European Journal of ePractice

A publication of epractice.eu

PKI in Government Digital Identity Management Systems

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

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

This article discusses the need for trust establishment to advance eGovernment in light of the existing and emerging realities. It looks at the evolving forms of identities, namely digital identities and the role of PKI technology in enabling such requirements.

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

Dr. Ali M. Al-Khouri

Director General,
Emirates Identity
Authority, UAE

Keywords

eGovernment, eService, PKI, identity management, ID card.

> “PKI technology, while becoming a critical infrastructure component in modern identity management systems and supporting the progress and evolution of eGovernment, also raises the need to share learning experiences from practitioners with the aim to understand associated challenges and critical success factors that should in turn contributing towards successful implementations.”

1. Introduction

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

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

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

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

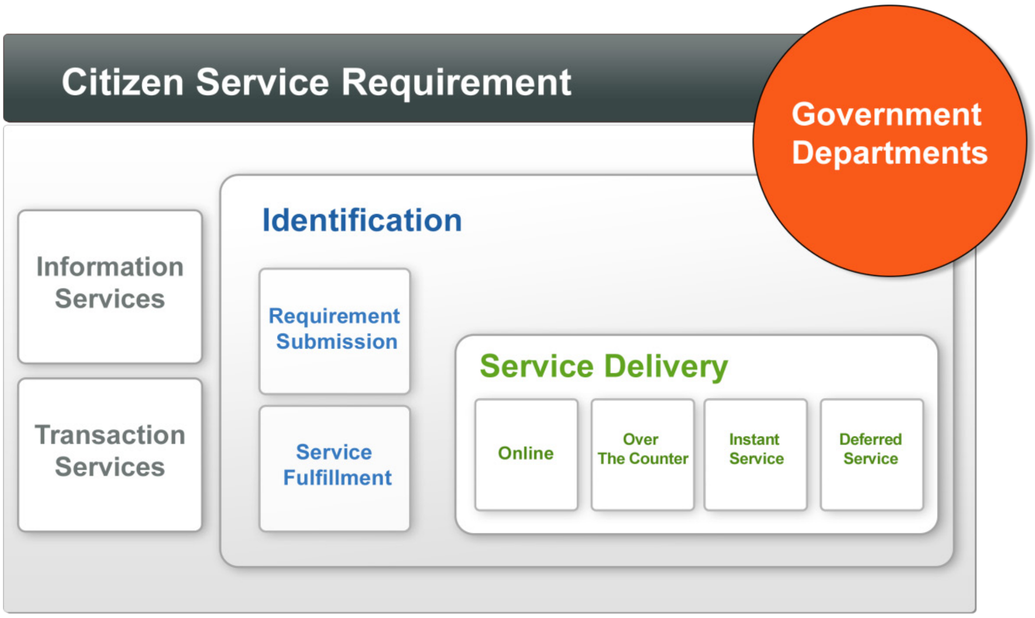


Figure 1: Citizens Interactions with Government Services

The key enabling factor between the service requested by the citizen and the fulfilment of the service itself is the Identity Establishment of the service applicant and the service recipient. Governments have put for a long time considerable effort and struggle, to some extent, in providing and ensuring effective and secure identification systems to their citizens. Different Government departments devised their own identity mechanisms in receiving service requests and service deliveries.

