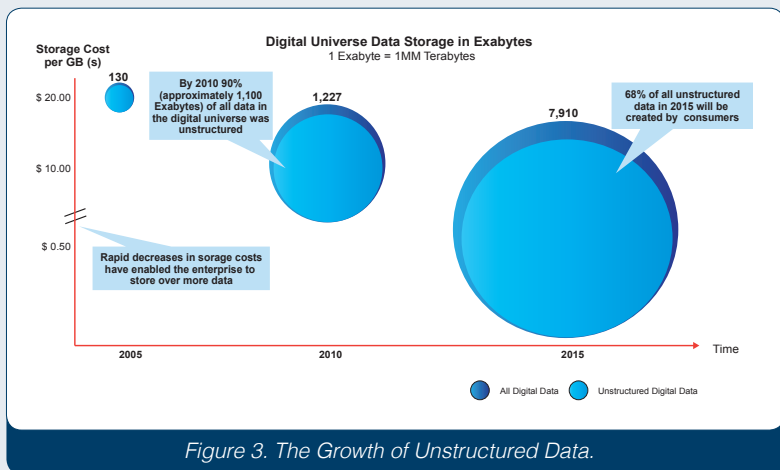


Figure 3. The Growth of Unstructured Data.

Source (IDC, 2011)

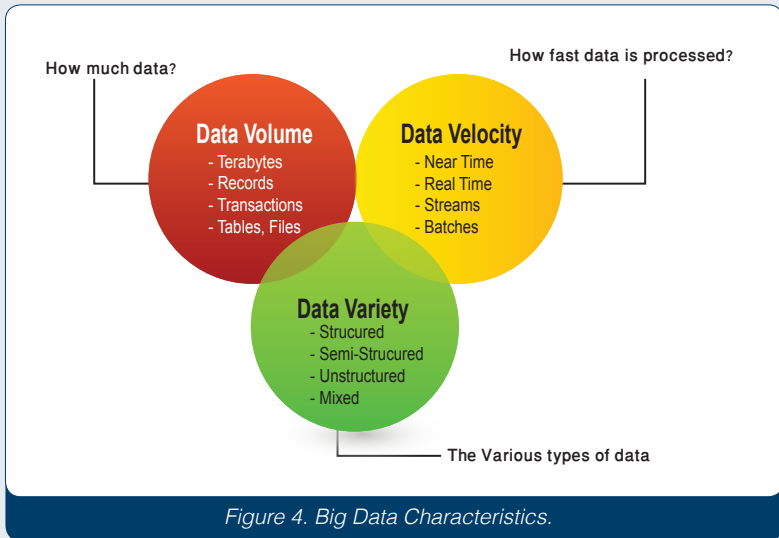
2. Big Data Characteristics

Big data has come to be characterized by the volume, velocity, and variety of data that is generated. These constitute the 3Vs of big data. See Figure 4. Volume refers to the amount of data and the form of data. Velocity refers to the rate at which the data are collected and analyzed. Meanwhile, variety provides the type of data collected.

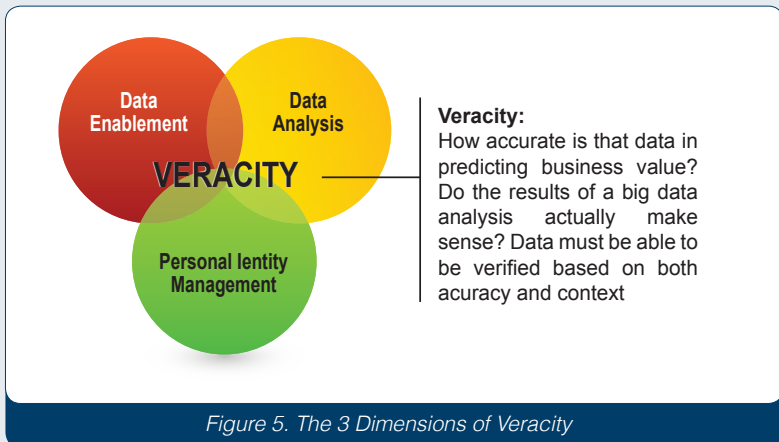
More recently, big data has been characterized by an additional fourth dimension—a fourth V—veracity, which encompasses the 3Vs. Veracity provides confidence in the truthfulness of the data. Veracity of data itself can be depicted using three dimensions. See also Figure 5. Veracity of data is established by how the data itself is enabled, which stands for the source of data. Veracity of data is established by the means and methods of analysis, thus providing discernible information. Veracity of data is then characterized by personal identity management to impact business outcomes. This is the critical dimension of big data veracity.

In principle, big data is not a new or unknown phenomenon. In fact, big data as volume data has been used in clinical trials for a long time, resulting in many groundbreaking innovations in medicines, for example. In addition, big data as volume data has been in existence in deoxyribonucleic acid (DNA) mapping and genetics, leading to many life-saving healthcare procedures. While the healthcare industry has been the initiator of big data analysis, retailers and marketing organizations have now begun to make use of big data to further their commercial activities.

Overall, the use of big data varies across sectors, where some sectors are poised for greater gains. Figure 6 depicts the results of an analysis that McKinsey conducted in 2011 and illustrates differences among sectors in the use of big data (Manyika et al., 2011). The study divided the sectors into primarily 5 clusters. These include Cluster A: computer and electronic products; Cluster B: finance, insurance and government; Cluster C: construction, educational services, and arts and entertainment; Cluster D: manufacturing and wholesale trade; and Cluster E: retail, health care providers, accommodation, and food.



Source: Russom (2011)



Cluster A sectors have already posted very strong productivity growth and are set to gain substantially from using big data since they have access to huge pools of data, and the pace of innovation is very high. Cluster B sectors, which include finance, insurance, and government, are positioned to benefit very strongly from big data as long as barriers to its use can be overcome. Because both clusters A and B are transaction- and customer-intensive sectors, the use of data and experimentation is envisaged to drastically improve overall performance. Clusters C, D, and E can derive significant value from big data, although doing so will depend on the extent to which barriers are overcome.

According to Gartner, «data-driven innovation,» will help to create 4.4 million information technology (IT) jobs globally by 2015, including 1.9 million in the United States (US) (Gartner, 2012). McKinsey's report indicates that big data has the potential to create massive saving and revenues in all sectors, i.e., create \$300 billion in potential annual value to U.S. health care (more than double the total annual health care spending in Spain); €250 billion potential annual value to Europe's public sector administration (more than the gross domestic product [GDP] of Greece); and \$600 billion in potential annual consumer surplus from using personal location data globally (Manyika et al., 2011).

All in all, big data is considered to have a huge impact on all sectors, providing endless arrays of new opportunities for transforming decision-making; discovering new insights; optimizing businesses; and, innovating their industries. However, with all of this data out there in the hands of "others," how can privacy be achieved for the individual? In fact, this could be construed as a blatant violation of individual privacy. Let us explore this further in the next section.

Some Sectors are positioned for greater gains from the use of big data

Historical productivity growth in the United States, 2000-08

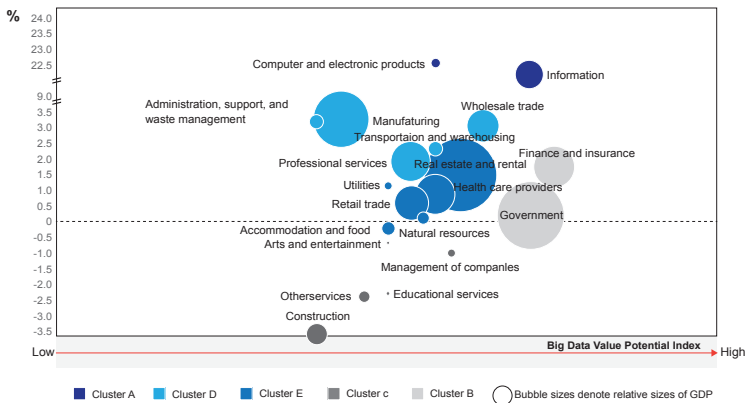


Figure 6. Big Data Value across Sectors.

Source: (Manyika et al., 2011)

3. Constructing Identity from Digital Behaviour

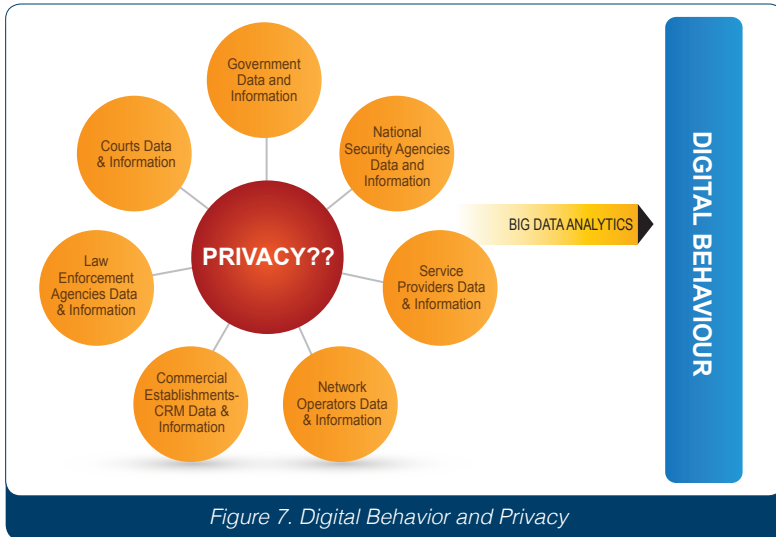
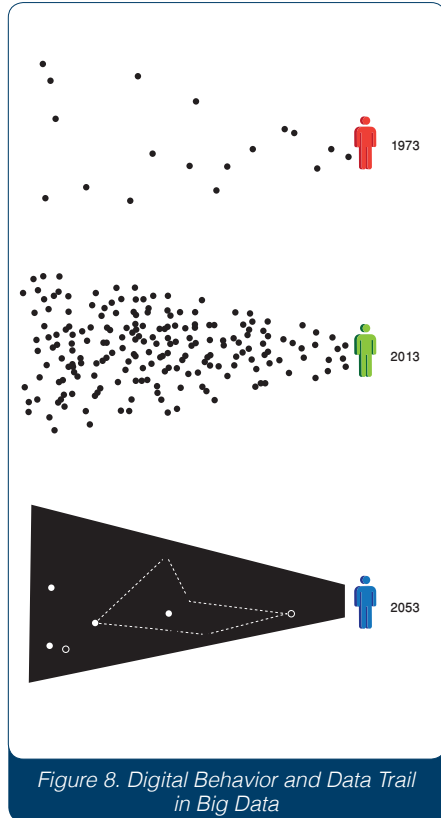


Figure 7. Digital Behavior and Privacy

Big data in information and datasets is captured based on the digital data we leave in our communications and transactions. See also Figure 7. In every interaction, we leave behind a huge trail of data that includes bits and pieces and pointers to our real behaviors. For reasons explained in earlier sections, we seek to analyze our communications using the argument that entities need to know their customers in order to predict our preferences and to enable the personalization of services and products based on our needs. This, in turn, raises many issues that govern privacy and our rights to be anonymous in the digital world.

In principle, it is understood that the collection of information from digital transactions and interactions is something that is unstoppable. Whether we like it or not, the digital trail we leave behind in the e-world is amazingly large. This digital trail when analyzed is almost like a signature that we leave behind, making it very easy for analysts to identify us as individuals in the purported anonymity of the World Wide Web (WEB).

O'Harrow (2006) indicates that although the emergence of a data-driven surveillance society has provided the conveniences of access to information and services (such as cell phones, discount cards, and electronic toll passes), it also has created new approaches to watching us more closely than ever before. He also points to the fact that as companies customarily collect billions of details about nearly every connected individual, the world will reach a state where people will lose control of their privacy and identities at any moment. Figure 8 depicts an illustrative diagram of the evolving possibilities of capturing a data trail of individuals in the digital world.



On a global perspective, the West, particularly the US and the European Union (EU), have made conscious moves to protect individuals' privacy from being abused using legal provisions. Anonymity has been the key consideration on which the legal provisions have been made so far. However, it has been proved beyond any reasonable doubt that anonymity is not guaranteed even when personal identifiers are removed from the data sets for analysis. Personal information can be revealed through searches by the user's computer, account, or Internet protocol (IP) address being linked to the search terms used (Blakeman, 2010). Thus, where does this leave an individual with respect to privacy?

Ohm (2009) says that possibilities always exist to re-identify or de-anonymize the people hidden in an anonymized database and that «data can be either useful or perfectly anonymous but never both.» In addition, Masiello and Whitten (2010) indicate that even anonymized information will always carry some risk of re-identification:

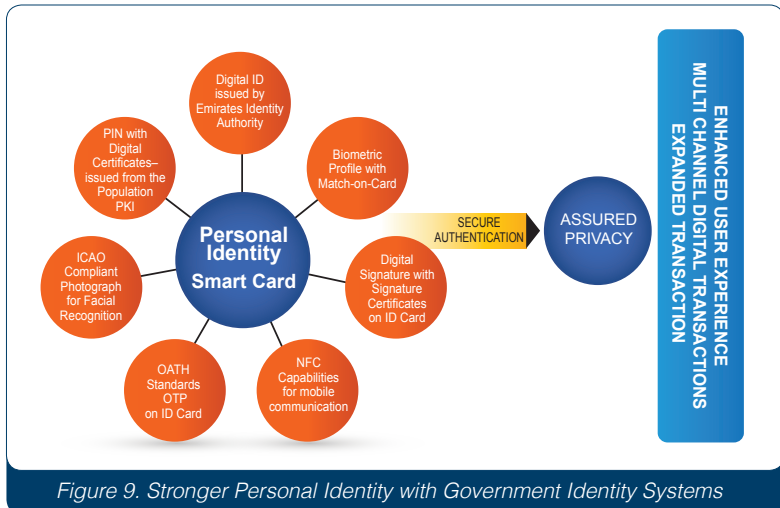
«.... many of the most pressing privacy risks... exist only if there is certainty in re-identification... that is if the information can be authenticated. As uncertainty is introduced into the re-identification equation, we cannot know that the information truly corresponds to a particular individual; it becomes more anonymous as larger amounts of uncertainty are introduced.» (p. 122)

Masiello and Whitten (2010) also indicate that a need exists for the development of not just a set of principles and policies but also a set of technical solutions that give users meaningful control. The next section attempts to present how modern identity management systems can address this need, i.e., privacy protection.

4. Government Identity and Privacy Many

governments throughout the world have launched modern identity management systems, aiming in principle to strengthen national security (Al-Khoury, 2012). Such systems attempt to establish unique identifications of individuals and to provide government-issued personal identity cards and digital identity profiles.

Digital identity profiles provide perfect PROXY for personal identities. Individuals would be known and authenticated as genuine persons by a “national identity authority” that will act as a third-party, online identity authentication service provider. In online transactions, no identity details are revealed to the service providers apart from basic identity details. Thus, service providers, in turn, can identify the potential service-seekers securely from the authentication that the identity authority provides. An individual will then be able to transact and interact freely without compromising his/her personal identity in e-government and e-commerce applications. See also Figure 9.



