International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:5, 2008

Electronic Government in the GCC Countries

A.M. Al-Khouri, and J. Bal

***Abstract*—**The study investigated the practices of organisations in Gulf Cooperation Council (GCC) countries with regards to G2C e-government maturity. It reveals that e-government G2C initiatives in the surveyed countries in particular, and arguably around the world in general, are progressing slowly because of the lack of a trusted and secure medium to authenticate the identities of online users. The authors conclude that national ID schemes will play a major role in helping governments reap the benefits of e-government if the three advanced technologies of smart card, biometrics and public key infrastructure (PKI) are utilised to provide a reliable and trusted authentication medium for e-government services.

***Keywords*—**e-Government, G2C, national ID, online authentication, biometrics, PKI, smart card.

I. Introduction

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

Evaluating current practices, recent studies show that the implementation of e-government programmes is not a simple task as many if not all governments lack the fundamental infrastructure, organisational culture, understanding and resources for a transformation of the magnitude that e-governments require.

Many researchers have addressed the technical and management issues surrounding e-government projects. Many others also have demonstrated the challenges associated with the implementation of e-government programmes, and put forward recommendations to overcome them. Despite the variety of approaches that were proposed in the literature to handling government electronic services, not one proven solution or framework to build e-government architecture appears to exist.

The objective of this research study is to provide a short overview of the current literature in the research area and relate this information to the issues surrounding e-government initiatives. In principle, the study is designed to:

(1) explore the potential applications of a national ID card and its suitability as a reliable medium to verify virtual online identities (if implemented with smart card, biometrics, and PKI technologies), and

(2) conduct a postal survey (followed by telephone interviews of executives) of organisations in the GCC[1] countries to understand their e-government practices and progress.

The finding of the study adds to the body of knowledge, as it draws a picture of the current practices, assesses the progress in the field of e-government and pinpoints the key obstacles and the degree to which national ID programmes can support the progress of G2C initiatives.

This paper is structured as follows. First a short overview of the current literature on e-government is provided to highlight current trends, patterns, and models for such initiatives as well as the barriers to successful implementation. The following sections establish a link between national ID card schemes and e-government by looking at the technology requirements for enabling a reliable digital ID framework that can support and enable e-government development. Then the research survey methodology is explained, findings are presented and conclusions drawn.

II. The Illusion of E-Government

Citizens' experience with the 24x7 world of the private sector has fuelled demands for similar experience with their governments; easy to deal with, available when you want them to be, one-stop service that is personalised with simple completion of transactions on line. This utopia bears little resemblance to most government's current capabilities; multiple agencies, multiple payment and delivery options, little coordination or standards, modest online functionality and variable customer service capabilities. Citizen demands are at odds with the current structure of most government agencies. Evidence is emerging however that when government does go online successfully, patterns of interaction are dramatically changed.

In principle, the literature examines e-government activities in terms of the interactions between sectors of government, businesses and citizens [1]. The matrix in Fig. 1 shows the nine principle interactions. Some research studies also included employees in this spectrum. However, many

Manuscript received March 27, 2007.

A.M. Al-Khouri is with Emirates Identity Authorit, Abu Dhabi, United Arab Emirates (phone: +97150-613-7020; fax: +9712-404-6661; e-mail: alkhouri@ emiratesid.ae).

J. Bal is with Warwick University, United Kingdom (e-mail: jaybal@warwick.ac.uk).

[1] The surveyed organisations in this study were all from the Southern Gulf countries; Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates often referred to as the Gulf Co-operation Council (GCC) countries.

researchers have considered the employee element to go under government activities.

Suppliers of services \ Recipient of Services	Citizen	Government	Business
Citizen	**Citizen to Citizen (C2C)** e.g., small advertisement	**Citizen to Government (C2G)** e.g., tax declaration by single person or family	**Citizen to Business (C2B)** e.g., job exchange by job seekers
Government	**Government to Citizen (G2C)** e.g., benefit processing	**Government to Government (G2G)** e.g., transactions between Pas	**Government to Business (G2B)** e.g., procurement of PAs
Business	**Business to Citizen (B2C)** e.g., Online order in a shopping mall	**Business to Government (B2G)** e.g., tax declaration by private organisation	**Business to Business (B2B)** e.g., procurement through EDI

Fig. 1 e-Government's interactions

A. *Government-to-Government (G2G)*

This represents the backbone of e-government. It involves sharing data and conducting electronic exchanges between governmental departments, rather than being focused on the specific agency or agencies responsible for administering programs and policies.

B. *Government-to-Business (G2B):*

It includes both the sale of surplus government goods to the public, as well as the procurement of goods and services. It aims to more effectively work with the private sector because of the high enthusiasm of this private sector and the potential for reducing costs through improved procurement practices and increased competition.

C. *Government-to-Citizen (G2C) – (the focus of this paper)*

This provides opportunities for greater citizen access to, and interaction with the government. This is what some observers perceive to be the primary goal of e-government. Thus, and from G2C perspective, many government agencies in developed countries have taken progressive steps toward the web and ICT use, adding coherence to all local activities on the Internet, widening local access and skills, opening up interactive services for local debates, and increasing the participation of citizens on promotion and management of the territory [2].

Several approaches were proposed in the literature to handling electronic services. However, the literature provides not one proven solution or framework to build e-government architecture. For this very same reason, e-government architecture development practices around the world vary according to several factors (the technical team experience, solution provider, consultants, budget, technological limitations, etc.), leaving those organisations with no choice but to go for a model and then enhance it based on new requirements and/or constraints.

To build such architectures, governments need to understand the complexity associated with the development and transition stages of e-government. One of the well-known models in the literature that outlines the stages of e-government development was developed by Layne & Lee [3] that outlines the stages of e-government development. In moving to the first two phases, government organisations are faced with technological challenges such as those in Fig. 2. Stage three and four is where governments instead of automation, they transform their services and integrate processes and functions across the different levels of the government to create an integrated information base, implementing a 'one-stop-shopping' concept for its citizens.

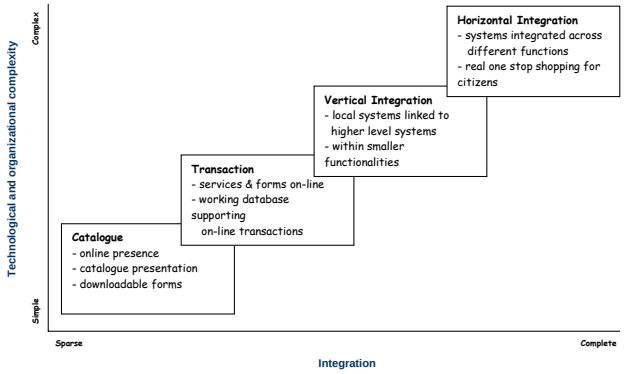

Fig. 2 Dimensions and stages of e-government

The model assumes that e-government initiative will require both horizontal and vertical integration; horizontal as e-government efforts must extend to all departments within a level of government (i.e., federal, state, local) and vertical as e-government initiatives must integrate across levels of government.

It was observed in the literature that some researchers used Layne & Lee's four phases and interpreted them as components of a maturity model to judge the maturity of the processes of an organisation and for identifying the key practices that are required to increase the maturity of these processes - see for example [4]. By focusing on a limited set of activities and working aggressively to achieve them, it is argued that the maturity model can steadily improve organisation-wide e-government processes and enable continuous and lasting gains in the e-government capabilities. However, and according to various studies of e-government practices around the world, many researchers have found that such initiatives are stuck in phase one and two, far from the ideal integrated digital government [5]. Researchers have identified many technical and organisational barriers challenging e-government progress to move up the ladder to stage three and four of Layne & Lee's model (see Fig. 3).