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

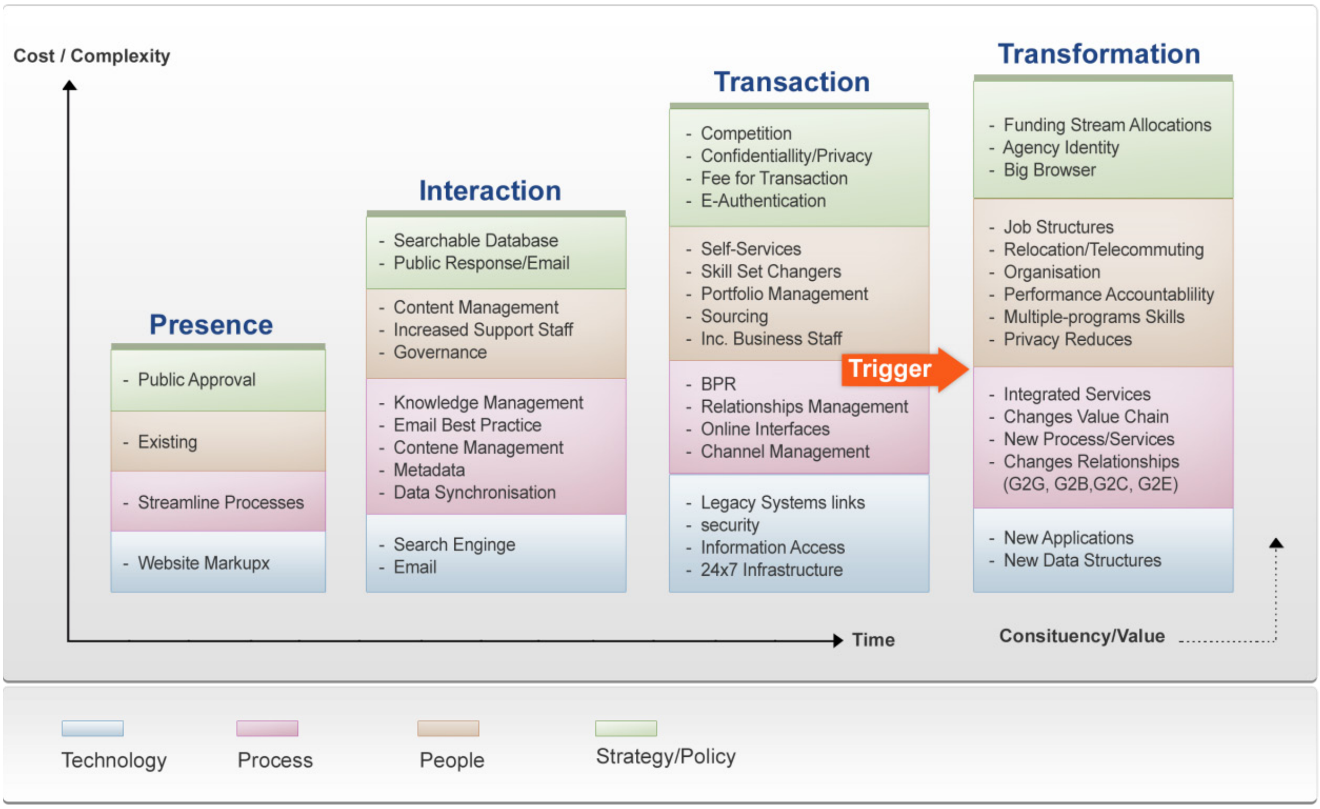


Figure 2: Four Phases of eGovernment – (Baum & Maio, 2000)