From a government perspective, such systems are envisaged to be extremely critical in big data and big data analytics in the sense that they provide the required privacy in anonymity yet provide meaningful data for analysis.

4.1 UAE National Identity Program

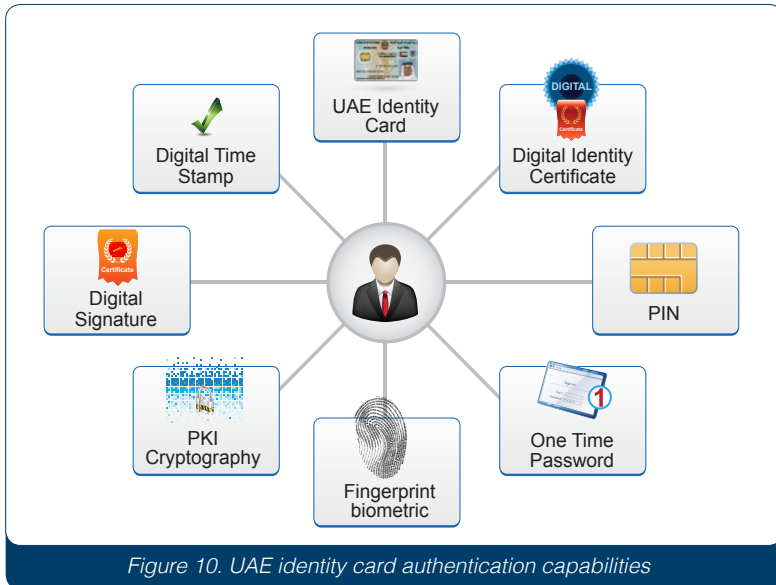


Figure 10. UAE identity card authentication capabilities

The UAE national identity management infrastructure was set up in 2005, and all citizens and residents were registered in the system by the end of 2012. All of the population has been issued smart biometric and Public Key Infrastructure (PKI)-based identity cards, with biometric enrollment being mandatory for those above the age of 15 years.

The smart cards issued are designed to provide multi factor authentication. The digital identity profile components in the card provide the ability to verify and to authenticate the identity of the individual for access.

An online validation gateway has been set up in the UAE to provide the necessary credential verification on the Web. The identity card could only

be used with the digital credentials on Web transactions. The validation gateway does not share personal information but provides credential verification. As such, service providers are accorded with verification and authentication services that enable secure remote transactions. Service-seekers remain anonymous on the Web because only digital certificates or biometrics would be used to establish credential verification. See also Figure 11.

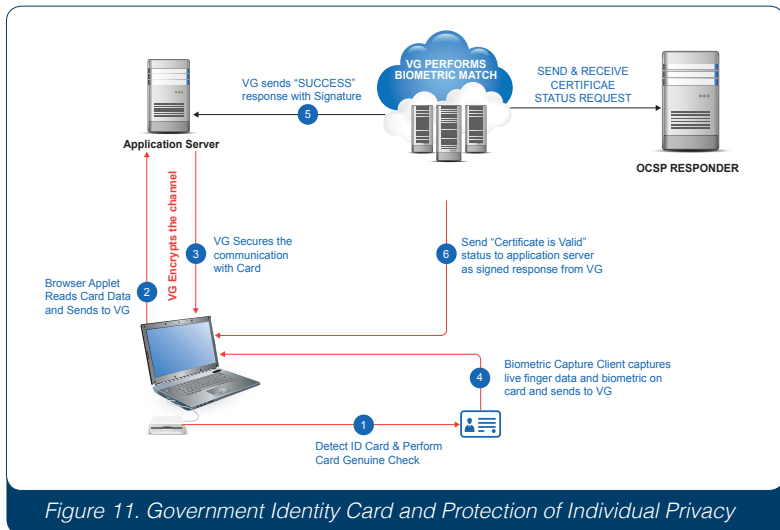


Figure 11. Government Identity Card and Protection of Individual Privacy

Anonymity to the service seeker is assured because no personal details are transmitted across the network channels. The service provider relies on the digital identity credentials provided in the national identity card. When the identity card is presented in the transaction, the service provider simply refers the credentials to the identity provider (national identity authority). The identity authority, in turn, verifies the credentials, establishes the credentials' validity, and sends back a digitally signed response that verifies the cardholder's identity.

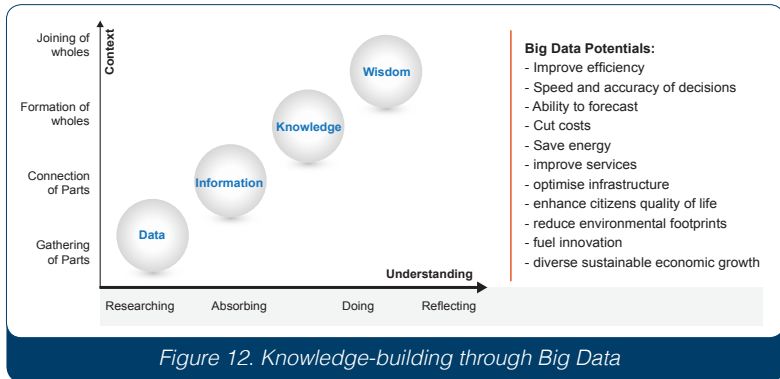
All of the interactions on identity verification are done using standard protocols of digital certificate verification. The true identity linked to these credentials is only with the service provider, the identity provider, and the ID holder.

The service provider is pleased with the fact that the presence of the correct entity is established in the transaction. The service-seeker is satisfied on the basis that none of his/her personal details are out in the open and that privacy is assured. Snoopers on the transaction collecting digital trails only get bits and bytes of data with no information on them. It is important to note that the information from the transaction remains only with the service-seeker and the service provider.

Let us consider a simple transaction on the Web where a purchase is affected. Let us assume that the seller on the Web has a policy of selling only to people above 18 years of age. Under the current conditions, the buyer online is expected to complete a form with personal details, such as name, address, gender, date of birth, etc., and sign a disclaimer that he/she is above 18. These data are worth their value in gold for snoopers. While the service provider seeks this information to protect his/her selling policies, the service-seeker is forced to provide verifiable information that the snoopers happily gather.

With the advent of the national identification card, the service seekers information is “read” off the card using secure applications, the identity is verified and signed digitally by the identity provider, the age information is verified digitally with no personal data being transferred across the networks. While big data collectors and snoopers can get valid information about a sale indicating that a person above 18 has transacted, the buyer’s identity is fully protected and is not divulged on the public channels.

5. Concluding Remarks



Despite all fears associated with it, big data should be viewed as being about building knowledge to support social, environmental, and economic development. However, complexity will remain an issue. Successfully exploiting the value in big data requires experimentation and exploration. The private sector will still lead the game, as big data will be viewed as a source of competition and growth.

The public sector will need to take big data more seriously and put in place data strategies to create new waves of productivity growth. The shortage of skills will be a primary challenge. It is reported that the US by 2018 will face a shortage of about 2 million managers and analysts who have the know-how needed to create and use big data to make effective decisions (Manyika et al., 2011).

Conversely, the notion of trust in how information is used, shared, archived, and managed is critical in this complex and highly fluid environment (Gantz and Reinsel, 2011). Governments will need to pay more attention to addressing policies that are related to privacy and security needs in today's digital world. From our perspective, we believe that data in whatever form should be treated as personally identifiable and as a result should be subjected to the regulatory framework.



In this article, we highlighted the potential role of modern government identity management systems in providing higher levels of privacy and security in online transactions. The presented case of the UAE provides a real case of a government practice in this field. Digital identity profiles provided and packaged in secure smart cards can be expected to play a pivotal role in balancing the needs of service providers and service-seekers. A secure identity would encourage users to be engaged more actively and more expansively in this digital world.

Acknowledgments

The content of this article was presented at Big Data Systems, Applications and Privacy Conference, organized by New York University, Abu Dhabi, UAE, 10 –11 March 2013.

References

I-Khoury, A.M. (2012). Biometrics Technology and the New Economy. *International Journal of Innovation in the Digital Economy*, 3(4), 1-28.

Blakeman, K. (2010). What Search Engines Know About You. *Online*, 34(5), 46-48.

Cooper, M. and Mell, P. (2012). Tackling Big Data. National Institute of Standards and Technology. US Department of Commerce. Retrieved from http://csrc.nist.gov/groups/SMA/forum/documents/june2012presentations/fcsm_june2012_cooper_mell.pdf

Craig, T. and Ludloff, M.E. (2011). *Privacy and Big Data*. Sebastopol: O'Reilly Media.

Gantz, J. and Reinsel, D. (2011). Extracting Value from Chaos. IDC. Retrieved from <http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf>

Gartner (2011). Big Data Creates Big Jobs: 4.4 Million IT Jobs Globally to Support Big Data By 2015. Retrieved from <http://www.gartner.com/newsroom/id/2207915>

Hagen, C., Khan, K., Ciobo, M., Miller, J., Walll, D. Evans, H. and Yadav, A. (2013). Big Data and the Creative Destruction of Today's Business Models, A.T. Kearney, Inc. Retrieved from <https://www.atkearney.com/documents/10192/698536/Big+Data+and+the+Creative+Destruction+of+Todays+Business+Models.pdf/f05aed38-6c26-431d-8500-d75a2c384919>

IBM. (2010). What is big data? Bringing big data to the enterprise. Retrieved from <http://www-01.ibm.com/software/data/bigdata>

Liebowitz, J. (2013). *Big Data and Business Analytics*. Verlag: Auerbach Publications.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. and Byers, A.H. (2011). Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute. Retrieved from http://www.mckinsey.com/~media/McKinsey/dotcom/Insights+and+pubs/MGI/Research/Technology+and+Innovation/Big+Data/MGI_big_data_full_report.ashx

Marz, N. and Warren, J. (2013). *Big Data: Principles and best practices of scalable realtime data systems*. NY: Manning Publications.

Masiello, B. and Whitten, A. (2010). Engineering privacy in an age of information abundance. In *Intelligent Information Privacy Management*, AAAI Spring Symposium Series, 119–124. Retrieved from <https://www.aaai.org/ocs/index.php>

SSS/SSS10/paper/view/1188/1497.

Mayer-Schonberger, V. and Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston, MA: Eamon Dolan/Houghton Mifflin Harcourt.

Minelli, M., Chambers, M. and Dhiraj, A. (2013). *Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses*. New Jersey: John Wiley & Sons.

Nair, R. and Narayanan, A. (2012). *Benefitting from Big Data Leveraging Unstructured Data Capabilities for Competitive Advantage*. Booz & Company Inc. http://www.booz.com/media/file/BoozCo_Benefitting-from-Big-Data.pdf

O'Harrow, R. Jr. (2006). *No Place to Hide*. New York: Free Press.

Ohm, P. (2010). *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*. *UCLA Law Review*, 57, 1701; Retrieved from <http://ssrn.com/abstract=1450006>

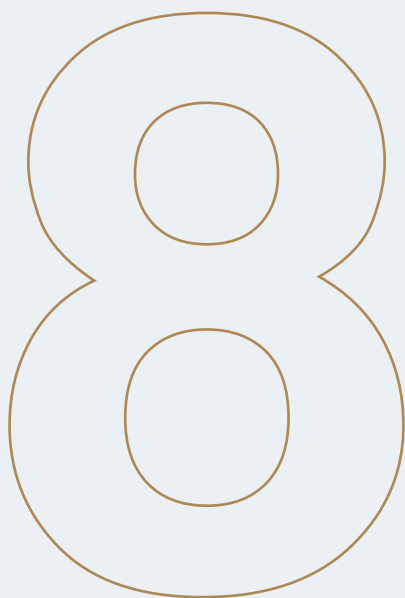
Russom, P.. (2012). *Big data analytics*. Retrieved from http://www.cloudtalk.it/wp-content/uploads/2012/03/1_17959_TDWIBigDataAnalytics.pdf

Sathi, A. (2013). *Big Data Analytics: Disruptive Technologies for Changing the Game*. USA: Mc Press.

Schroeck, M., Shockley, R., Smart, J., Romero-Morales, D. and Tufano, P. (2012). *Analytics: The real-world use of big data: How innovative enterprises extract value from uncertain data*, IBM Corporation, USA. Retrieved from http://www-03.ibm.com/systems/hu/resources/the_real_word_use_of_big_data.pdf

Smolan, R. and Erwit, J. (2012). *The Human Face of Big Data*. Sausalito, Calif.: Against All Odds Productions.

United Nations. (2012). *Big Data for Development: Challenges and Opportunities*. *Global Pulse*. Retrived from <http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf>



Identity Management in the Retail Industry: The Ladder to Move to the Next Level in the Internet Economy¹

Abstract

Over the past decade, significant changes have been affecting the retail industry, largely due to the rapid pace of technological developments. With the advent of mobility and self-service models, retailers are aggressively working to stay ahead of the technology curve and meet new customers' demands and buying preferences. As such, retailers are seeking to be ubiquitous in today's digital world. However, being ubiquitous is still not enough. To better personalize and enhance service delivery, businesses need to know the users of their products and their service preferences. They also need to have the means through which identities can be ascertained. This article provides an overview of the main challenges facing the retail industry in this regard and some of the emerging realities of the Internet age that are impacting the industry. This paper argues that the insecurity of the Internet and the risk of identity theft are major obstacles to the development and optimal use of the Internet economy. The study aims to explore the role of modern identity management in the retail industry, while shedding light on one of the world's most renowned identity management infrastructures—in the United Arab Emirates (UAE)—and examining how reliable identity management systems can push the retail industry into new frontiers.

Keywords: Retailing, digital identity, identity management, national ID, e-economy

¹ Please quote this article as follows:

Al-Khoury, A.M. (2014) "Identity Management in the Retail Industry: The Ladder to Move to the Next Level in the Internet Economy", *Journal of Finance & Investment Analysis*, Vol. 3, No. 1.

1. Introduction

Today's business world is metamorphosing! The forces shaping our world are immense, complex, surprising, and challenging (Pearson, 2010). More than ever, the prosperity of organizations, societies, and individuals depends on the extent to which they can adapt to these forces and use them to their advantage (Ibid).

Amid all this, the retail industry is in the throes of outgrowing conventional merchandising. The paradigm shift in consumer behavior from analogue to digital has not only affected the mode of sale but also the marketing modes and all other dimensions (see Figure 1). In fact, the Internet is increasingly influencing retail industry supply and demand (Levis, 2013). Mobile technology, online marketing, and advanced distribution systems are fundamentally changing the nature of retailing (Ibid).

Studies indicate that more retailers are going global to capture a larger share of the \$1.4 trillion e-commerce market (Dean et al., 2012). The competition is obviously fierce and the marketplace is becoming more global and crowded. As such, retailers are constantly trying to find customers by cutting through the layers of value perception with their products and services aided by enhanced brand presence, which feeds the higher purchasing power of targeted customers.