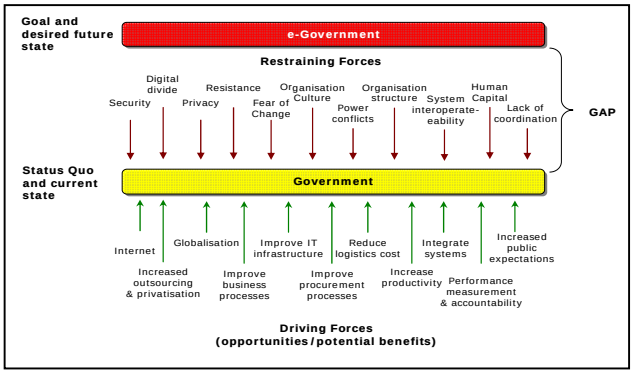

Fig. 3 e-government force analysis

It appears the current literature does not give enough attention to the need in e-government programmes for identity verification which is believed by the authors to be the foundation for G2C initiatives. It is argued by the authors that if governments are to complete phase two of the Layne & Lee (2001) model and enable a much larger and more comprehensive set of G2C transactions to take place online, they will need to ensure that citizens have the ability to authenticate themselves online and verify their identities - see also [6]. Governments need to develop clear vision of how they intend to authenticate individuals' digital identities [7]. A digital identity is the representation of a human identity that is used in a distributed network interaction with other machines or people [8]. Their vision need to look at the different options available for building a digital identity management infrastructure that "allows transactions in which the parties are separated in time and space while retaining the ability of these transactions to contain all of the human identity based attributes that transactions between people have always had" [8]. Only with a robust digital identity infrastructure can the true power of G2C applications be released.

Initiatives such as national ID projects are a key to G2C e-government progress, and a step towards building a secure digital infrastructure that can enable online identification and authentication. The national ID project is seen by the authors as a good opportunity to build the governments' central identity infrastructure component for e-government initiatives. The next section looks at how advanced technologies can support G2C e-government and provide a robust digital ID as well as a solid foundation for developing secure applications and safeguarding electronic communications.

III. National ID and G2C E-Government

National ID programmes may well address many of the security issues related to electronic communications and the verification of online identities, provided that appropriate technologies are utilised. This can also be realised by looking at one of the primary goals of such schemes, take for instance the UAE national ID project, which aims to improve the country's ability to accurately recognise peoples' identities through identification (1:N) and verification (also referred to as authentication) (1:1) methods as depicted in Fig. 4 [9].

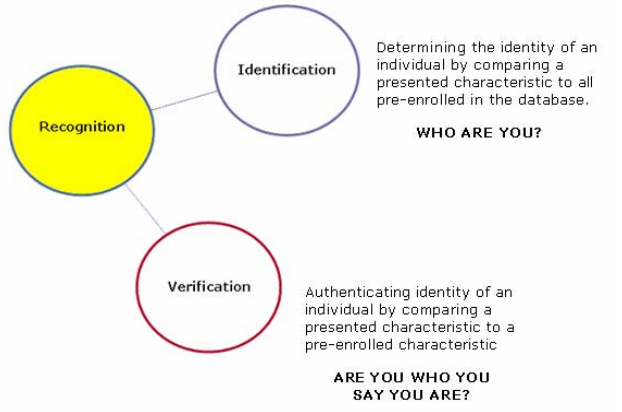

Fig 4 Identity recognition

The key to G2C e-government is authentication i.e., the ability to positively identifying and prove the authenticity of those with whom the government conducts business. Without authentication, other security measures put in place for many G2C transactions can be ineffective.

To clarify this further, governments need varying levels of authentication strength based on the value or sensitivity of their online information or services, balanced against other considerations like usability, deployment, and budget. The discussion in this section is limited to the presentation of authentication levels that organisations may consider in their G2C initiatives and some of the advanced technologies that can make such requirements possible.

It is important to heed that the essence of G2C e-government is that transactions occur between people that are represented by machines. The anonymity of these transactions makes it more difficult to identify the parties involved and to ensure a trusted business relationship. Since all successful business relationships are based on trust, establishing online trust should be one of the primary goals of any e-government initiative. The focus must be building a trust environment that provides a high level of data privacy, data integrity, and user authorisation. The real cornerstone of G2C e-business trust is authentication: that is, knowing with whom the government is doing business with. PKI, smart cards, and biometrics (see Table I) are the technologies that are believed to be the key components of the trust model to address both electronic transactions security and online identity authentication.

TABLE I
PKI, SMART CARDS, BIOMETRICS

(1) Public Key Infrastructure (PKI):	state-of-art in digital authentication & overall security infrastructure
(2) Smart Card:	a plastic card with an IC chip capable of storing & processing data that may also come with optional magnetic strips, bar codes, optical strips etc. viewed as n ideal medium for national ID schemes, e-government & e-commerce applications
Biometrics:	allow to connect individuals to their credentials and therefore enables the verification (authenticate or identify) of people's identity using the unique properties of their physical characteristics

Combining these three technologies can provide the government with a three-factor authentication capability such as depicted in Fig. 5:

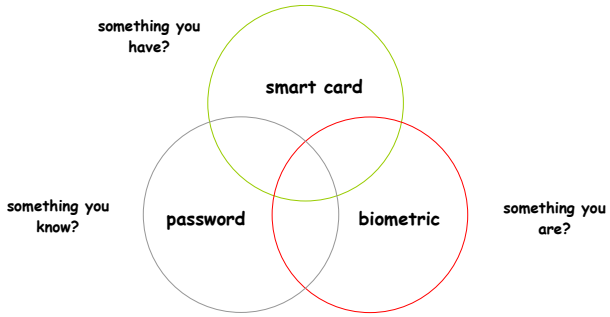

Fig. 5 Three factor authentication

(1) a password to ascertain what one knows,
(2) a token (smartcard) to ascertain what one has/posses, and
(3) biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customers account. This would be difficult, if not totally impossible. By requiring three forms of identification to access credentials, organisations will be able to bind users' digital identities to their physical identities which allows them to be more confident that the users are who they say they are, which should in turn give governments a high level of assurance of online identities. The following three sections will introduce the three main technologies, namely: PKI, biometrics, and smart cards.

A. Public Key Infrastructure

Due to the breadth and depth of the PKI subject, the discussion here is narrowed to address the online identity authentication issue. Several practical studies demonstrated that most of the e-government security requirements can be fulfilled through the public key infrastructure (PKI) security services. PKI is defined as a system of computers, software and data that relies on certain sophisticated cryptographic techniques to secure on-line messages or transactions [10].

The requirements imposing the need for additional security measures are either related to the hardware/ software infrastructure of the e-government platform (e.g. performance, availability, etc.), or to highly specialised-security critical applications (e.g. e-voting; anonymity, un-coercibility, etc.).

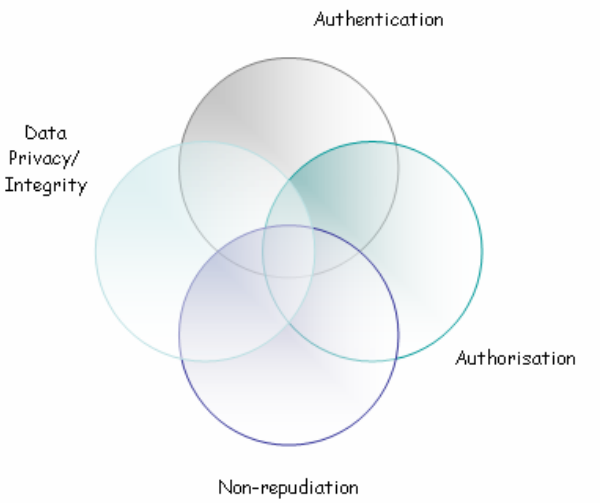

Fig. 6 PKI security framework

In principle, as depicted in Fig. 6, PKI provides four key features to secure online transactions:

- Authentication — to verify the user identity prior to an online exchange, transaction, or allowing access to resources (e.g., digital certificate[2], public key certificate, biometrics, etc.)
- Data privacy/integrity —to ensure the confidentiality of information and that data is not altered as it moves around the public Internet (e.g., encryption[3]).
- Non-repudiation — to prove that an individual has participated in a transaction (e.g., digital signature). Only two-factor authentication definitively binds a user's physical identity to his digital identity.
- Authorisation — to verify that the user has permission to

[2] A digital signature is sometimes referred to as an electronic signature, but is more accurately described as an electronic signature that is authenticated through a system of encryption logarithms and electronic public and private keys. A digital signature is often described as an envelope into which an electronic signature can be inserted. Once the recipient opens the document, the digital signature becomes separated from the document and the document can be modified. Thus, a digital signature only preserves the integrity of a document until it is opened.