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

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

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

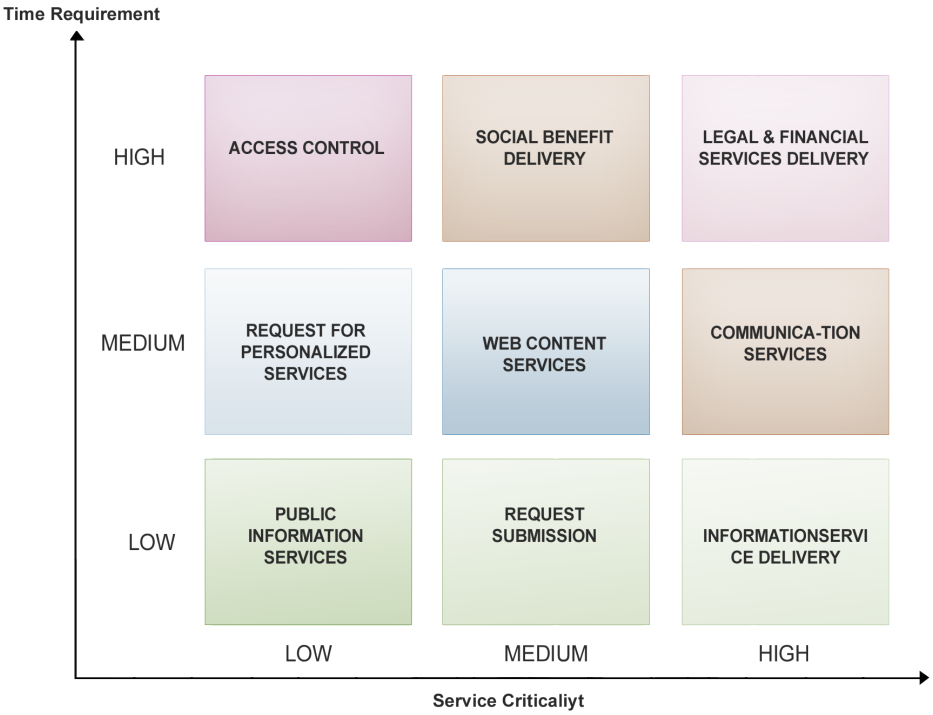
2. Trust Establishment by Identity

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

Table 1: Trust establishment and validation methods

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

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



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

Figure 3: Trust matrix

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

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

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

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

3. Digital Identities

For any Government transaction, citizens need a ‘recognised’ ID. This recognition is well accorded when it is issued by the Government itself. Government issued IDs are no new phenomenon. However, paper based IDs that were long issued (like passports, social security IDs, etc.) are no longer adequate.

Governments, in the last ten years have re-engineered their citizen identity systems to meet the challenges and needs of the eWorld and its new economy (Broster, 2011; Stavrou, 2005). In fact, the last few years have witnessed the evolution of the digital identities or so called eIdentities by various Governments across the world (Griffin, et al., 2007; Seifert, 2003).