The impact of digitalization has been immense on everything related to a seller reaching the buyer and vice versa. The social networks have added a new dimension to the customers' online behavior. The paradox of human behavior today is such that people spend time more with their own selves while connected socially on the Internet. They spend time in the virtual presence of others but are in their own physical presence.

The mobility accorded by the smart phones and the availability of Internet across these devices has made people much more reclusive while being omni-present on social networks. Herein lies the paradox and the complexity of reaching out to the customer in terms of safely, security, and risk.

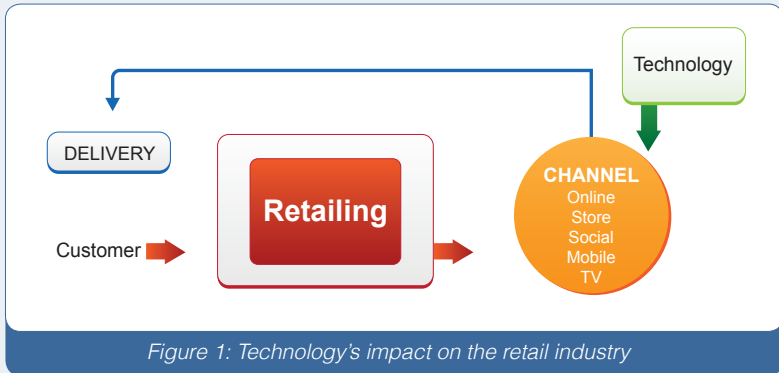


Figure 1: Technology's impact on the retail industry

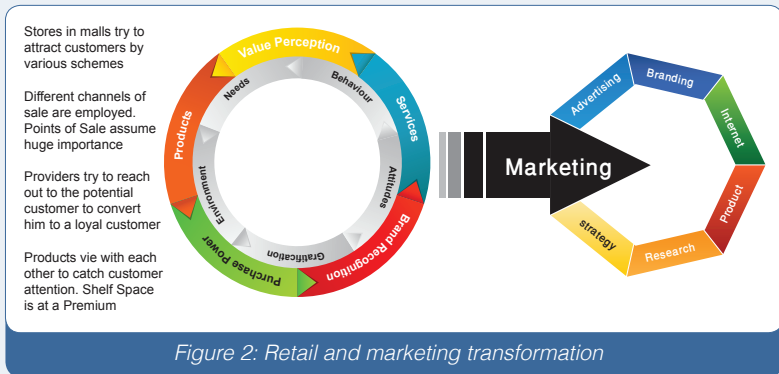


Figure 2: Retail and marketing transformation



The level of trust in existing electronic identity management practices is not high enough for users to engage in more online transactions. Besides, identity systems in use are not sufficient to combat the globally growing crime of identity theft, which is wreaking havoc on economies worldwide. So why are markets not providing appropriate responses? How should governments approach this and what should be their role?

The objective of this article is to examine the role of modern identity management infrastructures in the revitalization of the online retail landscape and drive a positive transformation. We provide an overview of one of the leading and renowned government-owned identity management infrastructures that aims to reap the benefits of the Internet economy, namely the UAE national identity management infrastructure, which plays a significant role in pushing the retail industry into new frontiers.

The article is structured as follows. In section 2, we outline some of the challenges and emerging realities of the Internet age facing the retail industry. In section 3, we present some statistics around the mounting crime of identity theft and how it is impacting the growth of the retail industry. We examine the existing electronic identity management practices and why they are not sufficient to combat identity theft in the retail industry. In section 4, we provide an overview of the UAE's national identity management infrastructure and explain how the government aims to provide individuals, businesses, and government organizations with secure and reliable management of digital identity and personal data. The article concludes in section 5.

2. Changing Face of Retailing

In today's virtually driven world, the 7.1 billion population on Earth constitutes a potential customer base. From a retail perspective, knowing who among these are the most likely to buy particular products or consume particular services is a decisive set of data. It is clear that retailers have an opportunity to capture new customers online and increase sales through a compelling omni-channel strategy (WalkerSands, 2013).

But how well do retailers know their customers in today's digital world? Global markets and innovative forms of multichannel retailing demand a fresh look at the dynamics of today's retailing environment (Kaufman-Scarborough & Forsythe, 2009). Figure 3 depicts some emerging new realities of relationship management. Retailers need to understand these emerging consumer perceptions, especially in markets that are undergoing rapid change (Ibid).

Retailers around the world are under intense pressure to deliver services for customers that are personalized and integrated rather than adopt a one-size-fits-all approach. The transactional approach that multichannel retailers have traditionally applied to loyalty programs is no longer sufficient to build longer-term customer affinity (Welch, 2013). The collision

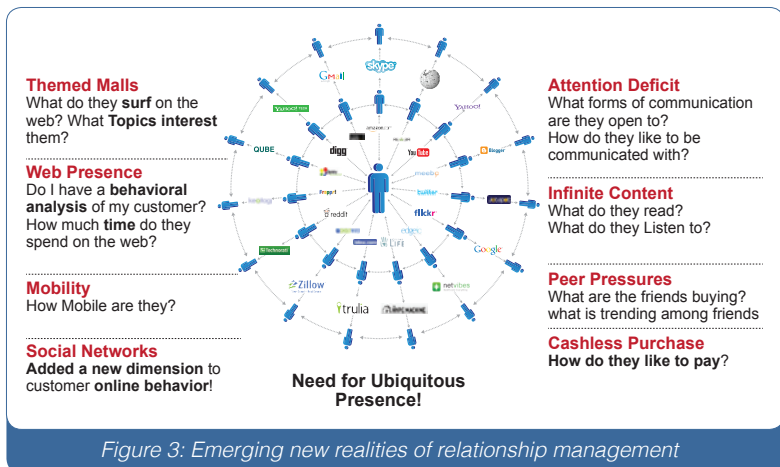


Figure 3: Emerging new realities of relationship management

of the virtual and physical worlds is fundamentally changing consumers' purchasing behaviors (Deloitte, 2013). Consumers are continuing to use the power of digital technologies to redefine the way in which they interact with retailers (Burt et al., 2013).

In essence, the realities of relationship management have changed. So one may wonder, how does this relationship get built? Collin Shaw in *The DNA of Customer Experience* argues that customers are driven by a set of emotional values. Shaw's emotional values consist of a pyramid of four clusters as depicted in Figure 4.

The lowest cluster means that if businesses evoke these emotions with their customers, then they will lose value. This lower cluster represents the feelings when people are disappointed and frustrated towards a service or a product. The next cluster, "attention cluster," is where the customers' emotions are garnered to indulge in the beginning of an interest in a product/service. The positivity moves up by an enduring relationship of trust and value, with the customer being taken care of by the retailers. Here is where the relationship building takes place and where the retailer needs to know the customer more closely and personally. This is the most crucial part of a relationship-building exercise. Once the trust is gained, the customer becomes the advocate of the seller. But the unfortunate reality is that retailers today do not know their customers well—do they really know?

According to a survey released in January 2012 by Boston Retail Partners (BRP), 31% of North American retailers remain unable to identify their customers at the point of sale (POS). The survey also found that no retailer could identify customers connecting through mobile devices. As depicted in Figure 5, the most common customer contact information available includes telephone numbers (38%), customer/identification number (34%), email address (34%), name and address (31%), and member/club number (28%). But these still do not provide the reliable identification data that retailers need, as they might be subject to change from time to time.

On the other hand, what makes this worse are the growing crimes related to identity theft, which has reached to a point where it is now threatening the growth of online retailers and the provisioning of financial and government services online as well. To shed light on the seriousness of this issue, the next section will provide some statistical elaboration.

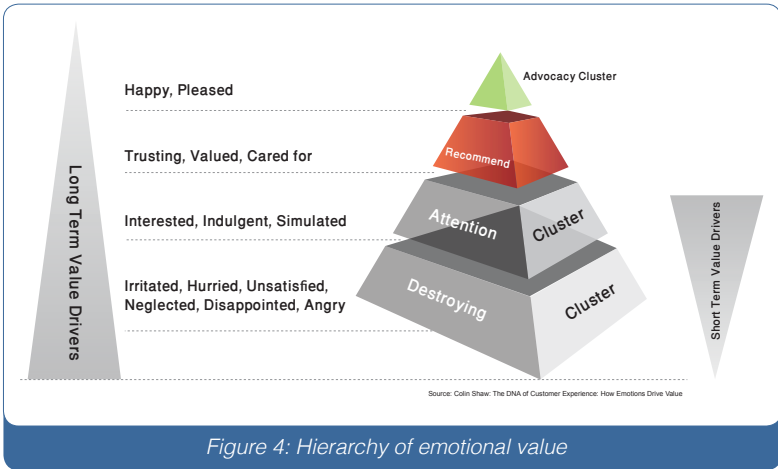


Figure 4: Hierarchy of emotional value

Source: Shaw (2007)

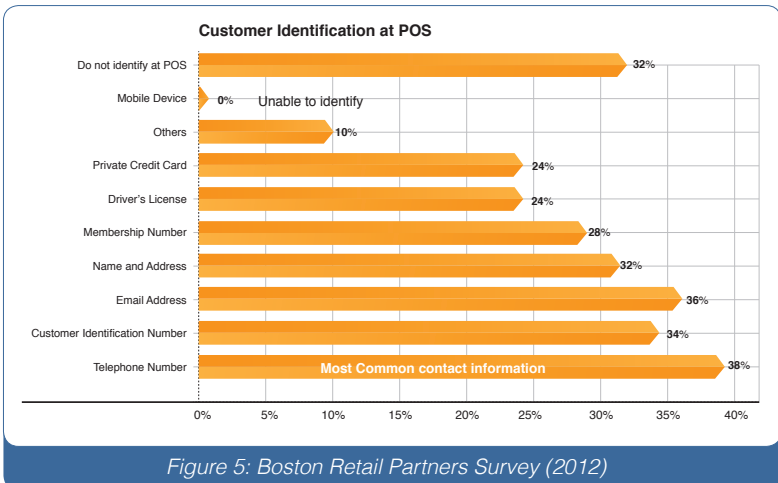


Figure 5: Boston Retail Partners Survey (2012)

3. Identity Theft

Retailers are turning to online systems to provide secure and easy-to-use transaction systems and to build deeper relationships with their now global customers. But such an online marketplace inspired newfangled risks for consumers and retailers (Lachut, 2013). For instance, online payment systems have created increasing demand for online customers to create and recreate identities with every retailer they interact with—all of whom are susceptible to different threats of identity theft (Ibid).

By definition, identity theft refers to the unauthorized use of an individual or entity's identity to conduct illicit activity (Craig et al., 2013). Identity theft has increased at an alarming rate over the past few years (Cantor, 2013). Personal information lost in data breaches are frequently used to commit fraud (ITAC, 2013). While credit card numbers remain the most popular item revealed in a data breach, in reality, other information can be more useful to fraudsters (Ibid).

Data breaches represent a multifaceted threat. According to a study conducted by the Urban Institute's Justice Policy Center, identity theft and fraud will continue to be the fastest-growing crimes in the next five to 10 years; however, the nature of identity theft is likely to shift to more organized, high-stakes, global attacks (La Vigne et al., 2008). The study also indicates that organized retail crime will continue to grow and become one of the most costly crimes experienced by the security industry (Ibid).

As per the Javelin Strategy report, identity fraud incidents in 2012 increased by more than one million victims and fraudsters stole more than \$21 billion—the highest amount since 2009 (Javelin Strategy and Research, 2013). See Figure 6.

In another study published recently by LexisNexis (2013), data breaches continued to play a significant role in identity fraud, resulting in greater liability for merchants as the percentages of incidents increased from 12% in 2012 to 17% in 2013. In general, online-channel frauds increased

by 36%, costing merchants \$3.10 for each dollar of fraud losses. Not surprisingly, mobile merchants have incurred the greatest fraud losses as a percent of revenue among all merchant segments (0.75% in 2013). This is the only segment not to have benefitted from a decrease in fraud as a percent of revenue from 2012 to 2013. Mobile merchants are seeing an increase in revenue through this channel from 14% in 2012 to 19% in 2013. As depicted in Figure 7, Javelin report suggests that among all online users tablet owners have been the most susceptible to fraud; 80% more likely than all other consumers to become fraud victims.

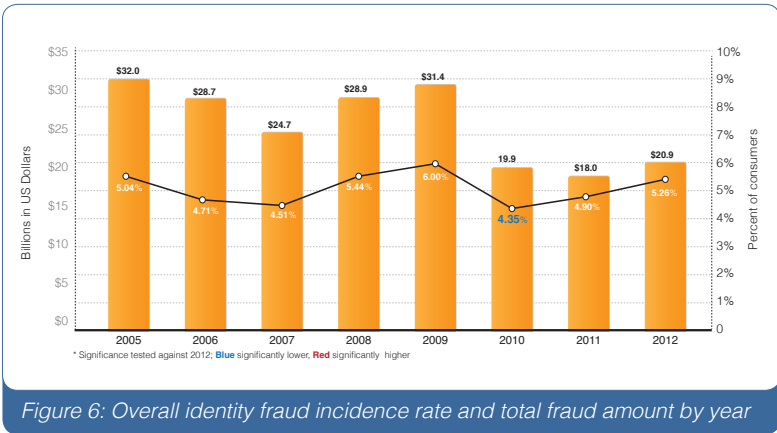


Figure 6: Overall identity fraud incidence rate and total fraud amount by year

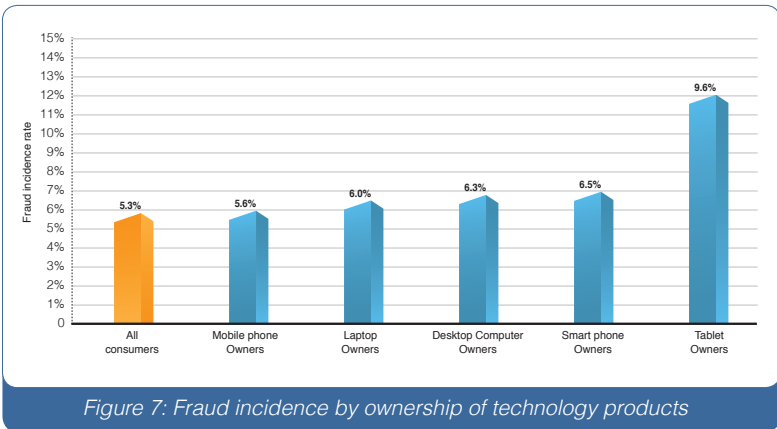


Figure 7: Fraud incidence by ownership of technology products

Source: (LexisNexis, 2013)

Beyond a doubt, new technologies have been developed to contain identity-related frauds. Chip-and-pin (C&P) smart cards have been introduced in the banking industry to enable more secure payment systems for credit, debit, and ATM cards. But, it was found that the C&P and other remote payment fraud is on the rise in 2013, with the proportion of fraudulent transactions initiated online increasing by 36%, and those initiated by mail or telephone doubling in the same time period.