[3] Encryption is a security method that transforms information into random streams of bits to create a secret code. There is software-based encryption such as Secure Sockets Layer (SSL) or Public Key Infrastructure (PKI). Hardware-based encryption, such as smart cards, is another type of encryption.

participate in an activity, a transaction, or is allowed access to resources (e.g., cross reference public key certificate with a privilege through the use of policy management servers).

PKI provides a mechanism for binding cryptographic keys, used to encrypt and digitally sign messages, to other credentials such as name, age or place of birth from key certificates and transporting those certificates around the internet electronically. A government agency can for example send messages using citizen's digital certificate encoded with relevant public key that only that specific citizen can open.

B. Biometrics

Biometric technology can be used in identity management systems to identify someone in a population (known as 1:N matching) or to verify someone against his/her own details (known as 1:1 matching). Apart from being non-transferable among individuals, biometrics do not provide data about the person; rather, information of the person.

When biometrics such as fingerprints or iris recognition is deployed in these contexts, for unique identification and for strong authentication, they provide an effective means for binding people to their identities. In the context of a national ID scheme, the biometrics process allows a technique of padlocking the citizen to the card. In doing so, the card cannot easily be transferred to another individual. In particular, given the current focus on the use of biometrics in national identity cards, it sets out architecture for strongly-authenticated identity cards that deliver (perhaps counter-intuitively) both enhanced security and enhanced privacy.

C. Smart Cards

In a smart card secure environment, users are not locked into one form of authentication, such as the ever-vulnerable password. Smart cards provide a mechanism for binding cryptographic keys to individuals, with appropriate authentication, so that when a key is used then the organisation or the individual can be certain of the identity of the person at the other end of the transaction or communication.

Mapping this to the earlier example of the government agency, when a person gets a message, he or she can put their smart card into their PC and punch in their PIN that will in turn lets the smart card use the relevant key to decode the message. Depending on the configuration, if a user loses the smart card, the card can be inoperable without the biometric. Forged fingerprints can be weeded out with the use of the PIN.

Smart cards allow on-card or off-card biometric matching. Off-card matching means that biometric authentication happens online where the biometric features are compared with backend databases. On-card matching technology means that biometric features are compared with a stored template within the card. The template is stored exclusively in the secure smart card environment, which reliably protects sensitive personal data against unauthorised access. On-card matching is an outstanding way of user authentication within security applications that meet the three paramount requirements of security, ease of use, and data privacy.

Using the power of these three technologies, government organisations and businesses alike can use varying levels of authentication depending on the level of security required for a particular transaction (Fig. 7). Citizens with simple readers attached to their PCs (at home, work) or even kiosk machines can logon onto the government internet portal and perform various transactions online in off-card or on-card authentication modes (Fig. 8). The next sections present the research methodology and the findings from a survey conducted to assess the current status of e-government projects in the Middle East.

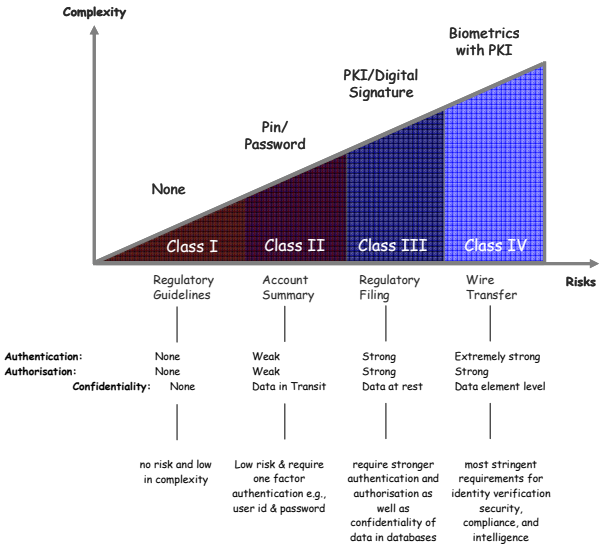

Fig. 7 An example of types of authentication for G2C e-gov services

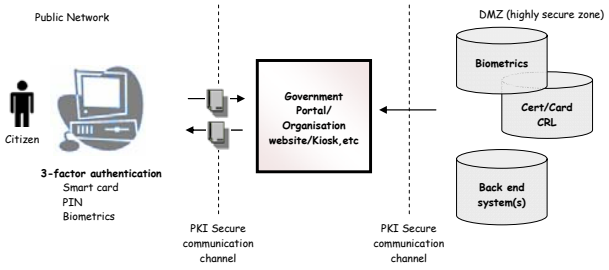

Fig. 8 Conceptual model for electronic authentication

IV. Research Methodology

The data of this study were gathered by two principal methods: personal interviews and a questionnaire survey. A six-page questionnaire was designed, consisting of structured and semi-structured questions, to gather information and understand the surveyed organisations practices in the field of

the e-government.

The questionnaire was first pilot tested through telephone interviews with four senior executives and two managers in two organizations - following the recommendation of [11],[12],[13]. These interviewees provided detailed feedback on the clarity of the questions and overall comprehensibility of the instrument. The result of this pilot study led to some adjustments to the content and format of the questionnaire and terminology used in the survey. The updated questionnaire was then pre-tested on 6 interviewees in four organisations before being administered to all participating organisations (excluding those who took part in the pilot study).

A total number of 198 questionnaires (both in English and Arabic-language versions) were sent to the contacted organisations through the chief information officer or the IT/IS manager, as advised by the sites. The majority of the questionnaires were mailed to respondents with pre-paid envelopes, while the rest were either faxed or e-mailed to respondents. Sixteen questionnaires could not be delivered to the intended recipients and were returned by the postal service.

A total number of 60 questionnaire forms were returned (by postal mail and electronically), giving a response rate of 30.3%. After evaluating the responses, it was found that eight responses were unusable owing to insufficient data. The removal of these unusable responses gave a total of 64 usable questionnaires (that is including 12 responses produced from the first pilot mailing), which represent an overall response rate of 30.5%.[4]

In the sample of 64 participants, 26 government organisations were represented. The characteristics of the respondents are summarised in Table II. The country with the most participants was the United Arab Emirates with a response rate of 38.1%, followed by Bahrain with 32.4%. Table III gives response characteristics for each site.

TABLE II
RESPONSES BY INDUSTRY

Industry (Government)	No.of organisations
Oil/Petroleum	4
Medicine/Health	3
Transportation	4
Telecommunication	3
Finance/Insurance	4
Other	8

A. Telephone Interviews

Respondents to questionnaires were asked if they could be contacted to provide some clarifications and to be asked some additional questions for the purpose of improving the quality of research information. It was also made clear that their right to anonymity would not be affected in either case. Out of the 64 respondents, 21 agreed to be interviewed, 18 of whom were executives and department directors, and 5 senior managers.

The initial draft of the questionnaire served as an interview guide to ensure that all the relevant questions were asked. Semi-structured, telephone interviews (transcribed for subsequent analysis) were administered to 19 individuals[5] in 12 organisations. The semi-structured interviewing approach was developed to ensure that the research questions were properly addressed while allowing for 'probing' questions to gain even greater understanding and insight into the issues. The qualitative data obtained through telephone interviews helped to fine tune the focus of the questionnaire survey and interpret its quantitative results.