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

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

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

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

4. Public Key Infrastructure (PKI)

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

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

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

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

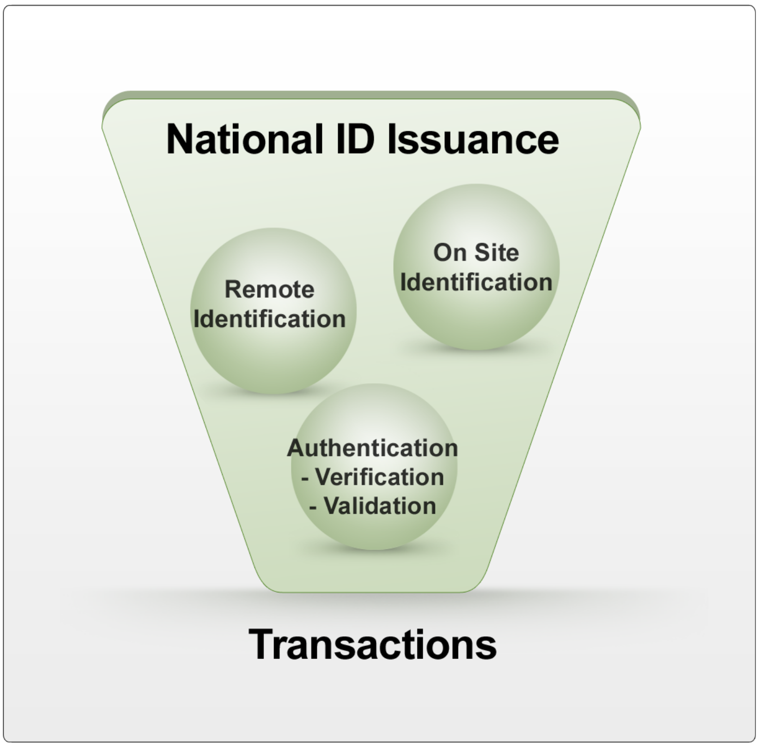


Figure 4: Citizen Service Model 2.3 Increasing social demand

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

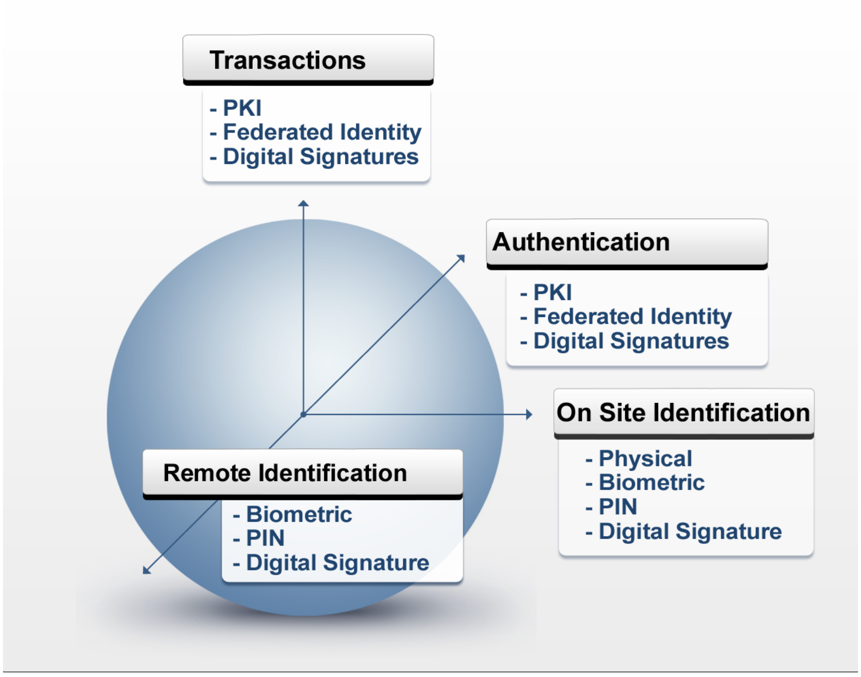


Figure 5: Identity Requirements

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

5. eGovernment and Identity Management Initiatives around the World

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

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

The Middle East has taken a cautious approach and it seems to seek to learn from existing implementations to avoid the pitfalls of early adopters and adopt successfully tested technologies in field of identity management. The 2010 United Nations eGovernment Survey (UN, 2010) and the 2010 Global Information Technology Report (Dutta, S. and Mia, 2011) amply validate this statement.

The United States, UK and most of European countries have implemented biometric identification systems to identify visitors and transform border control mechanisms. South Korea, on the other hand, has issued smart card based national IDs to all its citizens and residents and enabled eID-based transactions, with identity validated and verified by the Government. UAE, Oman, Bahrain, Qatar, and many other countries in the Middle East have also launched multiple large scale biometric-based identity programs providing secure and modern identity documents to their citizens and residents.

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

6. UAE Identity Management Infrastructure

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

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

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

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

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

The UAE card has many capabilities. Firstly it is related to the ePurse functionality, planned for 2013, which will enable service providers to offer micro payments for all cardholders with their identities validated, verified and authenticated by the national Government validation gateway. Another capability is related to signing documents and notarisation. Of specific interest would be the digital signature capability of the UAE national ID card. For example, electronic documents can be digitally signed using the certificates provided in the national ID card. These signatures can be represented on physical prints of the documents as QR codes that carry the digital signature. Thus digital signatures can be physically available on paper documents which can also be verified. A smart phone can read the QR[1] code on a digitally signed paper document and refer it to the OCSP[2] or the CRL[3] for verification. Verification of the signature can then be carried out in real time.