The opportunity and anonymity that are touted as the secure features make the C&P and other types of remote payment fraud appealing to fraudsters. Many means exist today to glean and misuse user payment information and account credentials. However, the fact that fraudsters are exploiting the online channel does not mean that they are abandoning the physical channel just yet. Merchants with a physical presence saw an increase in the proportion of fraud through the physical channel as well (figure 8).

Lost and stolen merchandise is declining as a percentage of fraud losses. Therefore, identity theft (involving fraudulent card, check, or mobile payments), and, to a lesser extent, fraudulent requests for return and refund, are likely driving the increase in the proportion of physical channel fraudulent transactions in all fraud. Proper authentication at the POS will help merchants avoid the charge-backs and fees to financial institutions that may result from identity fraud. Improving company policies designed to limit fraudulent returns and refunds may be a difficult balancing act for customer-service-focused merchants, but they may help to curtail the not-inconsequential 18% of fraud losses resulting from this type of fraud.

Going further on these reports, the merchant community is in general agreement with the existence of fraud owing to identity theft. The majority seems to have accepted this as a risk that is inevitable, but current risk mitigation mechanisms seem to do little to thwart these fraudulent activities (figure 9).

The message to note here is that, while the community accepts risks due to identity frauds as inevitable and might even consider them for defining their risk appetite, the loss of opportunity due to perceived threats is huge. Customers who find that there are little or no efforts in thwarting identity theft from the retailers are less likely to do business with them. The largest sector of the retail, the small and medium establishments, thus stand to lose and lose heavily.

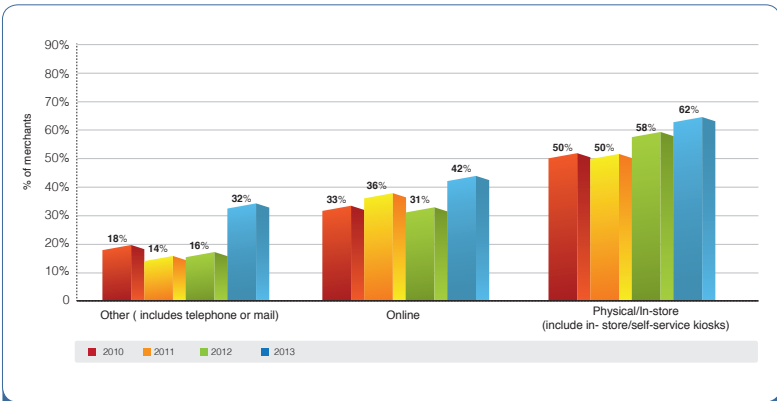


Figure 8: Percentage of fraudulent transactions attributable to channels among merchants

Source: LexisNexis (2013)

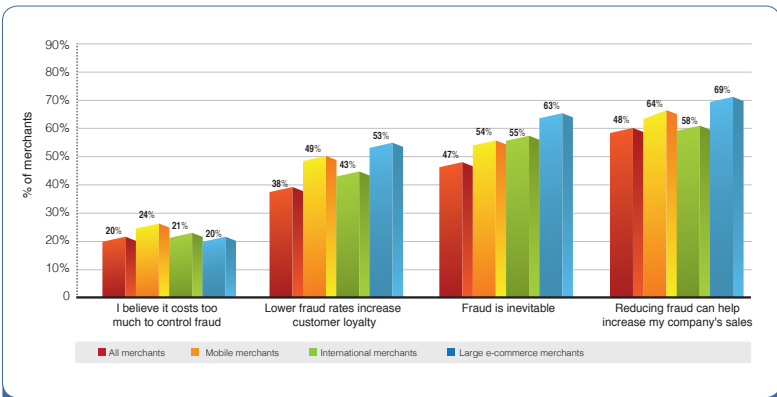


Figure 9: Merchants' attitude towards e-commerce fraud

Source: LexisNexis (2013)

As depicted in Figure 10, the biggest challenge to address is in the verification of customers' identities. Thirty-nine percent of merchants consider verifying customers' identity to be the most challenging aspect of selling to consumers at the point of sale and remotely.

The issue requires a more comprehensive approach to protecting personal information (Al-Khouri, 2013; 2012). The ad hoc way in which online identities are managed today cannot withstand the increasing assaults from expert criminal attackers (Microsoft, 2012). A new approach to securely managing online identity is essential—namely, a system that uses an interoperable, vendor-neutral framework and gives end users more direct control over their digital identity (Ibid).

To unlock the full value potential, the retail industry needs to embrace a new paradigm for digital identity applications. According to a report by the Boston Consulting Group, the value created through digital identities could reach 1 trillion euros in Europe by 2020 (Liberty Global, 2012). Two-thirds of digital identity's total value potential stands to be lost if stakeholders fail to establish a trusted flow of personal data (Ibid).

Faced with such business opportunities, governments around the world have initiated national identity management infrastructure development programs to leverage strong identity credentials in electronic environments for both public and private sectors use. The next section provides an overview of one of the most renowned and ambitious initiatives in the world that aims to provide individuals, businesses, and government organizations with secure and reliable management of digital identity and personal data.

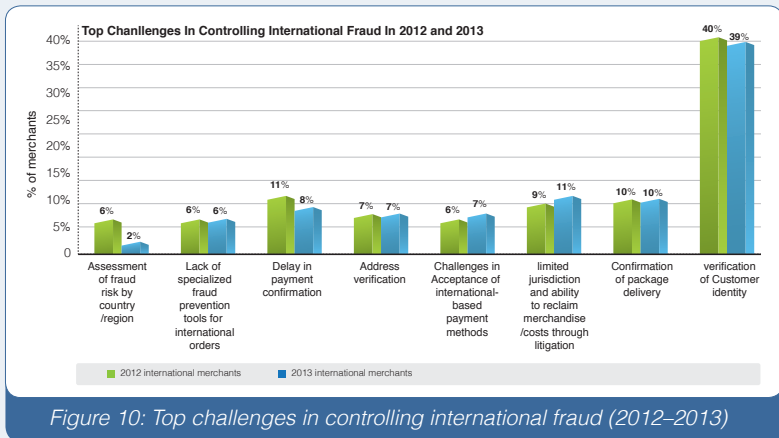


Figure 10: Top challenges in controlling international fraud (2012–2013)

Source: LexisNexis (2013)

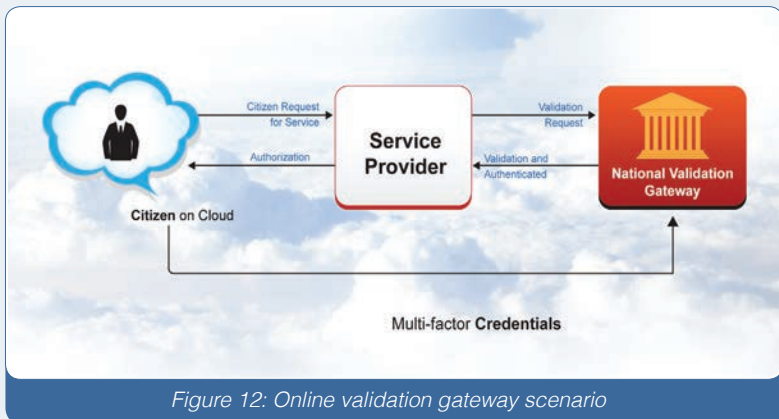
4. Government-Owned Digital Identity Management to Support e-Economy Development

The government of the UAE initiated a national identity management infrastructure development program in 2003. All citizens and legal residents were enrolled in 2012. The enrollment process consisted of capturing the biometrics of all those above the ages of 15, mainly fingerprints and facial recognition supplemented now by iris recognition, and issuing them in a digital format as the national identification in the form of a unique permanent number and smart card.

The national identity management infrastructure in the UAE is based on a key public infrastructure, which is a cryptographic technique that enables users to securely communicate on an insecure public network and reliably verify the identity of a user via digital signatures (Carlisle & Steve, 2003).

As depicted in Figure 11, the UAE smart card provides advanced user authentication capabilities more securely than standard usernames and passwords in addition to electronic signature capabilities to sign documents to ensure non-repudiation. The card also enables establishing a person's identity on-site or remotely, allowing secure and trusted transactions. The multi-factor authentication provides match-on-card and match-off-card features facilitates validation, verification, and authentication of an identity. The card holder then gets all of the identity-based services.

The UAE has recently set up an online national validation gateway to provide online card holder authentication, verification, and validation services to public and private sector organizations. The UAE national validation gateway's strong authentication services offer the widest array of authentication choices to meet the needs of public and private organizations. In principle, the use of the national gateway provides more secure, online, real-time validation, verification, and authentication of identity credentials (i.e., card, transaction, and holder genuineness; figure 11).



The national validation gateway ensures that not only are identification processes made seamless to enhance service delivery but they also vastly improve business processes, leading to strong bottom lines (figure 13). Prevention of identity theft leads to direct prevention of losses and contributes to growth in over-the-counter sales and online. Increased online sales directly implies a lower cost of sales and higher margins.

A recent study conducted by Ernst & Young for the UAE government reported that across different sectors in UAE, while the customer is “registered,” the business still asks for identification to be provided, but during the transactions a sizeable number of companies do not identify their customers securely. More importantly, for any identification need, the customer has to visit the service provider’s premises (figure 14). Moreover, this process is completely lacking in the retail industry. The study suggests that remote transactions are not secure enough due to lack of proper identity verification in the retail industry in the UAE.

The study also suggested that potential benefits to the UAE economy could exceed a trillion dollars in local currency (\$271 billion) in terms of productivity enhancement, direct consumer benefits, reduction in space utilization, paper reduction (contributing to a green environment), and cost savings from diverse other aspects (figure 15).

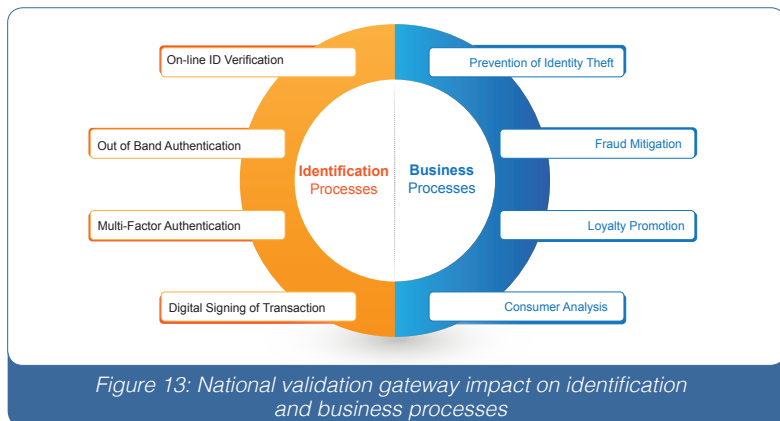


Figure 13: National validation gateway impact on identification and business processes

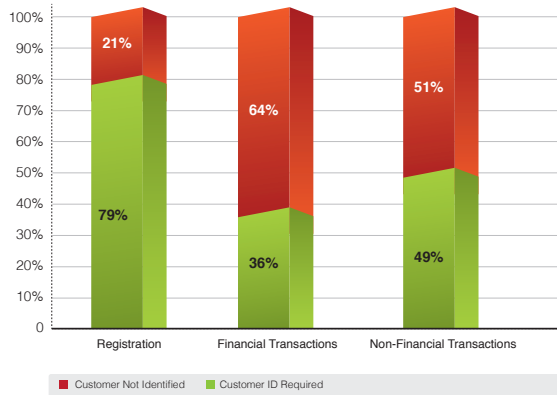


Figure 14: Survey results of ID verification in UAE

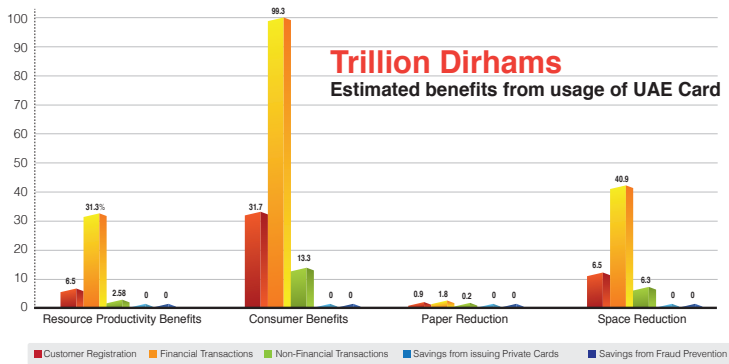


Figure 15: Identity management infrastructure potential benefits to UAE economy

The UAE identity management infrastructure offers significant opportunities for retailers. It provides the needed support to guide the public sector and businesses for setting efficient framework conditions for innovation across the public and private sectors while enhancing security, privacy, and trust in the Internet economy. The UAE government is also working on extending and leveraging its existing national identity management infrastructure to support the authentication of smart phone and mobile device users as well (Al-Khouri, 2014). Retailers will have the same credentials available for verification in such mobile environments and significant opportunities that may exceed current potential value reported above.

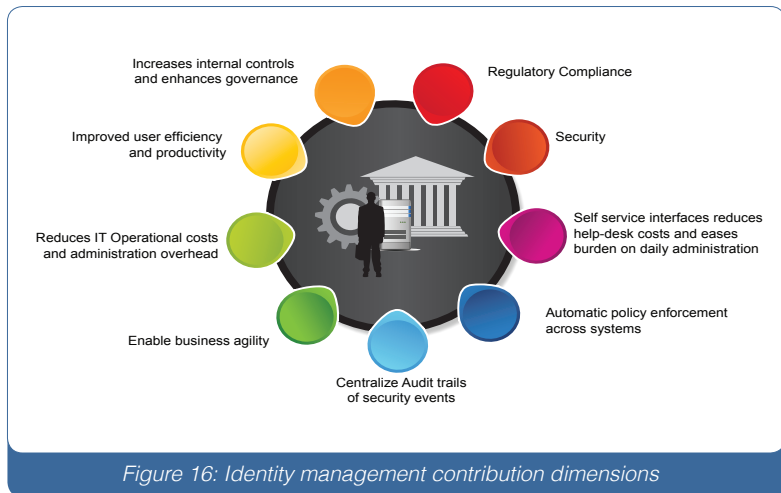
5. Concluding Remarks

Solid identity management and strong credentialing practices enable the verification of identities that are critical for the retail industry. In fact, identity management is the main vehicle for building sustainable economies. As a key instrument for establishing the identity, the UAE national identity card system provides a strong framework for increasing the governance and providing internal controls. The card and the identity management comply with all international standards and regulations and provide a secure verifiable identity for individuals. The outcome is the ability to have self-service interfaces that enable a reduction in costs for the services using automation for policy enforcement. This ability, backed by a centralized audit trail, provides a strong backbone for businesses to be carried out innovatively. This not only reduces IT operational costs but also provides the much-touted user efficiency and productivity (figure 16).

