Ali M. Al-Khouri / International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 3, pp.461-477

Optimizing Identity and Access Management (IAM) Frameworks

Ali M. Al-Khouri

Emirates Identity Authority, Abu Dhabi, United Arab Emirates
Email: ali.alkhouri@emiratesid.ae

ABSTRACT

Organizations in both public and private sectors are realizing the value of identity and access management technology to address mission-critical needs and to ensure appropriate access to resources across heterogeneous technology environments, and to meet rigorous compliance requirements. A well-designed identity management system is fundamental to enabling better information sharing, enhancing privacy protection, and connecting the diverse web of public and private sector agencies involved in the delivery of today's public service. This article provides an overview of identity and access management literature. It attempts to analyze the business drivers, trends, issues and challenges associated with the implementation of such systems. It then presents a strategic framework and an overall ecosystem for the implementation of identity and access management system in different contexts of applications. It also introduces possible strategies and solutions for the development of a federated national identity infrastructure. It finally sheds light on a recent government implementation in the United Arab Emirates that was launched to develop a modern identity management infrastructure to enable digital identities and support their application in e-government and e-commerce context.

Keywords - identity and access management; federated identity; national identity card.

1. INTRODUCTION

The rapid globalization of world commerce, converted conventional businesses that were used to be based on handshakes, into new electronic forms of commerce enabling remote impersonal transactions. This transformation of the way commerce is handled has largely been due to the explosive growth in Information and Communication Technology (ICT). Today's businesses rely solidly on ICT systems for their day-to-day operations. Business challenges that necessitate reaching out to far flung customers are forcing organizations to open up their internal systems to outsiders such as suppliers, customers and partners [1]. This has literally broken down the virtual perimeter conceived as part of the organizations' security strategy [2]. Due to this, many outsiders have now become an integral part of organizations' ICT definitions [3].On the other hand, governments are enormously investing in ICT to transform the way they deliver services to their citizens, residents and businesses. Convenience of transacting directly with the government and the attempts to reduce the red tape in government services has driven public sector to adapt to a more productive business processes. To many of us today, gone are the days when citizens had to visit a government office for a service. Our expectations of public services have risen to an extent where we expect now services to be delivered at our doorsteps. ICT is envisaged to transform government business and services to meet citizens' expectations for better services, and to create a more open government. These developments necessitate the ability to establish and confirm the identity of remote entities, provide identity assurance and ensure authorized access. Though the priorities and principal drivers of identity management differ from one sector to another, there exists a common foundation for identity and access management that is gradually converging based on trust establishment.

The intent of this article is to provide an overview of the literature surrounding the application of identity and access management. It also aims to establish a link between identity and access management technologies and the role of governments in establishing and managing the identity lifecycle of their citizen and resident population. Such governments' take up, is expected to momentously drive identity and access management developments to higher levels.

This article is structured as follows. First, a short overview of the literature on identity and access management is provided. Associated business drivers, trends, issues and challenges, and opportunities are identified. The value pyramid of identity and access management is explained in the context of an ecosystem. Next, the role of governments' national identity programs and underpinning technologies such as smart cards and PKI technologies in the

optimization of identity and access management systems is outlined. Finally, we delineate on a UAE government program that was launched to set up a national identity infrastructure and enable digital identities to support e-government transformation and e-commerce initiatives.

2. IDENTITY MANAGEMENT: AN EMBRYONIC DISCIPLINE

There is an old say we used to hear about trust: "Only a man you trust can breach your trust". This is the irony of trust. Identity has become a new focal point in today's global economy. It forms the basis of social and commercial interactions. As illustrated in Table 1, trust is defined and interpreted differently in various study domains such as computer science, psychology and sociology. Trust involves providing reliable identity assertion of the relevant parties. Achieving such goal requires building a "Trust Framework" for each identity system that addresses both the operational requirements and the legal rules necessary to define a trustworthy identity system [4].

Table 1: interpretation of Trust in different study domains

Trust Domain	Desc.
trusted systems:	related to security engineering and encompasses areas such as risk management, surveillance, auditing and communications.
"web of trust" systems:	related to cryptography and focuses on technologies like public key infrastructure.
trust metric:	considered within the areas of psychology and sociology and proposes a measure of how a member of a group is trusted by other members.

Source: Choi et al., 2006.

Ever since computing technologies have been applied for business operations, identities were managed in one form or another. Over time, identity management evolved as a separate discipline in line with the growing importance that this technology has gained over the years. There have been endless attempts by researchers and practitioners to construct community-aware identity management systems and for establishing higher trust levels between users of different digital networks [5]. However, the critical issue lies in the fact that there are few implemented systems in practice that provide strong user authentication capabilities and new levels of trust and confidence to how identities are established and verified.

Thus, the industry and governments alike are beginning to realize that *trust management* is intricately integrated with *identity management*. This is to say that trusted identity information is a key foundation element to privacy protection and information sharing. Access control is then built on a set of authorizations which are given as directives through the security policy. With the growing needs of security, compliance and newer infrastructure models like cloud platforms, identity and access management has become the corner stone for today's ICT enabled business models [6].