7. The UAE PKI Program

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

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

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

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

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

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

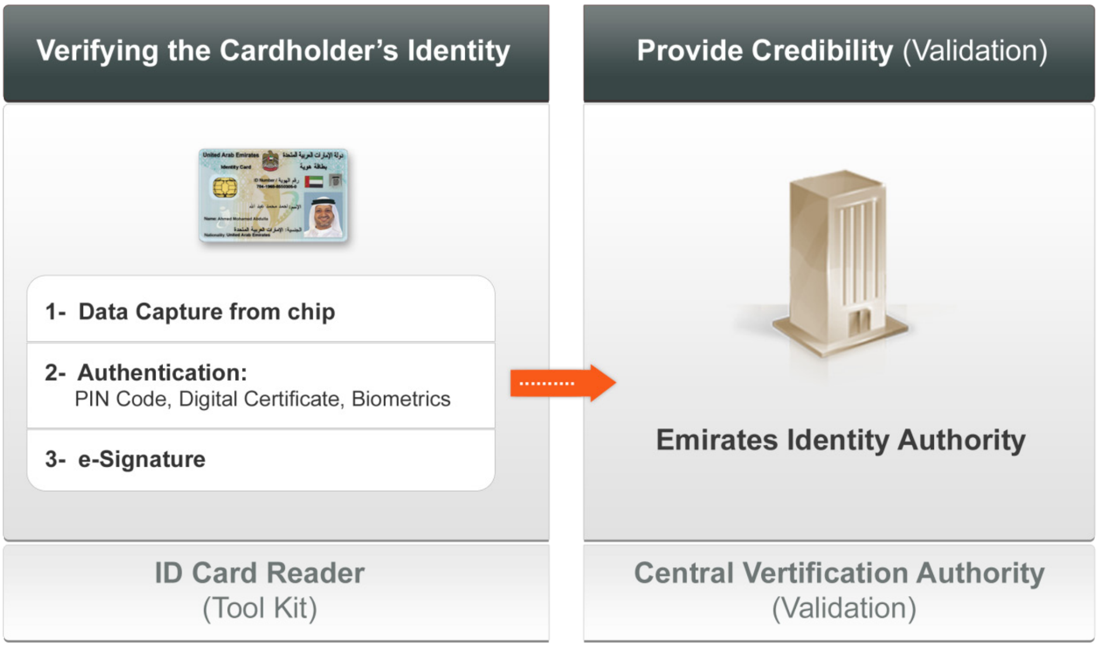

Verifying the Cardholder's Identity
Provide Credibility (Validation)
1- Data Capture from chip
2- Authentication:
PIN Code, Digital Certificate, Biometrics
3- e-Signature
Emirates Identity Authority
ID Card Reader
(Tool Kit)
Central Vertification Authority
(Validation)

Figure 6: UAE PKI project primary objectives

7.1 Central Certification Authority

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

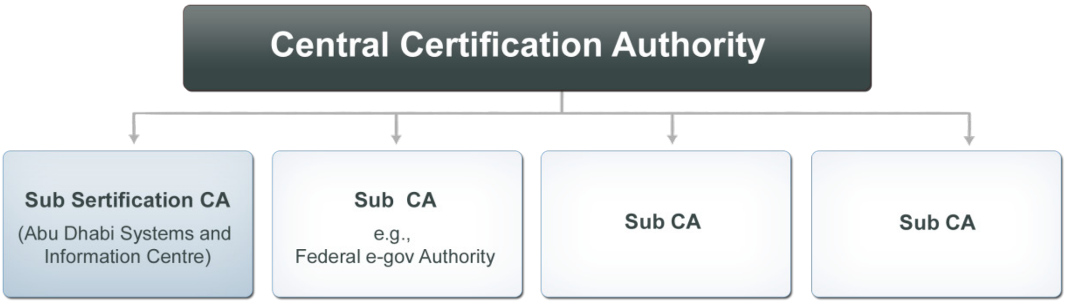

Central Certification Authority
Sub Sertification CA
(Abu Dhabi Systems and Information Centre)
Sub CA
e.g.,
Federal e-gov Authority
Sub CA
Sub CA