Adopting solutions designed to capitalize on national identity management infrastructure allows businesses to navigate the shifting retail landscape and drive positive transformation, including critical objectives such as the delivering a smarter shopping experience and building smarter merchandising and supply networks. These advanced technologies provided by government have staggering capabilities to revitalize the retail industry. The applications built on the use of digital identity can drive massive value growth for both public and private sector organizations

(Liberty Global, 2012). For retailers and online businesses, such an infrastructure has value potential to improve process automation, user enablement, personalization, enhanced delivery, personal data-driven R&D, and secondary monetization (Ibid). Government-owned identity management infrastructures are essential building blocks for the Internet to operate as a platform for economic development and social progress.

Different countries have taken different approaches. The approach followed by the government of the UAE is based on its leadership vision that governments' involvement is needed to succeed in the digital economy. This is to ensure ready and affordable access, a level playing field, and an open competitive environment that enables everyone to tap the economic benefit of the Internet (BSG, 2013). Governments need to intervene if they want to be winners. They should aim to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce (Ibid).



References

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.

Al-Khouri, A.M. (2012a) «PKI in Government Digital Identity Management Systems», Surviving in the Digital eID World, European Journal of ePractice, No. 4, pp. 4-21.

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

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

Baird, N. and Raj, W. (2012) Customer-Centricity Drives Successful Omni-Channel Retailing: Insights from a webinar presented by Retail Systems Research (RSR) and SAS. SAS Institute Inc. <http://www.storeconference.ca/sites/default/files/docs/ecobag/SAS.pdf>

Banday, M.T., Qadri, J.A. (2007). "Phishing - A Growing Threat to E-Commerce," The Business Review, ISSN: 0972-8384, 12(2), pp. 76-83.

Brust, A. (2013) Five Big Data Trends Revolutionizing Retail. <http://www.zdnet.com/five-big-data-trends-revolutionizing-retail-7000019510/>

Burt, M., Davison, J., Hetu, R. and Welch, K. (2013) Predicts 2014: Digitalization in Retail Means M-Commerce Grows, E-Commerce Slows, Personalization Misfires and 3D Printing Transforms. Gartner. <https://www.gartner.com/doc/2625216>

Cantor, R. (2013) Identity Theft. Destiny Image.

Carlisle, A. & Steve, L. (2003) Understanding PKI: concepts, standards, and deployment considerations. Addison-Wesley Professional. pp. 11–15.

Costa, L. and Fernandes, F. () Successful Retail Innovation in Emerging Markets: Latin American Companies Translate Smart Ideas Into Profitable Businesses. Booz & Company. <http://www.booz.com/media/file/SuccessfulRetailInnovationinEmergingMarkets.pdf>

Craig, J., Kerben, J., King, J.D., Lanoue, E.T., Lissy, K., Sailer, C., Schwomeyer, K., Thomas, J. and Yellen, B. (2013) The Current and Future Landscape of Identity Theft. <http://blog.thomsonreuters.com/wp-content/uploads/2013/11/IDT-WhitePaper-final-20131030-2.pdf>

Davenport, T.H. and Dyché, J. (2013) Big Data in Big Companies. SAS Institute Inc. http://www.sas.com/content/dam/SAS/it_it/doc/whitepaper2/big-data-big-companies-2282455.pdf

Dean, D., Digrande, S., Field, D., Lundmark, A., O'Day, J., Pineda, J. and Zwillenberg, P. (2012) The Connected World: The \$4.2 Trillion Opportunity - The Internet Economy in the G-20. The Boston Consulting Group. https://publicaffairs.linx.net/news/wp-content/uploads/2012/03/bcg_4trillion_opportunity.pdf

Deloitte (2013) Global Powers of Retailing 2013 Retail Beyond. Deloitte. http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Industries/Consumer%20business/Deloitte_Global_Powers_of_Retail_2013.pdf

Graham M. (2012). «Big data and the end of theory?». The Guardian. <http://www.theguardian.com/news/datablog/2012/mar/09/big-data-theory>

Gupta, Yuvika, When BI Meets CRM: An Emerging Concept in Retail Industry (July 16, 2013). Publishing India Group, Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2294468>

ITAC (2013) Research and Statistics. Identity Theft Assistance Center. <http://www.identitytheftassistance.org/pageview.php?cateid=47>

Javelin Strategy and Research (2013) How Consumers can Protect against Identity Fraudsters in 2013. https://www.javelinstrategy.com/uploads/web_brochure/1303_R_2013IdentityFraudConsumerReport.pdf

Kaufman-Scarborough, C. and Forsythe, S. (2009) Current issues in retailing: Relationships and emerging opportunities Introduction to the special issue from the American Collegiate Retailing Association 2005 and 2006 conferences. Journal of Business Research. 62 (2009) 517–520

La Vigne, N.G., Hetrick, S.S. and Palmer, T. (2008) The Urban Institute. http://www.urban.org/UploadedPDF/411758_crime_trends.pdf

Lachut, S. (2013) The Future of Retail 2014. A PSFK Report. PSFK LABS. <http://www.psfk.com/publishing/future-of-retail-2014>

LaValle, S., Lesser, E., Shockley, R., Hopkins, M.S. and Kruschwitz, N. (2011) Big Data, Analytics and the Path from Insights to Value. MIT Sloan Management Review. Vol. 52, No. 2. Pp. 21-31. http://www.ibm.com/smarterplanet/global/files/in_idea_smarter_computing_to_big-data-analytics_and_path_from_insights-to-value.pdf

Levis, R. (2013) The Impact of the Internet on Retail Property. Aviva Investors. http://www.avivainvestors.co.uk/pension_schemes/internet/groups/internet/documents/salessupportmaterial/pdf_029761.pdf

LexisNexis (2013) True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud. <http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf>

Liberty Global (2012) THE VALUE OF OUR DIGITAL IDENTITY. Boston Consulting Group. <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>

Liberty Global (2012) THE VALUE OF OUR DIGITAL IDENTITY. Boston Consulting Group. <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>

Microsoft (2012) Online Identity Theft: Changing the Game – Protecting Personal Information on the Internet. Microsoft Corp. USA. <http://www.telecomasia.net/content/online-identity-theft-changing-game>

Miriam Lips, M. (2010) Rethinking citizen - government relationships in the age of digital identity: Insights from research. Journal of Information Polity. Volume 15 Issue 4, December 2010. Pages 273-289

OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. <http://dx.doi.org/10.1787/5kgdzvn5rfs2-en>

Ohm, P. (2012) «Don't Build a Database of Ruin». Harvard Business Review. <http://blogs.hbr.org/2012/08/dont-build-a-database-of-ruin/>

Pearson, I. (2010) Business redefined. Ernst & Young. [http://www.ey.com/Publication/vwLUAssets/BusinessRedefined-FINAL/\\$FILE/BusinessRedefined-FINAL.pdf](http://www.ey.com/Publication/vwLUAssets/BusinessRedefined-FINAL/$FILE/BusinessRedefined-FINAL.pdf)

Shah, S., Horne, A. and Capellá, J. (2012) Good Data Won't Guarantee Good Decisions. Harvard Business Review». <http://hbr.org/2012/04/good-data-wont-guarantee-good-decisions/ar/1>

Shaw, C. (2007) The DNA of Customer Experience: How Emotions Drive Value.

Smith, R.G. (2013) Does economic crime really matter in the world of today? Public and business perceptions in Australia. Cambridge Symposium on Economic Crime. http://www.aic.gov.au/media_library/conferences/other/smith_russell/2013-09-cambridge.pdf

Snijders, C., Matzat, U., & Reips, U.-D. (2012). 'Big Data': Big gaps of knowledge in the field of Internet. International Journal of Internet Science, 7, 1-5. http://www.ijis.net/ijis7_1/ijis7_1_editorial.html

WalkerSands (2013) Reinventing Retail: What Businesses Need to Know for 2014.
<http://www.walkersands.com/pdf/Walker-Sands-Future-of-Retail-Whitepaper.pdf>

Welch, K. (2013) Excellent Execution of Customer Basics Is Key to Building Loyalty.
Gartner. <https://www.gartner.com/doc/2631834>

9

Environment Sustainability in the Age of Digital Revolution: A Review of the Field¹

Abstract

The world today has been witnessing phenomenal outgrowth in all fields during the past few decades. This augmentation has been largely stimulated by information and communication technologies (ICT). However, the inexorable evolution of technology and global economic development are being pursued at an ever-increasing societal cost with a snowballing potentially negative impact on the environment. Hence, one of the important challenges modern society faces is sustainability. This article attempts to explore the existing body of knowledge to provide a better understanding of the impact of ICT and digital revolutions on global carbon footprint and emissions. It also attempts to explore the presence of environmental sustainability initiatives in e-government programs worldwide. It presents some thoughts about how governments may address sustainability requirements in their e-government programs and enact responsible ICT-enabled transformation

Keywords: *environment; sustainability; e-government; low-carbon environment.*

¹ Please quote this article as follows:

Al-Khoury, A.M. (2013) "Environment Sustainability in the Age of Digital Revolution: A Review of the Field". *American Journal of Humanities and Social Sciences*, Vol. 1, No. 4, pp. 202-211.

1. Introduction: Sustainability and the Need to Find a Balance

With the deterioration of the planet's ecosystems along with climate change and global warming becoming the "hot" topics of the 21st century, information and communication technologies (ICT) are envisaged to play a significant role in reducing the global carbon footprint and emissions while maintaining economic growth and improving people's quality of life worldwide. Accordingly, sustainability is rapidly becoming a leading priority for organizations worldwide to improve energy efficiency and to reduce consumption.

Sustainability in simple terms refers to the capacity to endure. It is about the «development that meets the needs of the present without compromising the ability of future generations to meet their own needs» (Brundtland, 1987). In short, the term "sustainability" mandates respecting environmental limits while fulfilling social wants and needs. It stands on the reconciliation of the three primary pillars of environmental (protecting and restoring ecological systems), social equity (enhancing the well-being of all people), and economic demands (improving economic efficiency), also referred to as the three pillars of sustainability (United Nations [UN], 2005).

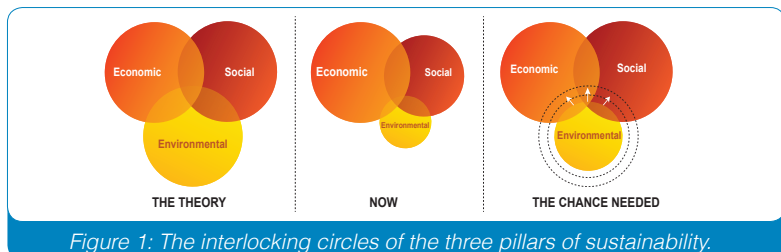
The international Union of Conservation of Nature (IUCN) illustrated the relationships among these three components of sustainability using overlapping circles, as depicted in Figure 1 (IUCN, 2012). See also Barton (2000), du Plessis (2000), Hardi and Zdan (1997), ICLEI (1996). The IUCN model attempts to demonstrate the theoretical, current, and needed auctioning change to redress the balance among the three dimensions of sustainability.

New studies suggest the need to develop policy frameworks that leverage ICT to achieve sustained growth and long-term societal benefits (Arnaud, 2012; Souter et al., 2013). Other studies suggest massive social, political, technological, cultural, and behavioral change to support such a transition, with environmental sustainability being a key focus area (Mansell, 2012; Vickery, 2012).

In most debates and examinations of sustainable development, either the environment or the economy is given priority (Giddings et al., 2002). Such a view of separation among sectors typically produces a technical fix approach (e.g., lowering resource use through taxation, etc.), but it is likely to distract governments or institutions from tackling the deeper issues or from seeing the connections among society, economy, and the environment.

Although many countries have initiated policies on global² and local levels to address sustainability needs, those policies are being challenged. The challenges are often about balancing the need to grow economies while at the same time ensuring that resources are not depleted for future generations (Info-communications Development Authority of Singapore [iDA], 2012).

This article's purpose is to contribute to a better understanding of the impact of ICT on global carbon footprint and emissions. It attempts to offer some thoughts regarding how governments may address sustainability requirements in their e-government programs and enact responsible ICT-enabled transformation. It also attempts to explore the presence of environmental sustainability initiatives in e-government programs worldwide. Based on the review of the field, the article presents some thoughts for governments to consider for the most responsible e-government and ICT-enabled transformation.



Source (IUCN, 2012)

² Globally, numerous international protocols and conventions on sustainable development exist, such as the Kyoto Protocol and the Copenhagen Accord, where nations come together to agree on meeting goals related to cutting carbon emissions as well as establish mechanisms to accelerate technology transfer in an effort to tackle climate change (iDA, 2012). Also, numerous national and local-level strategies exist in almost all countries throughout the world. However, a primary question remains about the effectiveness of such policies.

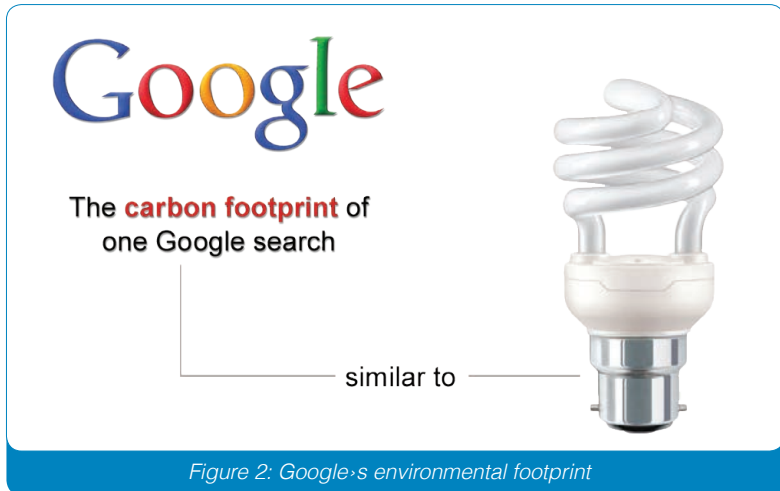
2. ICT: The Problem or the Solution?

Unquestionably, the digital revolution and advances in ICT have reshaped our world in terms of how we communicate and do business. With all of its contributions, ICT is also viewed as being behind increasing socio-economic inequality and environmental damage (Matthews, 2001; Ogbom et al., 2012). Although ICT can contribute to enabling a low-carbon economy, the energy and carbon impact of the sector itself is considered to be significant (Schluepa et al., 2009).

All in all and as the ICT sector continues to grow, the energy consumption and carbon emissions are also growing. The rapid growth of Internet use and the emissions generated from online activity are argued to vary considerably depending on the efficiency of operations and the type of energy used (Foster, 2013). For instance, the carbon footprint of one Google search is equivalent to an 11-watt light bulb that operates for one hour. This should be an issue if we realize that Google processes 100 billion queries every month. See also Figure 2.