Some additional follow-up interviews were also conducted by telephone and e-mail. All the interviewees were very friendly and were willing to share their experiences and ideas. Most of the interviews lasted between 20 and 30 minutes.

B. Measurement of Variables

The questionnaire was divided into two sections to help break the monotony, ease problems of comparison and, most importantly, enable the arrangement of the questions thematically [11].

Part I: This part was designed to be filled by the IT/IS department managers or the responsible department foreseeing the management and implementation of technology related services. The objective of this part of the questionnaire was to gain an understanding of some basic information about the IT infrastructure and technologies utilised to support the electronic strategies.

Part II: This part of the questionnaire was designed for all respondents. The objective of this part was to understand the perceptions of both executives and other senior managers about e-government opportunities, obstacles and future plans as well as their level of awareness.

[4] The results of the pilot and final questionnaires were merged here since the changes made to the initial questionnaire were only to clear out ambiguity and change the arrangement of questions. The additional questions included in the final questionnaire were questions 27 and 28 (See Appendix B: Research Questionnaire).

[5] Out of the twenty-one respondents who agreed to be interviewed, 2 senior managers declined later without any explanation.

TABLE III
SURVEY RESPONSE CHARACTERISTICS BY REGION

Site (Distributed/Returned/ %)	Functional areas of returned surveys (self-reported)		Hierarchical levels of returned surveys (self-reported)	
Bahrain	Corporate Mgmt	3	Executive	6
	IS/IT	3	Senior/mid mgr.	3
(34 / 11 / 32.4 %)	Human Resources	1	Missing Id's	2
	Planning & Development	1		
	Finance	1		
	Missing Id's	2		
	Total	11	Total	11
Kuwait	Corporate Mgmt	2	Executive	3
	IS/IT	2	Senior/mid mgr.	4
(29 / 8 / 27.6 %)	Human Resources	1	Missing Id's	1
	Planning & Development	1		
	Finance	1		
	Missing Id's	1		
	Total	8	Total	8
Oman	Corporate Mgmt	3	Executive	4
	IS/IT	2	Senior/mid mgr.	5
(31 / 9 / 29.0 %)	Human Resources	1		
	Planning & Development	1		
	Finance	1		
	Missing Id's	1		
	Total	9	Total	9
Qatar	Corporate Mgmt	2	Executive	4
	IS/IT	2	Senior/mid mgr.	3
(36 / 9 / 25.0 %)	Human Resources	2	Missing Id's	2
	Planning & Development	1		
	Finance	1		
	Missing Id's	1		
	Total	9	Total	9
Saudi Arabia	Corporate Mgmt	3	Executive	4
	IS/IT	1	Senior/mid mgr.	6
(38 / 11 / 28.9 %)	Human Resources	1	Missing Id's	1
	Planning & Development	3		
	Finance	2		
	Missing Id's	1		
	Total	11	Total	11
United Arab Emirates	Corporate Mgmt	6	Executive	9
	IS/IT	1	Senior/mid mgr.	6
(42 / 16 / 38.1 %)	Human Resources	2	Missing Id's	1
	Planning & Development	3		
	Finance	1		
	Missing Id's	3		
	Total	16	Total	16
(210 / 64 / 30.5 %)	Total	64	Total	64

V. Research Findings

The following table summarises the research findings.

TABLE IV
SUMMARY OF RESEARCH FINDINGS

1. How important do organisations perceive online presence and e-government initiatives?
Out of the 26 surveyed organisations, 20 had internet websites, 4 were planning to develop one, two indicated that they *"have no intention of developing one, "* with the justification that they had no interaction with citizens. Overall, all respondents perceived e-government as a concept that gives them an opportunity to revolutionise their organisations.
2. Major Driver for e-Government projects?
Customer expectations and Internal efficiency/cost reduction were found to be the most common drivers for e-government projects.
3. What plans/strategies do organisations have, to go about e-government projects?
None of the responding organisations indicated to have an e-government strategy but rather a set of guidelines and short term plans. These plans focused on augmenting internal operations, where G2C was left down to the operational departments to implement. In most of the cases, IT departments were tasked to champion such projects.
4. Impact of e-government on organisations operations?
e-government was viewed to enable the government to appear as one unified organisation and provide seamless online services.
5. What is the greatest obstacle to e-government initiatives as viewed by organisations?
Security was found to be a major concern. Ability to verify online identities was the seen to be the biggest obstacle when it came to G2C transactions.
6. Can national ID projects support e-government projects?
Many have viewed national ID projects to be mainly addressing homeland security issues and to replace existing cards such as driving licence, health card, bank cards, etc. However, a common view was that their governments, whether through a national ID or other programmes, must put a solution in place to address the need of online authentication of individuals, to support e-government progress.

1. How important do organisations perceive online presence and e-government initiatives?

The results of the survey revealed that almost 77 percent of government organisations that responded had an internet web site (See Fig. 9). Out of the twenty three percent of the respondents who responded "no" to having a web site, more than 66 percent planned to create a web site by this year or early next year.

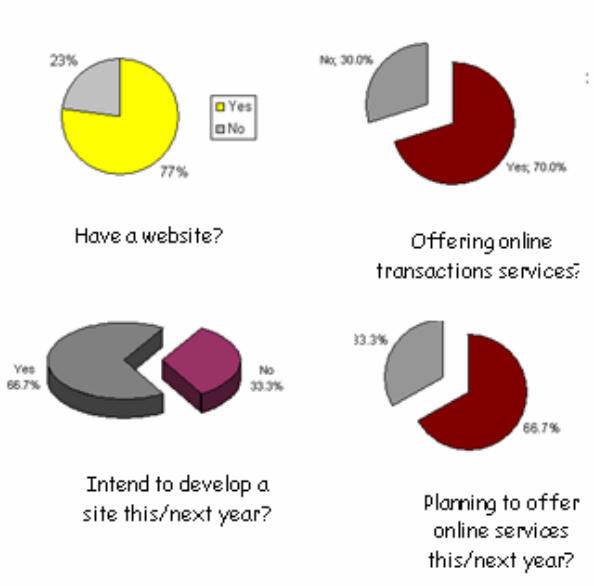

Fig. 9 Online presence

Out of the two organisations that did not have websites, one executive claimed that they did not see the need to have a website because of the nature of the services of their organisations which requires the physical presence of the citizens/customers. The other executive claimed to "have no intention of developing one, because of online security concerns."

On the other hand, around 57 percent of those who responded to have a web presence indicated to have automated online services such as payment of fees, bills and fines (see Fig. 10). Only three (21.4%) organisations indicated to have integrated their systems for limited online functionalities. This supports the findings of previous studies that most of the organisations are still in the cataloguing and transactional phases of Layne and Lee model.

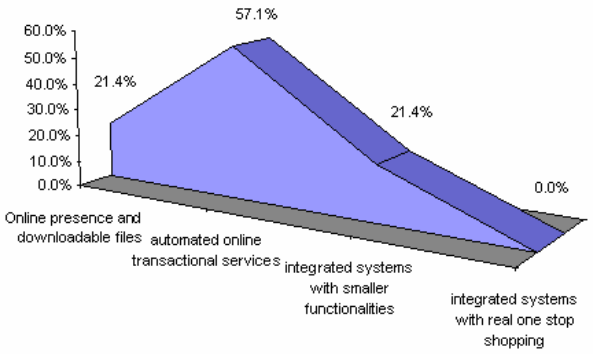

Fig. 10 Organisations own perception of their own electronic operations

2. Major Driver for e-Government Projects?

The majority of the respondents (85.9 percent) indicated that the major driver for e-government projects was the (1) growing expectations of citizens for online services and (2) internal efficiency and cost reduction (see Fig. 11). Though not in the form of policies or legislation, responding organisations also reported that a significant amount of pressure is being applied by the government to better coordinate business process and information flow among ministries and local departments.