Figure 7: UAE PKI Architecture

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

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

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

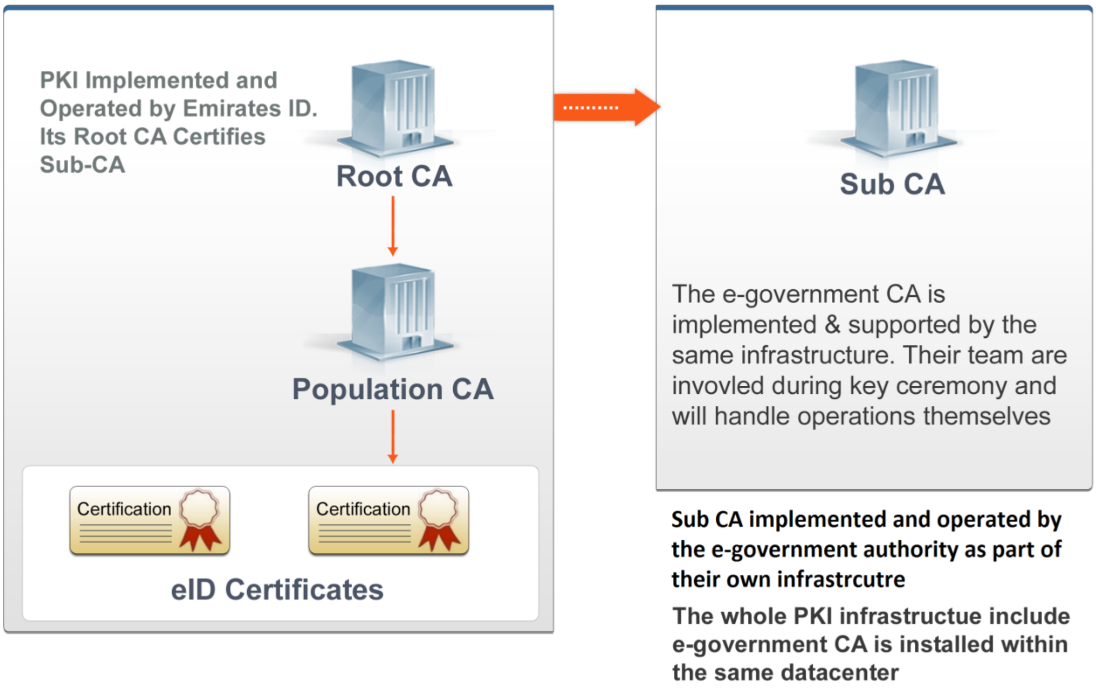

PKI Implemented and
Operated by Emirates ID.
Its Root CA Certifies
Sub-CA
Root CA
Population CA
Certification
Certification
eID Certificates
Sub CA
The e-government CA is implemented & supported by the same infrastructure. Their team are invovled during key ceremony and will handle operations themselves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

Figure 8: UAE PKI Architecture

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

7.2 Online Users Authentication

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

1. *Issuance of a smart card with the digital profile in a secure encrypted format:*

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

2. *Development and distribution of a toolkit that enabled service providers to integrate smart card readers with the ability to read the tamper proof encrypted data in the card:*

The developed toolkit allows service providers to integrate the UAE ID card reading, verification and authentication capabilities with their own legacy applications. Distribution of these toolkits meant that many Government departments could now securely establish the identity of the cardholder and deliver critical services to the citizens and residents in lesser time.