On a different note, an increasing demand for computing resources during the past few years has led, in turn, to significant growth in the number of data centers that support e-government and ICT initiatives. This has resulted in an estimated doubling in the energy that the servers use and the power and cooling infrastructure that supports them (Quintiliani et al., 2010). According to Forrester Research, a data center with 1,000 servers will use enough electricity in a single month to power 16,800 homes for a year (Burris et al., 2011).

According to a recent report from the Centre for Energy-Efficient Telecommunications at the University of Melbourne, by 2015, the energy used to run data centers will be a «drop in the ocean» compared with the wireless networks used to access cloud services (Centre for Energy-Efficient Telecommunications [CEET], 2013). The report predicts the energy use of cloud services accessed via wireless networks to grow up to 460% between 2012 and 2015, the equivalent of 4.9 million new cars on the roads.



Another fact related to ICT in this regard is regarding its short lifetime. The fast development pace of today's technologies is constantly shortening electronic devices' lifespans. The ever-growing flow of e-waste as a result is reported to be between 20 million tons to 50 million tons produced each year; e.g., computers, televisions, videocassette recorders (VCRs), stereos, copiers, and fax machines are common electronic products (Schluep et al., 2006).

Recent statistics show that the United States (US) discards 30 million computers each year (Gupta, 2012). A total of 100 million phones are discarded each year in Europe (Begum, 2013). It is forecasted that e-waste worldwide could rise by 500% within the next 10 years in some countries such as India, according to a recently released United Nations Environmental Program (UNEP) report (UNEP, 2009).

Most of the e-waste is exported to developing countries, where it is hidden under the umbrella of charity: "computers for the poor" and the like (Hull, 2010; Luther, 2010). Interestingly, 70% of global e-waste is dumped in China, with most of the rest going to India and to African nations (Liu et al., 2006). Meanwhile, a total of 15–20% of e-waste is recycled, while the rest of these electronics go directly into landfills and incinerators

(Sthiannopkao and Wong, 2012). In light of the informal processing procedures that countries follow coupled with a lack of clear standards, the consequences of such practices have the potential to cause serious health issues and to contribute to greater pollution problems (Robinson, 2009).

Although recent studies admit the significant increase of the ICT carbon footprint, they refer to the fact that the sector is causing only about 2% of global carbon dioxide (CO₂) emissions—as much as air transport—and that its benefits override its tribulations in multifold (Gartner, 2009).

The International Telecommunication Union (ITU) has estimated the contribution of ICTs (excluding the broadcasting sector) to climate change to be between 2% and 2.5% of total global carbon emissions (ITU, 2009). The main contributing sectors within the ICT industry include the energy requirements of personal computers (PCs) and monitors (40%), data centers, which contribute a further 23%, and fixed and mobile telecommunications that contribute 24% of the total emissions (Dunn, 2010).

Although ICT's footprint is projected to rise to 1.27 (2.3%) of Global Total Emissions [GtCO₂e] by 2020, proponents indicate that its abatement potential is seven times higher. See also Figure 3. They argue that ICT could reduce global carbon emissions through efficiency gains across sectors worldwide and is viewed as a high-impact sector in global efforts to address climate change. In addition, it is argued that ICT can play a key role in calculating, monitoring, optimizing, and managing domestic and industrial energy usage and in reducing ICT-related emissions globally. International reports indicate that ICT could save nearly \$1.9 trillion in 2020 and that 29.5 million jobs would be created worldwide as a result (Global e-Sustainability Initiative [GeSI], 2012).

Adversaries emphasize that the ICT industry's responsibility should be viewed as going well beyond facilitating the greening of other industries and enterprises and should rather focus on examining the role of ICT in

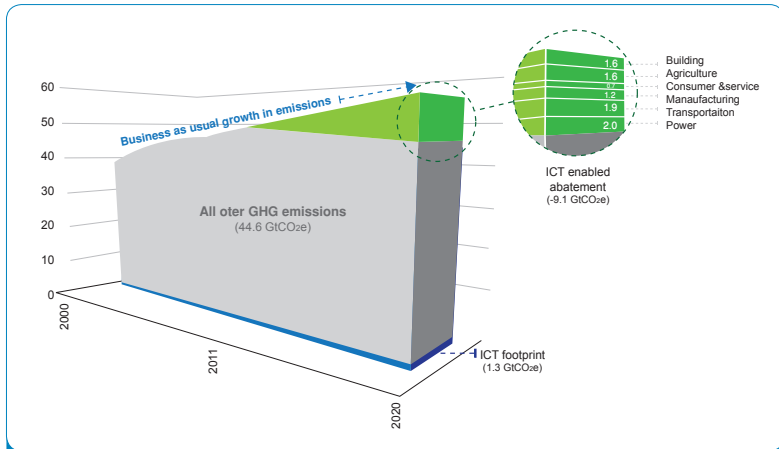


Figure 3: Abatement potential in 2020 plotted with the direct emissions from the ICT industry and total global GHG emissions.

Source: (GeSI, 2012).

climate change as well as the disposal of ICT waste (Dunn, 2010; Hull, 2010; Robinson, 2009).

From a different perspective, international institutions also refer to the fact that production that has a far greater impact on sustainability should not be considered in isolation from consumption (Strange and Bayley, 2008). Although electronic products and services are the shining side of ICT, it is essential to examine the trends and interactions between consumption and production (ibid.). Simply put, the virtual (or digital) economy has physical foundations, and digital products use resources and create waste.

Let us see the relation between production and consumption in the following examples. Emissions from the manufacturing and use of PCs alone will double over the next 12 years as middle-class buyers in emerging economies go digital (Boccaletti et al., 2008). Similarly, worldwide growth in the use of mobile phones will triple its carbon footprint by 2020, due in large to their consumption of silicon and rare metals. However, the fastest-increasing contributor to carbon emissions will be as a result of growth

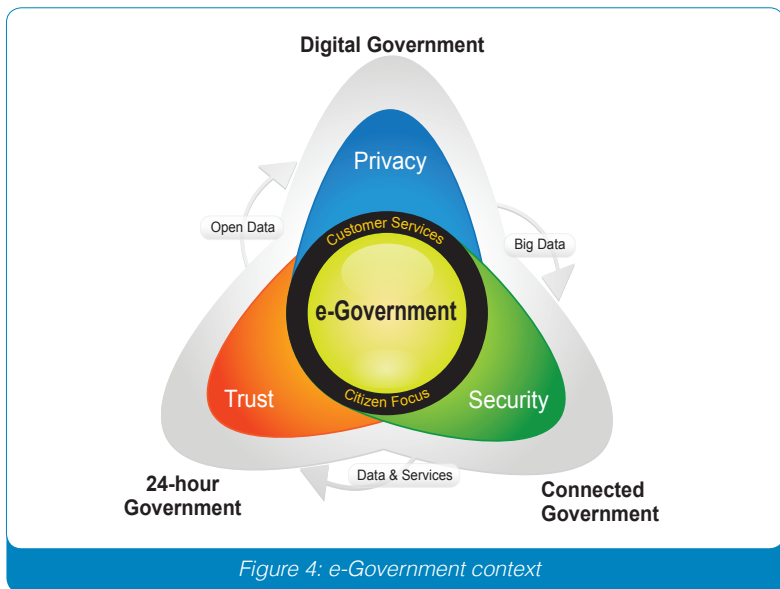
in the number and size of data centers, whose carbon footprint will rise more than fivefold between 2002 and 2020 as organizations in all sectors add servers to meet rising demand even as companies and governments alike attempt to become more energy-efficient (Boccaletti et al., 2008).

In general terms, the present concepts of sustainability and sustainable development are clearly inadequate to drive the transitions necessary to adapt human relations with the rest of the biosphere for the future (Adams, 2006). As currently formulated, they are too loose to drive effective change on the scale required (ibid).

Having said that, the next section attempts to explore environmental sustainability practices in the context of e-government and to discuss their implications for practitioners and researchers.

3. E-government and Sustainability

E-Government can be defined broadly as a service delivery engine that allows services to be requested and delivered over various electronic channels by enabling a connected government, thus resulting in all-around efficiencies in government operations. It is increasingly being seen as the answer to a plethora of problems that governments or public agencies in general face in serving their constituencies effectively (Kumar and Best, 2006). Various terminologies and benefits are associated with e-government, as depicted in Figure 4.



In principle, e-government is not limited to the often quoted services, convenience, availability, etc., but can rather have a big impact on the socio-economic landscape and on environmental sustainability—all three pillars of sustainability. It has a direct impact on time-saving in transactions and in interactions that contribute to potentially millions of dollars of productivity increase. Typically, productivity increases due to the redeployment of resources to the information and knowledge domains that contribute to socio-economic demographics. Add to this the savings

in costs due to transportation obviated by the need to visit government offices, the numbers compound themselves in savings to governments and to reduction in fossil fuel usage.

E-government contributes to the reduction of paper by removing the need to complete and submit cumbersome application forms. This further reduces the need for processing papers, storing, and making copies of them, thus contributing to further reduction of physical paper and hence storage.

Nonetheless, and although considerable attention has been focused on how e-government can help public agencies to improve their services, relatively few studies focus on how e-government programs are architected to facilitate low-carbon environments (Cohen, 1999; Cormier and Magnan, 2004; Devuyt and Hens, 2000; Haigh and Griffiths, 2008). Environmental sustainability is the soundless side in e-government initiatives. It comes as a rather surprising observation that in spite of such obvious environmental factors that e-government initiatives have addressed well, governments have failed in their strategic endeavors to include environmental sustainability and conservation in their e-government efforts. In addition, a dilution and misalignment of national government environmental strategies exist in e-government initiatives. Various research studies support our findings that governments have failed in their strategic endeavors to include environmental sustainability in their e-government efforts (Krishnan and Teo, 2011; Nishant et al., 2013).

Let us have a look at a recent report from the Organization for Economic Cooperation and Development (OCED), which examines e-government initiatives throughout the world (OCED, 2011). Figure 5 depicts the general objectives of e-government, mainly related to a reduction in administrative overheads, the cost reduction of government operations, and responsiveness to citizen needs.

Figure 6 depicts the associated e-government initiatives. Interestingly,

none of the initiatives include environment-related functions. This is hardly surprising since the underlying policies and laws in e-government programs that drive these objectives do not include environmental strategies.

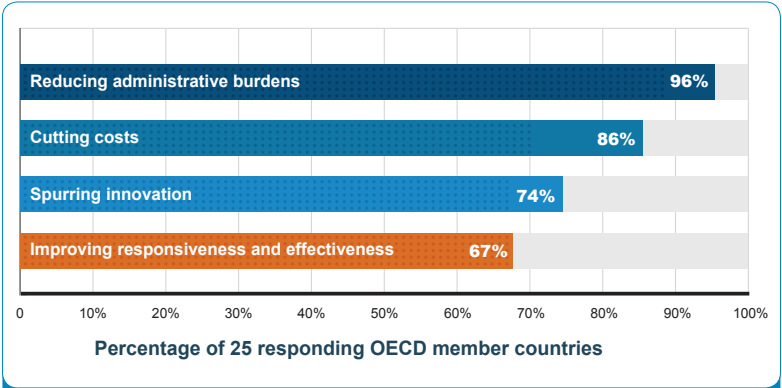


Figure 5: Top e-government objectives identified in central government (2010).

Source: (OCED, 2011)

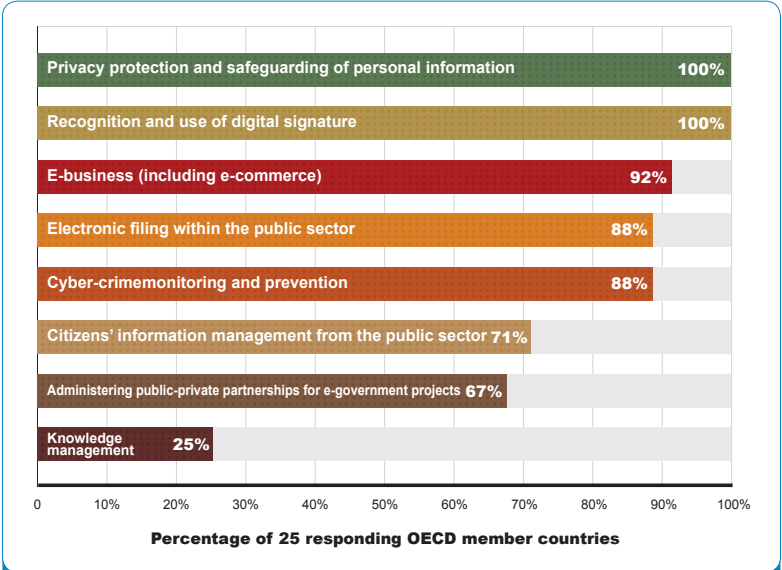


Figure 6: Central government initiatives that enable e-government.

Why exactly do we have this misalignment? The results of a study by Haigh and Griffiths (2008) indicate that while positive environmental outcomes were sought at higher-level e-government strategies, they dissipated as they made their way down to the e-government strategy implementation level. The authors also presented an illustrative framework of four layers in an effort to explain their point, as depicted in Figure 7.

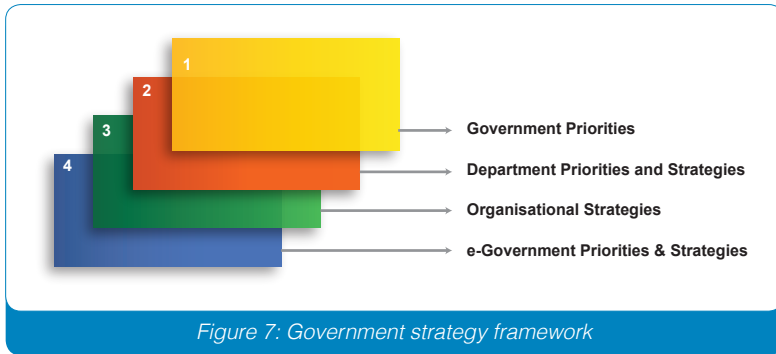


Figure 7: Government strategy framework

Layer 1 in the framework depicts government priorities at a national level. Priorities at this layer have large considerations and include strategic initiatives on the environment sustainability. At the next level of departmental priorities, at the implementation stage, the strategic intents become diluted, although clear initiatives exist under a green environment. At the operational level of organization, where the operational requirement drives strategies more than do national requirements, the environmental considerations become diluted substantially. At the last level of e-government strategies, the environmental considerations are virtually non-existent.

A recent study conducted to investigate environmental sustainability outcomes associated with implementing information systems in Australian government organizations supported the findings of Haigh and Griffiths (2008). Service quality improvements were observed to be a more compelling strategic issue for the organizations, and environmental sustainability outcomes were not sought at the organizational levels and thus not fulfilled at the operational level.