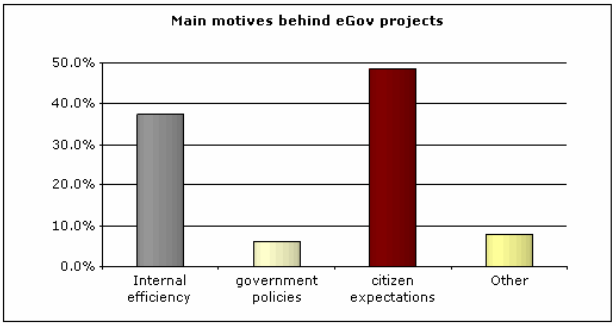

Fig. 11 Main motives behind e-government projects

Many of the interviewed executives said that because of the above two drivers for e-government, their organisations are in the process of planning to integrate stovepipes of automation and support collaborative business processes and streamline business operations. Yet others expressed concerns over the ability to effectively integrate their systems and technically collaborate with other government organisations because of technical and security constraints.

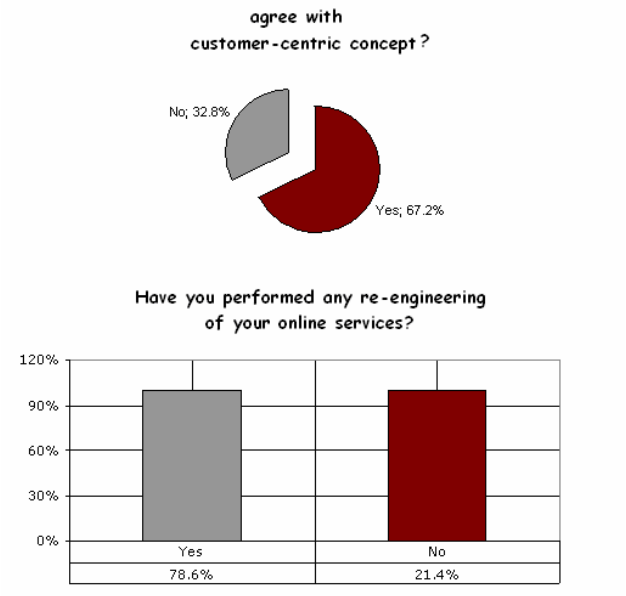

Fig. 12 Re-engineering and customer-centric services

Sixty seven percent of respondents agreed with the statement that "online government services must be customer-centric". The 21 percent of respondents who answered "no" to this statement indicated reasons such as confidentiality of records and current policies to hinder such concepts (see also Fig. 12).

Many of them have also expressed their concerns about their inability to automate many of their services and put them online since identity verification was a prerequisite function, as one IT director explains: *"with the pressure we have from the top management to improve performance and offer online services, we are still struggling to address the online identity verification issue."*

As depicted in Fig. 13, out of those organisations who indicated to have a website, 26.7 percent indicated that they have an IT infrastructure that can support limited online service plans. Not very surprisingly, 73.3 percent responded "no" to having one. With follow up phone calls to people in both categories, they indicated that they have invested in many advanced technologies to secure their services from any misuse, but the authentication of online identities was considered to be the lacking element in all organisations that made their infrastructure incomplete when it came to G2C transactions.

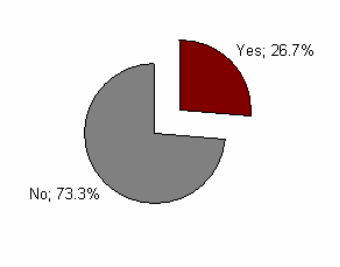

Fig. 13 IT infrastructure readiness

3. What plans/strategies do organisations have, to go about e-government projects?

Only 26.9 percent of respondents indicated that they have an e-government plan but not a strategy and that 61.9 percent of them tasked information technology departments to create such plans and carry out the implementation (see also Figure 14). Two of the organisations indicated to have no clear vision or plan regarding their e-government, and said that they are in the process of appointing a consulting company to develop an e-government roadmap for their organisations.

During the course of interviews with the executive management it was found that almost all organisations had a draft blueprint for going about e-government programs. However, they claimed that those strategies do not address the one-stop-shopping concept, and it focuses more on internal organisational efficiency. Overall, many of the current e-government plans and strategies were believed not to address the G2C aspect, and are left to the ministries and other government departments to address.

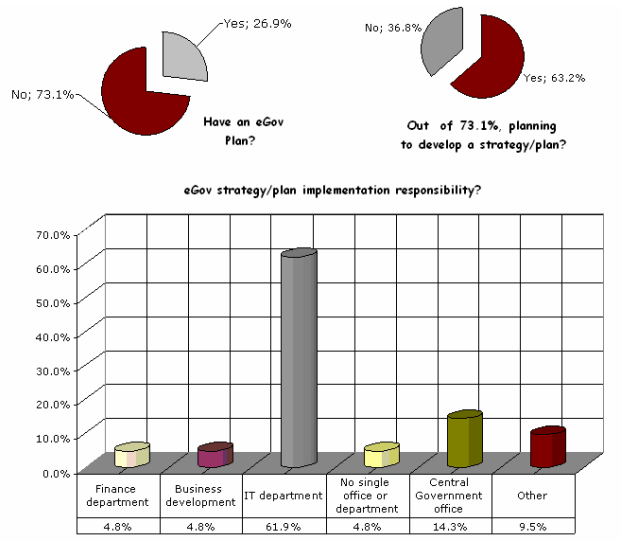

Fig. 14 e-government strategy

Some organisations indicated that the information technology departments have better understanding of what e-government involves, as one explains: "the IT department knows more about these technological projects. We tasked them to coordinate with other departments to create e-government plans. In this way, the other departments can focus on their core business." (Translated from an interview) This was a common and shared view among many of the interviewed executives.

This is also cited in literature as one of the key reasons that system projects fail. Information technology people tend not to know much about the business goals and strategy. Hence organisations get IT systems that are not aligned with the business strategy; a most common cause for project failure.

4. Impact of e-Gov on organisation's operations?

More than 30 percent of organisations indicated that e-government projects have increased the demand on forward thinking management and technical staff. It was also cited that such demand and skill shortages in different management and technical fields put upward pressure on wages. Follow up pone calls were made to get some clarification from those who reported a reduction in the number of staff as a result of e-government programmes. The feedback received was that some of the re-engineering activities automated many of the internal processes reducing the size of the work forces. However, they also indicated that e-government projects have placed greater emphasis and demands on the need for solid project management and business process analysis skills, as well as the technical staff who can manage and administer complex technical systems.

It was also indicated during the interviews that many of the e-government projects caused a sharp rise in the use of outside contractors and consulting companies due to the complexity of the projects and to meet pressing deadlines. There was also this common view among many of the participants that e-government can improve the traditional service channel strategies, which enables governments to appear as one unified organisation and provide seamless online services. The following factors were also among the cited impacts of e-government as captured during the course of the interviews (see also Fig. 15):

- improving business productivity (simplification of processes)
- efficiency and improvements in processing internal activities as well as public administration operations
- reducing expenditures through savings on data collection and transmission
- sharing of data within and between governments
- promoting information society
- public management modernisation and reform
- enabling citizen engagement
- promoting open and accountable government
- prevent corruption as it promotes more transparency

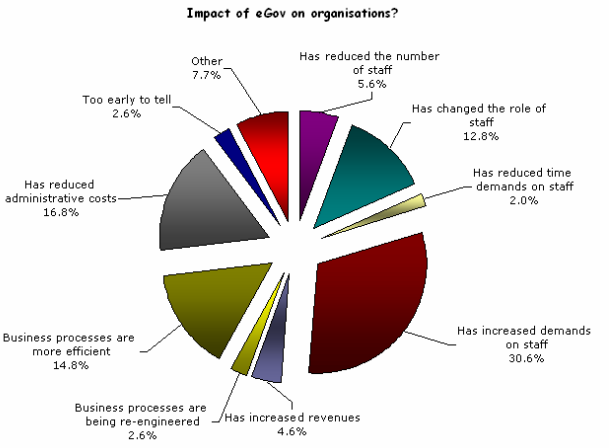

Fig. 15 e-government impact on organisations

5. What is the greatest obstacle to e-government initiatives as viewed by organisations?

Quite surprisingly, not one organisation indicated public concerns over their privacy to be an obstacle to e-government projects. Perhaps, this may be due to the culture and demographic nature of the studied countries. However, most organisations indicated to be using secure socket layer (SSL[6]) capabilities to ensure the privacy of information especially for financial transactions and the transmittal of sensitive information.