3. *Publish a CRL on website and setup an OCSP:*

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

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

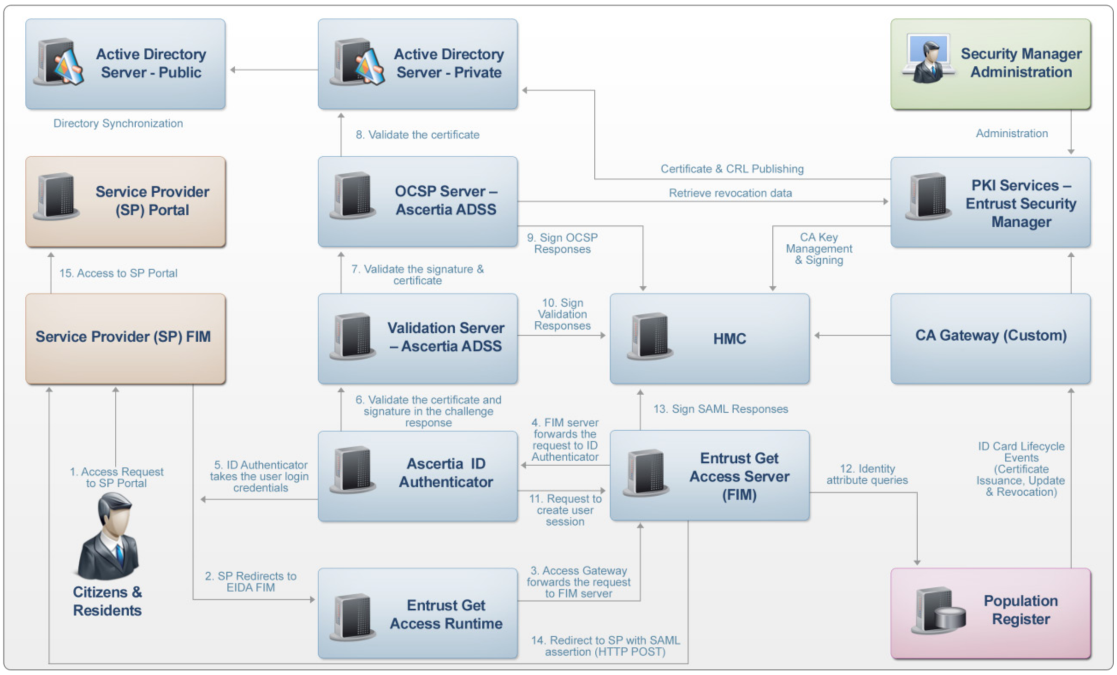

Active Directory Server - Public
Active Directory Server - Private
Security Manager Administration
Directory Synchronization
8. Validate the certificate
Administration
Certificate & CRL Publishing
Retrieve revocation data
Service Provider (SP) Portal
OCSP Server – Ascertia ADSS
PKI Services – Entrust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