Identity and access management system is considered as a framework for business processes that facilitates the management of electronic identities [8]. The framework includes the technology needed to support identity management. IAM technology is used to establish, record and manage user identities and their related access permissions in an automated approach. This ensures that access privileges are granted according to corporate policy and that all individuals and services are properly authenticated, authorized and audited. Let us look at some surveys related to the domain of trust and access management, which should clarify the seriousness of the topic being discussed here.

2.1 RECENT SURVEYS

A 2009 Data Breach Investigations Report by the Verizon Business RISK shows that almost one third of data breaches were linked to trusted business partners, such as suppliers and contractors [8]. In addition, and according to findings of another recent study conducted by Deloitte and the National Association of State Chief Information Officers (NASCIO), surveyed organizations reported that the majority (55 percent) of internal information breaches were traced to either the malicious or inadvertent behavior of employees [9]. See also Fig. 1.

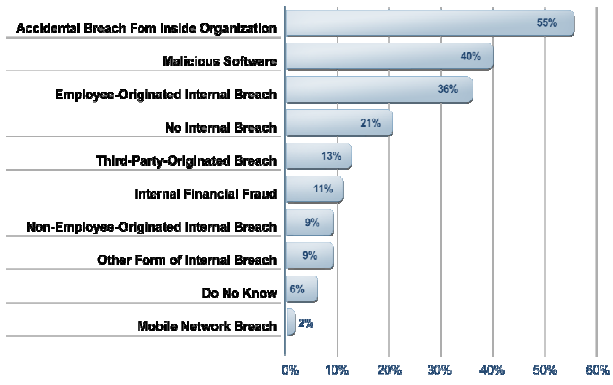

Fig.1: Source of breaches

According to a study conducted to better understand activities affecting information systems and data in critical infrastructure sectors, it was stated that the incidents studied were caused mainly by "Insiders" [10,11]. The study which was collaboratively developed by United States Secret

Service's National Threat Assessment Center (NTAC) and the CERT® Program (CERT) and the Carnegie Mellon University (CMU), revealed that:

- The majority (58%) of insiders were current employees in administrative and support positions that required limited technical skills.
- **Financial gain was the motive (54%) for most insiders' illicit cyber activities.**
- Most (85%) of the insiders had authorized access at the time of their malicious activity.
- **Access control gaps facilitated most (69%) of the insider incidents.**
- Half (50%) of the insiders exploited weaknesses in established business processes or controls such as inadequate or poorly enforced policies and procedures for separation of duties (22%).
- Insider actions affected federal, state, and local government agencies with the major impact to organizations being fraud resulting from damage to information or data (86%).

These are indeed very disturbing facts. Today, it does not take a technical wizard to commit frauds in technology oriented systems. There are always opportunities for various technical and non-technical employees to use legitimate and authorized access channels to engage in insider attacks. The insiders involved in the cases studied in the above survey did not share a common profile, and showed considerable variability in their range of technical knowledge. So we argue here that it is the breach of trust that is the root cause for such illicit activities.

In the following sub sections, we will look at how IAM technology have evolved, and outline key business drivers, trends, issues, challenges, and business opportunities of IAM across the globe that contributed to the maturity of this technology. This would give us an overview of the evolving capabilities of IAM solutions that help organizations to address today's challenges.

2.2 IDENTITY AND ACCESS MANAGEMENT EVOLUTION

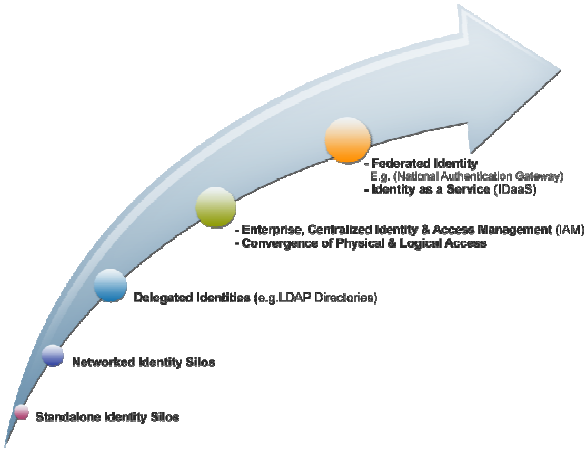

Fig. 2. IAM evolution

Identity and access management technologies arose from the necessity to satisfy basic business needs of improving security and cost savings. At this early stage, IAM existed in standalone identity silos. As businesses began to turn to automation in an effort to cope with market speed and enhance business results, the need to secure transactions became more important, which paved the way for networked access models to appear. As the time went on, IAM technologies were further developed to simplify resource access related processes and as a tool to meet increasing compliance issues surrounding client privacy, data integrity, and security (e.g., LDAP concept, centralized access models).

Larger networks and interconnected systems in a geographically diverse environments resulted in IAM federated identity access models. This approach enables organizations to optimally pursue business automation goals and higher operational efficiencies and market penetration through aligning together their business models, IT policies, security and privacy goals and requirements. In other words, identity federation is referred to the set of business and technology agreements between multiple organizations to allow users to use the same identification data to access privileged information across many disparate network domains. Obviously, identity federation offers economic savings, security and privacy as well as convenience, to both enterprises and their network users. However, and in order for a federated identity to be effective (i.e., developing an integrated service model in the supply chain), organizations must have a sense of mutual trust. This will be elaborated in more detail in the next section.