[6] with SSL, data is encrypted, or scrambled, prior to sending it and then decrypting it on the receiving end. By encrypting the data as it travels the Internet, it is virtually impossible for the transaction to be translated if intercepted.

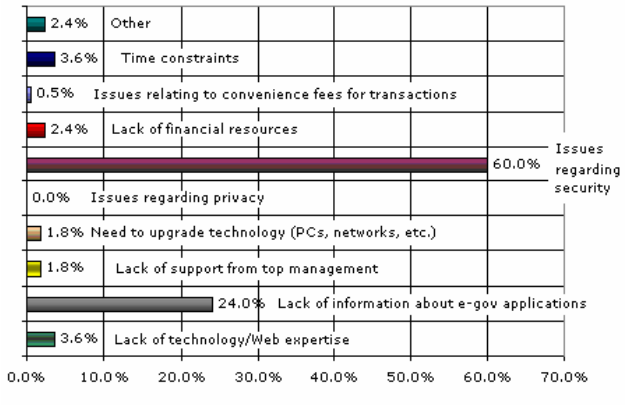

Fig. 16 e-government obstacles

As depicted in Fig. 16, the majority of respondents (60%) considered security issues to be the primary obstacle to their e-government projects, whereas 24 percent indicated lack of strategic direction and information about e-government applications to be the second most concerning and challenging issue. It was obvious that security was a common concern among the interviewed executive management in all surveyed organisations. Although organisations indicated to be using many security technologies, online identity verification was stated as the biggest concern that led to slow down their "e-services plans" where identity assurance was required. This finding is consistent with the findings of Javelin Strategy & Research's 2005 Identity Fraud Survey Report published in 2005[7]. Other organisations have indicated that although some services require authentication of their identities, and because of the pressure of the top management, they are offering those services online, but using intermediaries such as postal or courier services to authenticate peoples' identities before delivering government documents/products to them.

As a part of the study, the online identity problem was further investigated. The interviews showed that many of the surveyed organisations faced transactions where people presented false credentials or those belonging to others to take advantage of some of the services the government provides. Three organisations have indicated that they have pulled back some of the online services they provided on the Internet after discovering that some people provided false credentials to gain access to sensitive information and benefit from some of the government online services. This area was noted as a common concern at some sites, as one executive said:

"Though we have invested a great deal in information technology and communication security, we are being challenged with attempts from some people trying to play around and take illegal advantage of the services we offer on the Internet."

[7] Javelin Strategy & Research's 2005 Identity Fraud Survey Report. Published in January 2005, this report was co-released by Javelin Strategy & Research and the Better Business Bureau, and served as an update to the Federal Trade Commission's (FTC) 2003 Identity Theft Survey Report.

Another Interviewee said:

"we definitely need an identity management solution that guarantees to us the identity of those interacting with us online. Putting legislation in place that criminalises identity theft activities could be one part of the solution. But bear in mind that all those who perform such activities know that they are breaking the law. We need a mechanism to authenticate those people online."

More than 50% of the respondents indicated to be utilising personal details or passwords to authenticate online individuals (see also Fig. 17). None of the respondents indicated to be using PKI or biometric technologies for their online services. However, many of the IT department executives indicated that they are currently studying the possibility of introducing PKI and smart card technologies to address this growing area of concern.

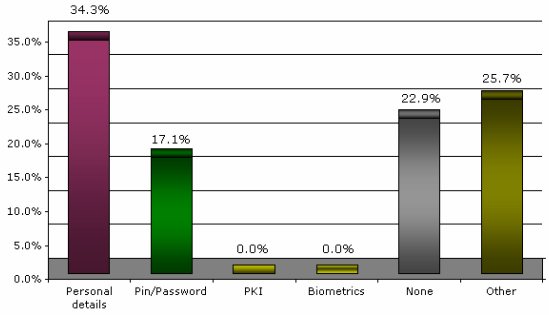

Fig. 17 Utilised technologies for virtual identity authentication

6. How can national ID projects support e-Gov projects?

Though with some variations in the confidence level, more than 55 percent of respondents seemed to have confidence in biometrics to address the need for online verification. Around 38 percent had some doubts about its suitability for online usage, whereas less than 7 percent indicated to have no confidence at all (see also Fig. 18).

It was also found that during the interviews that some organisations were using smart cards and biometrics for authentication applications both for internal access control purposes, as well as for some public services such as airports[8].

[8] In Dubai International Airport in the UAE, the electronic gate (e-Gate) project was launched in 2002 to allow frequent flyers fast access through immigration via electronically controlled gates. This fully automated passport control system replaces manual checks with proximity smart card and fingerprint technology to identify and clear registered passengers. It is also the intention of the government to use the new national ID card, and the (thumb prints) stored in the chip of the smart card for auto immigration clearance without the need for registering for e-gate service anymore.

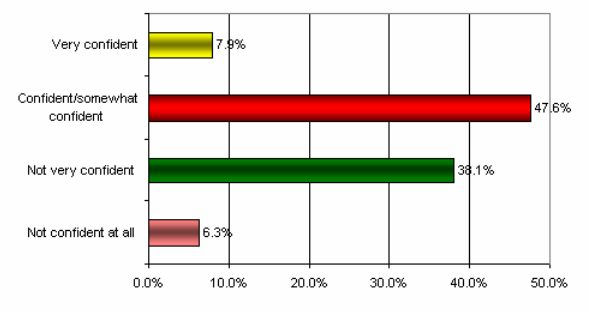

Fig. 18 Level of confidence in biometrics

As depicted in Fig. 19, more than sixty-four percent of respondents viewed national ID projects to more likely address homeland security than (online) identification of people. Only 29.7 percent indicated that they think national ID projects will support e-government projects, and 51.6 percent indicated their lack of knowledge in this regard.

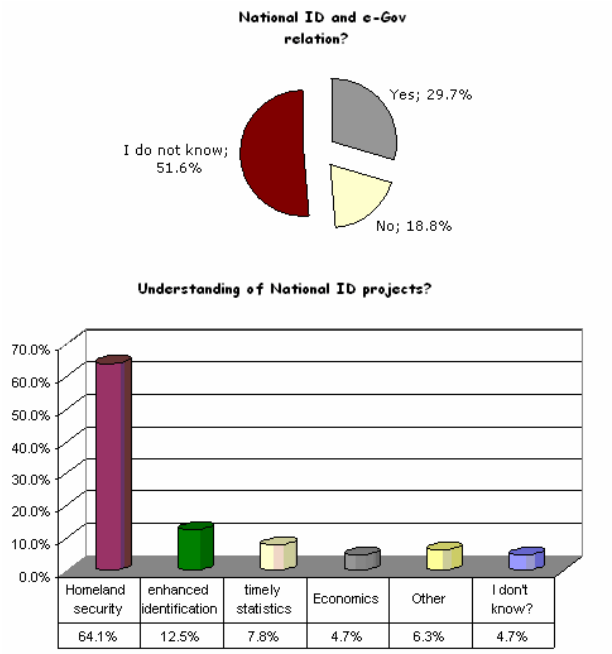

Fig. 19 Awareness of the relationship between national ID projects and e-government

Many of the interviewed executives believed that their governments need to put in place appropriate mechanisms to identify people online, as one executive explains:

"I agree with the fact that the government has the responsibility to provide its population with identification means that proofs their identities and who they are. Today, there is pressure from the top to automate our operations and put the 'e' in our services. Whether through a national ID or other programmes, the government should provide the people with an 'e' identity that we can use to authenticate them online" (translated from the interview).