Figure 9: UAE PKI Deployment Overview

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

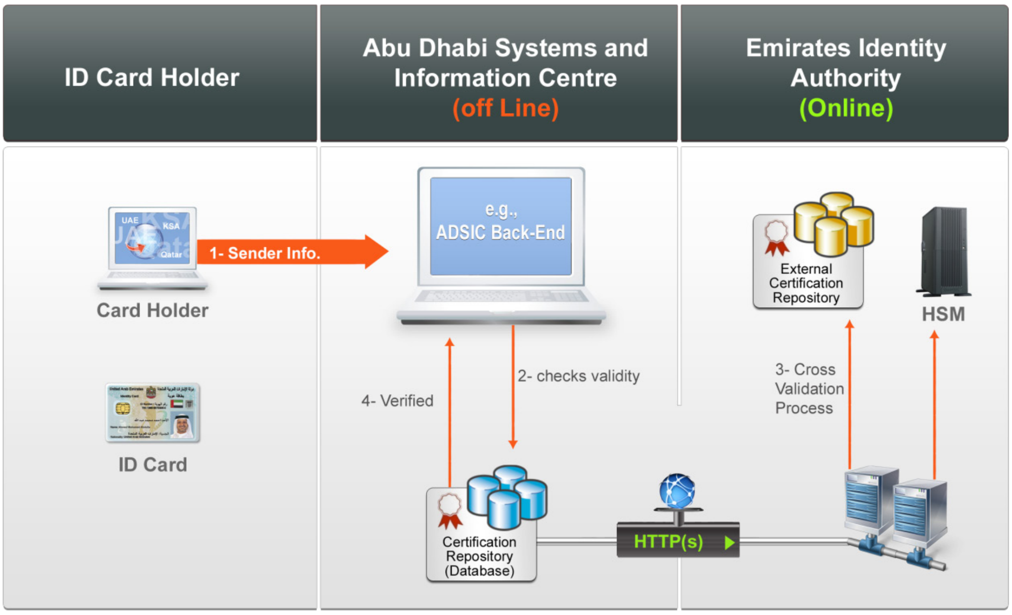

ID Card Holder
Abu Dhabi Systems and Information Centre (off Line)
Emirates Identity Authority (Online)
1- Sender Info.
Card Holder
ID Card
e.g., ADSIC Back-End
4- Verified
2- checks validity
Certification Repository (Database)
HTTP(s)
External Certification Repository
HSM
3- Cross Validation Process

Figure 10: PKI Authentication and Validation Workflow

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

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

Following the example set by UAE, more countries in the Middle East are moving towards implementing their own national PKI solutions. Moves are afoot in the region to ensure that there is interoperability among the various national ID cards and more specifically between GCC countries[4]. Similar to the European initiative GCC, countries are working on developing a common eIdentity infrastructure that will enable the authentication of GCC citizens by any service provider at a member state e.g., border control, public services, etc (Al-Khouri and Bechlaghem, 2011).

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

8. Managing the Implementation

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

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

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

meetings to ensure that the technical implementations morph into business deployments. This was a key lesson learned from our PKI implementation.

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

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

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

9. GCC and UAE PKI Program in reference to European leaders

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

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

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

On a different level, the GCC identity interoperability project underway draws many parallels with the European Interoperability Framework which looks at specifying how administrations, businesses and citizens communicate with each other within and across Member States' borders. Several EU Member States have rolled out smartcard based electronic ID (eID) solutions for their citizens. There are good references of national ID card equipped with PKI digital certificates being deployed in Europe with Belgium, Estonia, and Germany, as leading examples.

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

10. Conclusion

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

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

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

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

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

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

11. References

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

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

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

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

Basu, S. (2004). eGovernment and developing countries: an overview. International Review of Law Computers, 18(1), 109-132.

Baum, C., & Maio, A.D. (2000). Gartner's four phases of eGovernment model. Gartner Group Inc., Stamford.

Becker, J., Algermissen, L. and Falk, T. (2011.) Modernising Processes in Public Administrations: Process Management in the Age of eGovernment and New Public Management. Springer.

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

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

Broster, D. (2011). Digital Governance Tomorrow: Extrapolation or Discontinuity? Establishing a Dialogue on Identity & Behaviour in a Digital Society. Borderless eGovernment Services for Europeans, 6th European Ministerial eGovernment Conference, Poznan, 17-18 November 2011, retrieved December 12, 2011 from http://www.egov2011.pl/egov2011/public/main/attachments.html?co=show&instance=12&parent=81&lang=en&id=121.

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

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

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

Heeks, R. (2006). Implementing and Managing eGovernment: An International Text, London: Sage Publications Limited.

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

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

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

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

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

UN. (2010). UN EGovernment Survey – 2010: Leveraging eGovernment at a time of financial and economic crisis, UNDESA, retrieved December 6, 2011 from http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan038855.pdf.

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

Author

Dr. Ali M. Al-Khouri
Director General, Emirates Identity Authority, UAE
Ali.AlKhouri@emiratesid.ae
http://www.epractice.eu/en/people/271476