Another study conducted by Nishant et al. (2013) found that empirical support exists for the negative relationship between sustainable IT practices and emissions. The study indicates that organizations basically need to work more collaboratively in order to derive maximum benefits from information obtained about the direct and indirect emissions of their IT initiatives.

Kumar and Best (2006), building on the work of Heeks and Bhatnagar (1999), proposed a number of critical success/failure factors that may explain the adverse relationship between e-government programs and environmental sustainability. These factors are depicted in Table 1.

Table 1: e-Government Success and Failure Factors

Kumar and Best (2006) Critical Failure	Heeks and Bhatnagar (1999) Factors
<ul style="list-style-type: none"> ▸ Training ▸ Sustained leadership, institutionalization ▸ Evaluation and monitoring ▸ Power shift 	<ul style="list-style-type: none"> ▸ People factor ▸ Management, cultural, structural factors ▸ Process and management factors ▸ People, management, cultural, structural factors

Kumar and Best (2006) indicated that public managers should clearly understand the importance of their leadership role in the development and institutionalization of the low-carbon environmental initiatives. They should also focus on the cost/benefit analysis to measure the environmental footprint of main and sub e-government initiatives, both direct and indirect, from production and consumption viewpoints as well.

Zadek (2011) stated that technology providers and users need to have a stake in such initiatives. However, first, governments need to comprehend that a practical, communication, and policy gap currently exists among public awareness, ICT usage, and low-carbon agendas (ibid.).

All in all, e-government initiatives need to reflect national government environmental priorities. If e-government initiatives are not regulated from an environmental perspective, they will potentially result in counter-productive and misaligned initiatives.

E-government by design contributes to the development of virtual environments: electronic transactions that lead to the generation of lots of content. However, if this content is not managed with a clear policy or with the intention of being printed again for archival reasons, for example, the very purpose of environment conservation and sustainability would be defeated. Another example would be in the use of electronic channels and the devices. All electronic devices consume power, although with variances. Inefficient devices consume more power and are counter-productive to environmental sustainability. Governments need to work more effectively to demonstrate their ability to deliver large savings in energy consumption. Figure 8 shows that the use of more efficient technologies have the potential to cut electricity consumption by an estimated 30% in 2030, compared with the business-as-usual scenario (2009)³.

E-government programs also rely on high-tech and large data centers for enabling virtual and electronic environments. Governments need to re-evaluate the ICT infrastructure to minimize inefficient power consumption, i.e., badly designed data centers may increase energy usage, while poorly designed or over-designed servers and storage may also lead to the same results. Governments need to work more effectively to demonstrate their ability to deliver large savings in energy consumption.

3 The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) is a standards-publishing organization for specifications for green buildings. Many data centers and buildings adopt these standards now for the green environment. They specify the air conditioning and heating requirements based on different cooling systems. Further, data centers use a very crucial index to determine "green efficiency" as power utilization efficiency (PUE). This is the ratio of the total power used in a data center/ICT Load. PUE shows how well a data center has been defined. All of the supporting equipment (such as pumps, blowers, motors, heat exchangers, UPS, etc.) that are used in the data centers consume power. Ideally, PUE should be about 1.2 and go up to an acceptable 1.7. This means that the auxiliary equipment that is used for the data centers should consume no more than 70% max of the power that the ICT equipment uses. It is estimated that 80% of data centers in the world have a PUE of 2.5 and above. See also ASHRAE (2009).

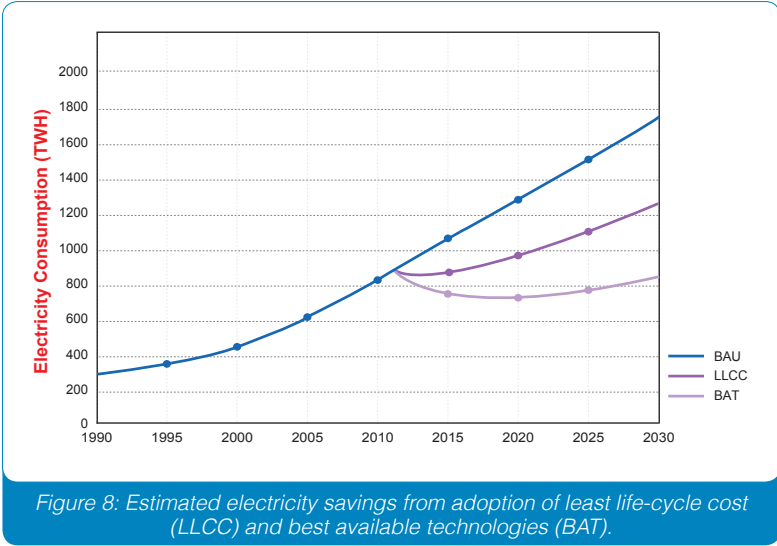


Figure 8: Estimated electricity savings from adoption of least life-cycle cost (LLCC) and best available technologies (BAT).

Source: (IEA, 2009)

Several other such examples that could be cited include the disposal or rather unregulated disposal of devices such as desktops, laptops, and mobile phones, which may contribute to major land pollution disasters. Governments need to develop clear policies to regulate the disposal of devices, especially in relation to the overall management of e-waste.

Definitively, it is imperative that governments need to examine their e-government programs and initiatives in the context of environment sustainability. They need to focus on redressing the increasing carbon footprints that stem from high-energy infrastructures and applications, such as call centers, cloud computing data centers, ultra-fast servers, complex telecommunications networks, equipment-cooling devices and expensive air conditioning, the use of multiple PCs, powerful modems, and ubiquitous mobile phones (Dunn, 2010).

Two of the areas to which governments need to pay attention in their overall e-government design strategies are related to (1) cloud services and (2) shared resources:

- **Cloud Services:** Government initiatives to move to the cloud may substantially contribute to hardware (servers) consolidation and efficiency improvements in the delivery of service.
- **Shared Resources:** From a government perspective, national data centers as shared data centers should be considered in order to reduce the burden of individual data centers. This obviates the need for individual data centers for each department and ensures higher productivity in service provisioning. This approach is being followed in South Korea and India.

In short, environmental sustainability must be defined as a key and strategic pillar in the overall e-government and ICT production and consumption equilibrium. E-government initiatives and programs need to adhere to national and international policies and frameworks for sustainable development. National strategies related to environmental sustainability need not only to focus on idiosyncratic descriptive measures, but must focus on the set of functions and on promoting a coherent effort in establishing mechanisms to ensure effective implementation and anticipated outcome realization.

4. Conclusion

Without a doubt, ICTs and e-government programs by design contribute positively to both socio-economic and sustainable development. It is imperative that e-government strategies and objectives need to explicitly include environmental sustainability as a key strategic objective. Such alignment must happen at a national level and must be monitored at implementation levels for efficiency and effectiveness. It needs to be managed diligently across all of the layers of strategic prioritization, i.e., laws, policies, regulations, compliance, etc.

Governments today give less attention to how their agencies develop e-government services and have little or no awareness of how they were designed in principle. Governments need to create a mindset that establishes linkage between consumption and production. In light of the gigantic investments in technological development, governments need to be aware of their practices' impacts with relation to environmental sustainability.

Governments have to identify the critical relations among the many factors that are likely to shape economic, social, political, and environmental quality. These elements need to be viewed together but not in isolation. Governments need to find a balance between the need to improve the quality of life of their people and addressing the demand for increased ICT access and services provisioning. However, simultaneously, governments need to work harder to reduce the overwhelming environmental footprint of their current practices and the environmental impact associated with evolving ICT use. This should also be balanced with the environmental impacts (positives and negatives) associated with such needs.

Leadership at the national level is one key element. Furthermore, strategies that are seen as simply one more government program imposed from above have less of a chance of succeeding than do those defined through consultation and debate (Zadek, 2011). Such strategies need to be developed based on the use of local human resources in the context

of social equity and sustainable socio-economic and environmental development.

Governments need to establish sound policies and incentivizing practices alongside tough environmental regulations in order to align e-government objectives with social requirements for the more environmentally responsible use of ICTs (Dunn, 2010). Such incentives need to be followed by vibrant targets and rules in order to promote the development of sustainable e-government models.

Governments clearly need to work together at both national and international levels to create standards and practices in relation to ICT usage in different sectors. Such policies and standards need to be rigorous enough to be effective, but they also must be flexible enough to be adapted as circumstances and priorities evolve (Kuhndt et al., 2003; Strange and Bayley, 2008). This should be seen as a critical activity for supporting the transition toward a lower-carbon world and in order to improve the quality of life for impoverished and underserved communities of people worldwide while simultaneously reducing our overwhelming environmental footprint.

The bottom line is that environmental sustainability cannot be left to individual countries, organizations, and persons. Rather, governments need to work together more seriously to systematically react to changing needs and changing social and environmental pressures. Without this, the game of «Is it the chicken or the egg?» will keep surfacing as accountability is lost between the complex ecosystem of stakeholders.

References

Adams, W.M. (2006). The Future of Sustainability: Re-thinking Environment and Development in the Twenty-first Century. Report of the IUCN Renowned Thinkers Meeting, 29–31 January 2006. http://cmsdata.iucn.org/downloads/iucn_future_of_sustainability.pdf

Arnaud, B.S. (2012). Using ICT for Adaptation Rather Than Mitigation to Climate Change. The International Institute for Sustainable Development. http://www.iisd.org/pdf/2012/com_icts_starnaud.pdf

ASHRAE. (2009). Proposed Standard 189.1P, Standard for the Design of High-Performance Green Buildings Except Low-Rise Residential Buildings, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., Atlanta, GA. https://osr.ashrae.org/Public%20Review%20Draft%20Standards%20Lib/189.1P_3rd_PPRDraft.pdf

Brundtland, B.H. (1987). Our Common Future (Oxford: Oxford University Press, for the World Commission on Environment and Development).

Barton H. (2000). Conflicting perceptions of neighbourhood. In Sustainable Communities, Barton H (ed.). London: Earthscan, 3–18.

Begum, K.J.A. (2013). Electronic waste (e-waste) management in India: A review. IOSR Journal of Humanities and Social Science, 10 (4): 46–57.

Blakemore, M. and Wilson, F. (2009). MC-eGov: Study on Multi-channel Delivery Strategies and Sustainable Business Models for Public Services addressing Socially disadvantaged Groups. European Commission. http://ec.europa.eu/information_society/activities/einclusion/library/studies/docs/mc_egov_final_report.pdf

Boccaletti, G., Löffler, M. and Oppenheim, J. (2008). How IT can cut carbon emissions, The McKinsey Quarterly, October, p. 2. www.mckinsey.com/client/service/sustainability/pdf/how_it_can_cut_carbon_missions.pdf

Burris, P. Mines, C. and Wang, N. (2011). 2012 IT Budget Planning Guide for CIOs. Forrester Research.

Centre for Energy-Efficient Telecommunications [CEET]. (2013). The Power of Wireless Cloud. Centre for Energy-Efficient Telecommunications, The University of Melbourne, Australia. http://www.ceet.unimelb.edu.au/pdfs/ceet_white_paper_wireless_cloud_jun13.pdf

Cohen, N. (1999). Greening the Internet: Ten ways e-commerce could affect the environment. *Environmental Quality Management*, 9 (1): 1–15.

Cormier, D. and Magnan, M. (2004). The impact of the Web on information and communication modes: the case of corporate environmental disclosure. *International Journal of Technology Management*, 27 (4): 393–416.

Devuyt, D. and Hens, L. (2000). Introducing and measuring sustainable development initiatives by local authorities in Canada and Flanders (Belgium): A comparative study. *Environment, Development and Sustainability*, 2 (2): 81–105.

du Plessis, C. (2000). Cities and sustainability: Sustaining our cultural heritage. In *Cities and Sustainability: Sustaining Our Cultural Heritage*, Conference Proceedings, Brandon P, Lombardi P, Perera S (eds). Sri Lanka: Kandalama.

Dunn, H.S. (2010). The Carbon Footprint of ICTs. University of the West Indies. www.giswatch.org/thematic-report/sustainability-climate-change/carbon-footprint-icts

Foster, P. (2013). The EC is working with the ICT companies to measure the carbon footprint of their industry. *The Green IT Review*, <http://www.thegreenitreview.com/2013/03/the-ec-is-working-with-ict-companies-to.html>

Gartner. (2009). Gartner estimates ICT industry accounts for 2 percent of global CO2 emissions. www.gartner.com/it/page.jsp?id=503867

Global e-Sustainability Initiative [GeSI]. (2013). GeSI SMARTer 2020: The Role of ICT in Driving a Sustainable Future. 2 Global e-Sustainability Initiative aisbl and The Boston Consulting Group, Inc. http://gesi.org/assets/js/lib/tiny_mce/jscripts/tiny_mce/plugins/ajaxfilemanager/uploaded/SMARTer 2020 - The Role of ICT in Driving a Sustainable Future December 2012.pdf

Giddings, B. Hopwood, B. and O'Brien, G. (2002). Environment, economy and society: Fitting them together into sustainable development. *Sustainable Development*, 10, 187–196. <http://200.23.34.56/convocatoria/lecturas/sustainable%20development.pdf>

Gupta, D. (2012). E- Waste: A global problem and related issues. *International Journal of Scientific & Engineering Research*, 3 (10): 1–12. <http://www.ijser.org/researchpaper%5CE--Waste-A-Global-Problem-and-related-issues.pdf>

Haigh, N.L. and Griffiths, A. (2008). E-government and environmental sustainability: Results from three Australian cases. *Electronic Government: An International Journal*, 5 (1): 45–62.

Hardi, P. and Zdan, T. (1997). Assessing Sustainable Development. Winnipeg: International Institute for Sustainable Development.

Hull, E.V. (2010). Poisoning the poor for profit: The injustice of exporting electronic waste to developing countries. *Duke Environmental Law & Policy Forum*, 21 (1). <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1038&context=delpf>

Info-communications Development Authority of Singapore [IDA]. (2012). Co-creating the Future InfoCom Technology Roadmap 2012: ICT and Sustainability. Info-communications Development Authority of Singapore. <http://www.ida.gov.sg/~media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/ICTandSustainability.pdf>

International Energy Agency [IEA]. (2009). *Gadgets and Gigawatts: Policies for Energy Efficient Electronics*. France, <http://www.iea.org/publications/freepublications/publication/gigawatts2009-1.pdf>

International Council for Local Environmental Initiative [ICLEI]. (1996). *The Local Agenda 21 Planning Guide: An Introduction to Sustainable Development Planning*. Toronto: ICLEI.

International Telecommunication Union [ITU]. (2009). *ICTs and Climate Change*, background paper for the ITU Symposium on ICTs and Climate Change, Quito, Ecuador, 8–10 July.

International Union for Conservation of Nature [IUCN]. (2012). *The Future of Sustainability: Re-thinking Environment and Development in the Twenty-first Century*. [Online]. Available from: http://cmsdata.iucn.org/downloads/iucn_future_of_sustainability.pdf [Accessed 9th July 2012].