A common view among the interviewees was also that the new smart ID card will allow the citizens and residents to authenticate themselves in an easy and completely secure electronic way whenever they access e-government applications. Another claimed advantage of the new card was that it will allow individuals to put their own electronic signature to digital documents such as declarations or application forms, which will have the same value and legal status as the documents that are nowadays signed by hand.

VI. Discussion & Conclusion

The findings of this study are seen to be critical and have several implications for practitioners specially if attempting to understand some practices related to G2C e-government in the GCC countries. Overall, the findings in general suggest that organisations need to have a more global view of what e-government is all about as many organisations tasked their IT departments to champion e-government projects. E-government was seen more of an automation activity.

This study shows that G2C e-government initiatives in the surveyed countries, is progressing but in a slow motion because of the lack of a trusted and secure medium to authenticate the identities of online users. In the surveyed organisations, many managers stated that the lack of a reliable authentication medium is preventing them from enabling many of their services to online state. Consistent with the literature, the analysis of questionnaire responses and data collected from interviews with managers revealed that, passwords remains one of the most popular approaches used currently to address online authentication requirements.

With little variations in the perceptions of their impact, many of the obstacles to e-government presented earlier were highlighted by management in the surveyed organisations as so. Security and overall system integration were by far the most widely quoted obstacles. Many of the interviewed management indicated to have computerised almost all their administrative functions, and in many cases their core business and support functions as well.

Many organisations indicated that they had formed review committees to review their corporate plans and facilitate communication between departments and to oversee the overall programme implementation. However, they appeared to have no structured approach to e-government strategy formulation and development. Though each organisation had constituted a body in the form of committee or department to carryout the 'e-readiness' assessment and thereafter draft a strategic plan for the implementation of e-government, it seemed according to the interviewed executives to focus merely around G2G operations. The G2C was left to the individual ministries and departments to implement.

A. The smart ID card & e-Government

As viewed by many of the survey respondents and interviewees, governments must take the responsibility of putting in place a reliable identity management infrastructure. With the rapid evolvement of technologies, governments need

to introduce new and stronger means of identification and authentication for its population. Traditional paper and conventional ID cards do not cope with the nature of e-government environment which requires advanced technologies to authenticate virtual identities over the web. Electronic authentication must be viewed as a fundamental part of the security infrastructure needed for the safe delivery of online government services that gives both the user and the service provider the confidence in the identity of the other party in a transaction.

It is argued by the authors that initiatives such as national ID card schemes can very well address this requirement and can bring answers to many of the security concerns. The UAE national ID programme is a good example, as it aims to build a robust and secure national identity infrastructure. The roll-out of this new national identity card in the UAE will mark a major milestone in the development of e-government due to the nature of technologies it utilises e.g., biometrics, smart cards and public key infrastructure. The use of these technologies is seen to provide a more secure and reliable G2C electronic authentication services.

Indeed, such schemes would pave the way for greater penetration and usage of government services and reap the promising benefits of e-government. It cannot be re-emphasised much more that for governments to fulfil their critical functions, they must be able to authenticate their citizens' claims about their own identities and characteristics [14]. As digital government becomes a reality, the need for reliable digital identifiers becomes increasingly urgent (ibid.).

B. Further Research

This study was aimed only at organisations in the GCC countries. However, additional work must be carried out if a better understanding of worldwide e-government programmes is to be established. Some areas in which further research may yield valuable insights for more comprehensive understanding and assist management in determining optimal courses of action are:

(1) a follow-up study in the same countries with a larger sample of organisations to gain insight into their perspectives and practices in the field of e-government development and implementation and to test the findings of this study,

(2) a similar study should be conducted in other countries that could show the findings reported here are indeed generalisable and might increase the robustness of the findings,

(3) a study to shed light on the different views on power and control in organisations in relation to e-government adoption from both theoretical and empirical perspectives,

(4) a field research for testing the impact of each identified obstacle to e-government programmes. This, in turn, should give a greater understanding of those obstacles and pave the way to put forward appropriate and/or develop frameworks that can overcome such obstacles.

(5) understanding of the suitability of the national ID card with further detail as an authentication medium of online users.

As explained earlier, the authors intend to carry out a short practical study on the use of national ID card (item 5 above) as a medium for online identity verification, in a separate study.

ACKNOWLEDGMENT

The authors would like to thank those who participated in the survey. They also would like to extend their gratitude the reviewers who provided feedback that improved the overall structure and quality of this paper.

APPENDIX: RESEARCH QUESTIONNAIRE

Purpose

The purpose of this questionnaire is to investigate issues related to field of e-Government and its practices in GCC countries as part of a research project. This form is also available on the Internet for electronic submission. The web site can be found at: http://www.alkhouri.itgo.com/research/questionnaire.html. If you have any queries about this questionnaire or need additional information, please contact the researcher through the following e-mail address: alkhouri@itgo.com.

Date: _____

Name: _____

Position: _____

Organisation: _____

Telephone: _____

e.g., you may not provide your telephone number if you prefer and/or any of the other information.

All information will remain strictly CONFIDENTIAL

Part A: This section is to be completed by IS/IT managers.

1. *Does your organisation have an Internet website?*

Yes / No *(Delete as appropriate).*

If "*No*", then do you intend to develop a website by this year or early next year? otherwise, go to question 2.

Yes / No *(Delete as appropriate).*

2. *Are you offering any online transactional services?*

Yes / No *(Delete as appropriate).*

If "*No*", are you planning to offer any online service(s) by next year? otherwise, go to question 3.

Yes / No *(Delete as appropriate).*

3. *Have your organisation performed any re-engineering of the manual processes/services before offering it/them online?*

Yes / No *(Delete as appropriate).*

4. *How do you perceive your organisation on-line services in the following categories?*

a. Online presence and downloadable files	[ ]	*(Please tick as appropriate).*
b. automated online transactional services	[ ]	
c. integrated systems with smaller functionalities	[ ]	
d. integrated systems with real one stop shopping	[ ]	

Other _____

(Please specify) _____

5. *What security methods do you use to secure online transactions?*

a. Personal details	[ ]	*(Please tick as appropriate).*
b. Pin/Password	[ ]	
c. PKI	[ ]	
d. Biometrics	[ ]	
e. None	[ ]	

Other _____

(Please specify) _____

6. *Does your organisation have an IT infrastructure that supports you online services plans?*

Yes / No *(Delete as appropriate).*

If "*No*", then please clarify, otherwise go to question 7.

_____

Part B: This section is to be completed by all.

E-government is the delivery of services and information, residents, 24 hours a day, seven days a week.

6. *From your current work position, what do you think are the main motives behind e-government initiatives in your organisation?*

a. Legislative requirements	[ ]	*(Please tick as appropriate).*
b. technology advancements	[ ]	
c. efficiency	[ ]	
e. cost effectiveness	[ ]	
f. services to citizens	[ ]	
g. constituent/(citizen) demand	[ ]	
h. Don't know	[ ]	

Other _____

(Please specify) _____

7. ***Do you agree that government services must be customer-centric?***

Yes / No

please specify why?

_____

8. *Does your organisation have an overall e-government strategy and/or master plan to guide its future e-government initiatives?*

Yes / No *(Delete as appropriate).*

If 'no,' are you planning to develop a strategy/plan in the next year? otherwise, go to question 9.