Jens Schippl, J. and Weinberger, N. (2008). *Assessing the Potential of ICT to Increase Energy Efficiency and Fight Climate Change—Key Technologies and Prospects*. European Parliament, <http://www.itas.fzk.de/deu/lit/2009/scwe09a.pdf>

Krishnan, S. and Teo, T. (2011) *Moderating Effects of Environmental Factors on E-Government, E-Business, and Environmental Sustainability* (December 6, 2011). ICIS 2011 Proceedings. Paper 2.

<http://aisel.aisnet.org/icis2011/proceedings/ebusiness/2>

Kuhndt, M., von Geibler, J., Turk, V., Moll, S., Schallaböck, K. and Steger, S. (2003). *Virtual Dematerialisation: Ebusiness and Factor X: Final Report: Forum for the Future*. http://www.ecotic.es/files/Informe_ebusiness_and_factor_x.pdf

Kumar, R. and Best, M.L. (2006). *Impact and Sustainability of E-Government Services in Developing Countries: Lessons Learned from Tamil Nadu, India*. *The Information Society*, 22: 1–12. <http://mikeb.inta.gatech.edu/papers/infosoc.egov.kumar.best.pdf>

Labelle, R., Rodschat, R. and Vetter, T. (2008). *ICTs for e-Environment Guidelines*

for Developing Countries, with a Focus on Climate Change, International Telecommunication Union, Geneva, Switzerland. <http://www.itu.int/ITU-D/cyb/app/docs/itu-icts-for-e-environment.pdf>

Liu, X.B., Tanaka, M. and Matsui, Y. (2006). Generation amount prediction and material flow analysis of electronic waste: A case study in Beijing, China. *Waste Manag Res*, 24: 434–45.

Luther, L. (2010). Managing Electronic Waste: Issues with Exporting E-Waste. <http://www.fas.org/sgp/crs/misc/R40850.pdf>

Mansell, R. (2012). ICT Innovation and Sustainable Development. The International Institute for Sustainable Development. http://www.iisd.org/pdf/2012/com_icts_mansell.pdf

Matthews, H.S. (2001). The Environmental Implications of the Growth of the Information and Communications Technology Sector, paper for Environment Directorate, OECD, Paris, 2001.

Nishant, R., Teo, T.S.H. and Goh, M. (2013). Understanding the Environmental Impact of Sustainable IT: An Empirical Examination. Proceedings of the 18th Pacific Asia Conference on Information Systems (PACIS 2013), Jeju Island, Korea, June 18–22 <http://www.pacis-net.org/file/2013/PACIS2013-094.pdf>

OECD (2011) Government at a Glance. Organisation for Economic Co-operation and Development (OECD). <http://www.oecd.org/inclusive-growth/Government%20at%20a%20Glance%202011.pdf>.

Ogbomo, M.O., Obuh, A.O. and Ibolo, E. (2012) Managing ICT Waste: The Case of Delta State University Abraka, Nigeria. *Library Philosophy and Practice* 2012, <http://www.webpages.uidaho.edu/~mbolin/obuh-ogbomo-ibolo.htm>

Quintiliani, A. Chinnici, M., Kolentini, E., Racovičan, I., Ionescu, I., Destree, K., Kester, J., Franchioni, G. and Chebbo, M. (2010). ICT and Environment Protection: Report on ICT requirements, offers and needs. European Commission within the ICT Policy Support Programme. http://seesgen-ict.rse-web.it/content/files/documents/Deliverables/Deliverable_20D6-2_20R0-1.pdf

Robinson, B.H. (2009). E-waste: An assessment of global production and environmental impacts. *Science of the Total Environment*, 408, 183–191.

Schluepa, M., Hageluekenb, C., Kuehrc, R., Magalinic, F., Maurerc, C., Meskersb, C., Muellera, E., and Wangc, F. (2009). Recycling—from E-waste to Resources. United Nations Environment Programme & United Nations University. http://www.unep.org/pdf/pressreleases/E-waste_publication_screen_finalversion-sml.pdf

Souter, D., MacLean, D. and Creech, H. (2013) Towards Knowledge Societies for

Peace and Sustainable Development. UNESCO Conference Paris 25–27 February 2013. <http://ictstheinternetandsustainability.wordpress.com/>

Sthiannopkao, S and Wong, M.H. (2012). Handling e-waste in developed and developing countries: Initiatives, practices, and consequences. *Sci Total Environ*, vol (issue): xx–yy.

Strange, T. and Bayley, A. (2008) Sustainable development: Linking economy, society, and environment. OECD Publishing. <http://www.oecd-ilibrary.org/docserver/download/0108121e.pdf?expires=1374871268&id=id&accname=guest&checksum=D7E1A6C9EC49B00AD295E3A6B1AB4659>

United Nations [UN]. (2005). World Summit Outcome, Resolution A/60/1, adopted by the General Assembly on 15 September 2005, http://data.unaids.org/Topics/UniversalAccess/worldsummitoutcome_resolution_24oct2005_en.pdf

United Nations Environment Programme [UNEP]. (2009). Recycling—from e-waste to resources—solving the e-waste problem. Sustainable innovation and technology transfer industrial sector studies. United Nations Environment Programme. http://www.unep.org/PDF/PressReleases/E-Waste_publication_screen_FINALVERSION-sml.pdf

United States (U.S.) Environmental Protection Agency. [Online]. Available from: <http://www.epa.gov/epawaste/conserva/materials/eycling/manage.htm>. Retrieved 2012-03-13.

Vickery, G. (2012). Smarter and Greener: Information Technology and the Environment: Positive or Negative Impacts? The International Institute for Sustainable Development. http://www.iisd.org/pdf/2012/com_icts_vickery.pdf

Zadek, S. (2011). Green growth's invisible ingredient. *China Dialogue*. www.chinadialogue.net/article/show/single/en/4163-Green-growth-s-invisible-ingredient



About Emirates Identity Authority

هيئة
الإمارات
للهوية
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.

About the Author



H.E. Prof. Dr. Ali Mohamed Al-Khouri is the Director General (Under Secretary) of the Emirates Identity Authority (Emirates ID), a federal government organization in the United Arab Emirates (UAE). He was appointed to this role in 2009. Prior to joining Emirates ID, he worked with the Ministry of Interior where he got involved in many successful strategic and mission-critical projects. With his strategic and performance driven orientation, he played a vital role in converting the organization into one of the most successful government agencies in the UAE and a benchmark both regionally and worldwide in strategy and management practices, and niche technology implementations.

He was recently selected and joined the World Economic Forum Global Agenda Council on Social Security Systems, as one of the world's most relevant and knowledgeable thought leaders in this field, and to support the Council deliver pertinent insights and collaboratively develop solutions to address major global challenges. He is also a Special Advisor to the European Union for Single Electronic Identification and Authentication Project in Europe (STORK 2.0), and as an Advisory Observer for Secure Identity Alliance in Europe.

Dr. Al Khouri is a fellow and member of many scientific and research associations, and is recognized both nationally and internationally as think-tank, and for his management expertise and technical knowledge in various field of practices in government and public sector. He has developed different intellectual methodologies and frameworks to handle the challenges faced by government organizations, among which is an innovative methodology for planning and strategic management of government sector projects, and another innovative methodology for e-government transformation to enable the concept of customer centrality and improve public sector service delivery. He has got more than 12 patented inventions and intellectual properties.

Dr. Al-Khouri is also a Professor of Identity and Security and Follow of the British Institute for Technology and e-Commerce in London, UK, and is also on several advisory boards of academic institutions. He is an active researcher in the field of organizational development and transformation, e-government, knowledge-based digital economy, identity management, and in many other specialized fields. He has published many books and over 80 scientific research articles in international peer-reviewed journals in the past 12 years. He received many national and international awards among which, was the «Most Influential Personality in Digital Identity World in a Decade» in 2011 in Italy.

Dr. Al Khouri attained his higher education from the top UK universities, where he received his B.Sc. (Hons.) in «Business Information Technology Management» from Manchester University, M.Sc. in «Information Management» from Lancaster University, and an Engineering Doctorate (EngD) from Warwick University in the field of «Strategic and Large Government Projects Management».



Some Recent Articles for the Author:

2013

1. Al-Khouri, A.M. (2013) "Digital Identity: Transforming GCC Economies", Special issue on Research, Innovation and Entrepreneurship Reforms in Gulf Cooperation Council (GCC) Countries, *Journal of Innovation: Management, Policy & Practice*.
2. Al-Khouri, A.M. (2013) "e-Government in Arab Countries: A 6-Stage Roadmap to Develop the Public Sector", *International Journal of Management and Strategy*, Vol. 4, No. 1.
3. Al-Khouri, A.M. (2013) "Identity and Mobility in a Digital World ?", *Technology and Investment*, Vol. 4, No. 1.
4. Al-Khouri, A.M. (2013) "Triggering the Smart Cards Supply Chain", *Technology and Investment*, Vol. 4, No. 2.

2012

5. Al-Khouri, A.M. (2012) "Data Ownership: Who Owns 'My Data'?", *International Journal of Management and Information Technology*, Vol. 2, No. 1, pp. 1-8.
6. Al-Khouri, A.M. (2012) "Customer Relationship Management: A Proposed Framework from a Government Perspective", *International Journal of Management and Strategy*, Vol. 3, No. 4, pp. 34-54.
7. Al-Khouri, A.M. (2012) "Biometrics Technology and the New Economy", *International Journal of Innovation in the Digital Economy*, Vol. 4, No. 4.
8. Al-Khouri, A.M. (2012) "e-Voting in UAE FNC Elections: A Case Study", *Information and Knowledge Management*, Vol. 2, No. 6, pp. 25-84.
9. 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. 3, No. 2, pp. 57-69.
10. Al-Khouri, A.M. (2012) "eGovernment Strategies: The Case of the United Arab Emirates", *European Journal of ePractice*, No. 17, pp. 126-150.
11. Al-Khouri, A.M. (2012) "Corporate Government Strategy Development: A Case Study", *Business Management Dynamics*, Vol. 2, No. 1, pp. 5-24.
12. Al-Khouri, A.M. (2012) "PKI in Government Digital Identity Management Systems", *Surviving in the Digital eID World*, *European Journal of ePractice*, No. 4, pp. 4-21.
13. 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.
14. Al-Khouri, A.M. (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.
15. Al-Khouri, A.M. (2012) "Population Growth and Government Modernisation

Efforts", *International Journal of Research in Management & Technology*, Vol. 2, No. 1, pp. 1-8.

16. Al-Khouri, A.M. (2012) "Projects Management in Reality: Lessons from Government Projects", *Business and Management Review*, Vol. 2, No. 4, pp. 1-14.
17. 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.

2011

18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. Al-Khouri, A.M. (2011) "Improving Organizational Performance through understanding Human Motivation". *Chinese Business Review*, Vol.10, No.5, pp. 384-394.
24. 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.
25. 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.

2010

26. 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.
27. 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.
28. 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.

29. Westland, D.D. and 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. This article was published on United Nations website and was recognised as one of the major studies on e-government in the Arab and Middle East region.
30. Al-Khouri, A.M. (2010) "Improving Organisational Performance", *Proceedings of the 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.
31. 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.
32. 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.
33. 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.

2008

34. Al-Khouri, A.M. (2008) "Why Projects Fail? The devil is in the detail," *Project Magazine* [Online]. Available from:www.projectmagazine.com.
35. 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.

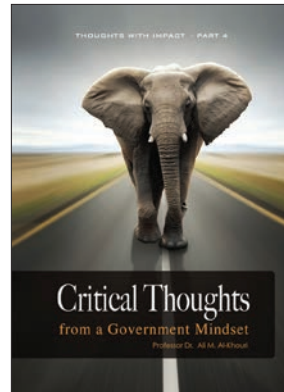
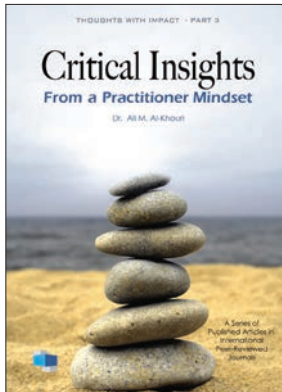
2007

36. 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.
37. 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.
38. 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.
39. Al-Khouri, A.M. (2007) "UAE National ID Programme Case Study," *International Journal Of Social Sciences*, Vol. 1, No. 2, pp.62-69.
40. 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.

41. Al-Khoury, A.M. (2007) "Quality Models for IT Systems," Proceedings of World Academy of Science, Engineering and Technology, Vienna, Austria, Vol. 21.



previous volumes in this series



Log on to our Website to read them
www.id.gov.ae

International Standard Book Number

ISBN 978-9948-20-683-5

All Information, Photos, Charts and Designs Found in this Book Belongs to Emirates Identity Authority
Any usage or duplication without formal authorization form is prohibited
© 2014 Emirates Identity Authority. All Rights reserved.

Production and Design: **Mohamed Mabrouk**

THOUGHTS WITH IMPACT PART 5

Critical Insights

from a Government Line of **Attack**



The author in bullets:

- Director-General (Under Secretary) of Emirates Identity Authority, UAE since 2009.
- Holds Engineering Doctorate in Strategic & Large Government Projects Management from Warwick University, UK.
- Participated in many mission-critical & strategic projects implementation with a total of 25 years of experience.
- Renowned practitioner & internationally recognized as a think-tank & reflective researcher.
- Professor and Fellow of the British Institute of Technology & E-commerce.
- Published many books & more than 80 papers in international journals in the last ten years.
- Special Advisor to the European Commission (STORK 2.0) project.
- Member of the Global Agenda Council on Social Security Systems, World Economic Forum.
- Awarded (Most Influential Personality in Digital Identity World in a Decade) in 2011.
- Won (Al-Owais Award for Research & Scientific Studies) twice.
- Developed many methodologies & frameworks & has more than 12 patents & intellectual property rights.
- A member in government boards & committees, & many national & international scientific & research associations.

This book is the fifth in a series that groups together research articles published in prominent international peer-reviewed journals between 2013 and 2014. The articles document UAE government plans and practices in the field of identity management, & the context in which governments may fabricate trusted & secure cross-border identity authentication & validation infrastructure to support the development of the digital economy.

Articles included:

Smart Government

- Technological and Mobility Trends in e-Government
- Exploring the Role of Technology in a Joined up Government: A Proposed Framework for Service Governance
- Connected Government: UAE Government Integration Strategy

Digital Identity

- Digital Identity: Transforming GCC Economies
- Federated e-Identity Management across the Gulf Cooperation Council
- Identity Management in the Age of Mobilificaiton

Identity Applications

- Privacy in the Age of Big Data: Exploring the Role of Modern Identity Management Systems
- Identity Management in the Retail Industry: The Ladder to Move to the Next Level in the Internet Economy
- Environment Sustainability in the Age of Digital Revolution: A Review of the Field

ISBN 978-9948-20-683-5