Yes / No *(Delete as appropriate).*

9. *Who has overall responsibility for implementing this strategy or plan or currently looking after eGov initiatives? (Check only one)*

a. Finance department	[ ]	*(Please tick as appropriate).*
b. Business development	[ ]	
c. IT/IS department	[ ]	
e. No single office or department	[ ]	
f. Central Government office (specific Ministry or government department)	[ ]	

Other _____

(Please specify) _____

10. *How has e-government changed your local government? (Check all applicable)*

a. Has reduced the number of staff	[ ]	*(Please tick as appropriate).*
b. Has changed the role of staff	[ ]	
c. Has reduced time demands on staff	[ ]	
e. Has increased demands on staff	[ ]	
f. Has increased revenues	[ ]	
g. Business processes are being re-engineered	[ ]	
h. Business processes are more efficient	[ ]	
i Has reduced administrative costs	[ ]	
j. Too early to tell	[ ]	

Other _____

(Please specify) _____

11. *Please give an indication of your level of satisfaction with the services provided by your own orgnaisation?*

(Check only one, on a scale of 1 - very unsatisfied – to 5 - very satisfied)

Very unsatisfied 1 2 3 4 5 very satisfied

12. ***Which if any of the following barriers/obstacles to e-government***

initiatives has your local government encountered? (Check all applicable.) rate 1 to 7

a. Lack of technology/Web expertise	[ ]	*(Please rate as appropriate).*
b. Lack of information about e-gov applications	[ ]	
c. Lack of support from top management	[ ]	
e. Need to upgrade technology (PCs, networks, etc.)	[ ]	
f. Issues regarding privacy	[ ]	
g. Issues regarding security	[ ]	
h. Lack of financial resources	[ ]	
i. Issues relating to convenience fees for transactions	[ ]	
j. Time constraints	[ ]	

Other _____

(Please specify) _____

13. *In your opinion, what is the purpose of national ID projects?*

a. Homeland security	[ ]	*(Please tick as appropriate)*
b. enhanced identification environment	[ ]	
c. timely statistics	[ ]	
e. Economics	[ ]	
f. I don't know	[ ]	

Other _____

(Please specify) _____

14. *If a biometric were used in these situations, how confident would you be that this technique would guarantee the identity of online users?*

a. Not confident at all	[ ]	*(Please tick as appropriate)*
b. Not very confident	[ ]	
c. Somewhat confident	[ ]	
e. Very confident	[ ]	

Other _____

(Please specify) _____

15. *Do you think that if appropriate technologies such as PKI and biometrics were utilised, the national ID project will support your eGov initiatives by means of providing a safe and secure verification environment?*

a. Yes	[ ]	*(Please tick as appropriate)*
b. No	[ ]	
c. I don't know	[ ]	

16. *What would be the purposes of a national identity card?*

a. To prevent identity theft?	[ ]	*(Please tick as appropriate)*
b. For voting purposes?	[ ]	
c. To combat terrorism?	[ ]	
e. To facilitate international travel?	[ ]	
f. To replace many documents with a single card?	[ ]	
g. To access government services?	[ ]	
h. To combat illegal immigration?	[ ]	

Other _____

(Please specify) _____

17. *If you have any additional comments, which you feel would be helpful to this study, in particular, any difficulties, important factors or considerations which have not been mentioned, please state them here.*

_____

_____

18. *If you have any additional comments, which you feel would be helpful to this study, in particular, any difficulties, important factors or considerations which have not been mentioned, please state them here.*

If your answer is *Yes*, please make sure that you have included your telephone number at the front sheet.

We are very much grateful indeed for your help. Please return the completed questionnaire in the stamped addressed envelope provided to:

Ali M. Al Khouri
P. O. Box: 27126, Abu Dhabi, United Arab Emirates

Thank you once again for completing this questionnaire.

REFERENCES

[1] A. Chadwick and C. May, "Interactions between states and citizens in the age of the internet: e-government in the United States, Britain and the European Union." Governance: an International Journal of Policy, Administration and Institutions, vol. 16, no. 2, 271-300, 2003.
[2] S. Graham and A. Aurigi, "Virtual Cities, Social Polarisation, and the Crisis in Urban Public Space." Journal of Urban Technology, vol. 4, no. 1, 19-52, 1997.
[3] K. Layne, and J.W. Lee, "Developing Fully Functional E-Government: A Four Stage Model," Government Information Quarterly, vol. 2, 122-36, 2001.
[4] P. J. Windley (2002) "eGovernment Maturity" [Online]. USA: Windleys' Technolometria, Available: http://www.windley.com/docs/eGove-rnment%20Maturity.pdf.
[5] P.R. Devadoss, S.L. Pan & J.C. Huang, "'Structurational analysis of e-government initiatives: a case study of SCO," Decision Support Systems, vol. 34, 253-269, 2002.
[6] A. Leigh & R.D. Atkinson, Breaking Down Bureaucratic Barriers: The next phase of digital government. USA: Progressive Policy Institute, 2001.
[7] P. Windley, Digital Identity. USA: O'Reilly Media, Inc, 2005.
[8] Digital ID World (2004) 'What is Digital Identity?' [Online]. Digital World. Available from: http://www.digitalidworld.com/local.php?op=vi-ew&file=aboutdid_detail.
[9] A.M. Al-Khouri, "UAE National ID Programme Case Study," International Journal Of Social Sciences, vol. 1, no. 2, pp.62-69, 2007.
[10] C. Lambrinoudakis, S. Gritzalis, F. Dridi, & G., Pernul, "Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy'," Computer Communications, vol. 26, 1873-1883, 2003.

[11] G. Hoinville and R. Jowell, Survey Research Practice. London: Heinemann Educational Books, 1978.
[12] A.N. Oppenheim, Questionnaire Design, Interviewing and Attitude Measurement. London: Pinter, 1992.
[13] M. Shipman 'Information through asking questions', in The Limitations of Social Research (third edition). London: Longman. pp. 78-115, 1988.
[14] L.J. Camp (2003) 'Identity in Digital Government - A research report of the digital government civic scenario workshop' [Online]. Cambridge, USA, Kennedy School of Government. Available: http://www.lj-ean.com/files/identity.pdf.

A.M. Al-Khouri is currently holding the position of the Assistant Director-General for Central Operations; a sector that consist of IT department, card production, research and development, and many other units. He also chairs the technical committee overseeing the national ID card programme in the UAE. He received his Bachelor's and Master's degrees in Business IT Management with honors and distinction from Manchester and Lancaster Universities in the UK, and currently doing his doctorate degree in the field of engineering management and advanced technologies.

He has been involved in the UAE national ID card project since early 2003 as a member of the technical executive steering committee, and was later appointed as the Director for the department of Information Technology and Systems when Emirates ID was established. He started his career as an IT project manager and then the head of the development division in the Ministry of Interior during which he managed several important IT projects and was involved in many strategic government development projects. His research interests are in leadership & management, e-government and the applications of advanced technologies in large contexts.

Dr. Jay Bal is an Associate Professor, University of Warwick, UK. He joined the Rover Advanced Technology Centre at the University as "IT and Organisational Strategy" Program Manager in 1986 as a founder staff and set up a program of research and consultancy for the Centre. Concurrently he helped to develop Rover IT strategy and managed a number of key IT projects. Since joining the University Dr. Bal has devised and taught courses in Information Technology, Artificial Intelligence and on Design and Manufacturing systems in the Electronics Industry to senior managers in Hong Kong, Malaysia, India, China and South Africa as well as the UK. In the last five years he has published over 10 papers in International Journals, and spoken at many international conferences on aspects of EBusiness. The papers are based on his work on Virtual Teaming, eBusiness and Process Analysis. The work that he did with the government of Tuvoli was awarded the Sunday Times Internet Innovation of the year in 2000. He has consulted for several governments on E-Commerce to promote SME's. This work can be seen in the novel emarketplace and business environment built by his team at www.wmccm.co.uk.