2.3 BUSINESS DRIVERS AND TRENDS

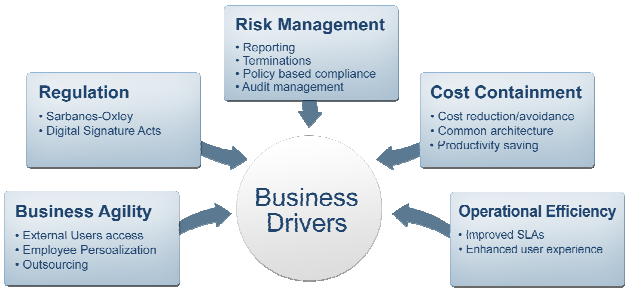

Fig. 3. IAM business drivers

According to a recent Forrester Research [12] identity and access management was identified as a top security issue for 2011 that needed to be considered as a critical component of corporate security strategies [see also 13-15]. Forrester predicted that IT administration efficiency and business agility will become the main drivers for using identity and access management. It also indicated that there will be tighter integration between data security and the identity lifecycle. Along with the requirement to secure mobile devices with second factor authentication, this is expected to drive both on-premises and cloud-based IAM implementations.

Apart from security needs, there are various other factors that influence the adoption of identity and access management. In a survey conducted by KPMG [16] in 2008, it found that the primary reasons to implement IAM solutions were related to business agility, cost containment, operational efficiency, IT risk management and regulatory compliance. Fig. 3 below captures the essence of the business drivers for IAM.

Table 2: IAM Trends

Convergence of Physical & Logical Access Management	• There is a greater level of convergence between physical and Logical access management, through centralization of Identities, policies and credentials management
Authentication & Identity Federation	• Demand for strong authentication is growing as enterprises and government agencies seek to deter cybercrime
Authorization	• Fine grained authorization is increasingly in demand • SAML is a broadly used standard protocol and successful business models have been implemented
Identity Assurance	• National ID initiatives enhances Identity Assurance
Roles & Attributes	• There is a growing acceptance of role based access control in production systems
Regulation	• Government regulations (e.g. SOX, HIPAA/HITECH), will continue to expand, both on national and international levels
Personalization & Context	• Personalization can enhance the value of online user experience. Both identity and context are essential for personalization
Identity Analytics	• Advanced data analytics will bring value to many identity-based activities such as Authentication, Context/Purpose and Auditing • Analytics brings tremendous value in monitoring the key usage patterns and statistics •
Internet Identity	• User-centric or user-managed Identity technologies such as Infocard/Cardspace and OpenID, are trying to address the security and ease-of-use requirements
Identity in the Cloud	• Identity as a Service (IDaaS) is a critical foundation for Cloud Computing

The ability to on-board different external and internal resources on one integration seamless environment results in high business agility. The need for identity management and access control and authorization cannot be understated in this case. Government and audit regulations stipulate proper controls for audit trail. Without a proper identity management, no audit trail can be established. Security and risk management dictate the use of identity management. Loss of data results in loss of business. The cost containment due to adoption of IAM technology drives the IAM strategy and architecture to be adopted. Last but not least, is the improvement in operational efficiencies sought to be provided due to identity management. These define the key drivers for IAM.

The KPMG report [16] referred to above indicated that improving compliance was among the main drivers of IAM projects to comply with the increasingly stringent regulatory requirements, posed by laws and legislation. The survey respondents indicated that some of the more prominent benefits that their organizations expected were related to quicker handling of accounts, of authorization of employee, employee lifecycle management, as well as of the automation of associated repetitive manual activities. Such process improvement was envisaged to enhance consumer experience and federate with partners in an efficient, secure business processes that lead to operational efficiency and cost containment.

When IAM is used as a preventive mechanism to enforce polices by automated controls, it is viewed to ensure an

organization wide secure access control infrastructure. Table 2 depicts further trends identified by identity and access management vendors as shaping the market in the next five to seven years.

2.4 Issues and Challenges

The implementation of identity and access management possess its own challenges and risks, as it potentially requires capital investment and changes in personnel and existing business operations [17,18]. The introduction of identity and access management processes into an organization can expose it to new risks while mitigating existing ones [19-21]. For instance, as organizations open up their systems to allow more external entities to access sensitive internal data, the risk of breaches from external sources (partner-facing risk) would continue to be a threatening factor.

In practice, identity and access management as a technology must scale to match the need of the heterogeneous ICT environments found in most organizations [22]. As more systems come online and new partnerships are formed, and with systems in numerous locations, the task becomes more and more resource intensive without it [23]. What is more, in recent years regulatory requirements have added complexity and increased external scrutiny of access management processes. Organizations need to develop an understanding of such risks as they implement new or modified identity and access management processes. Table 3 provides an overview of these risks.

Table 3: Identity and access management risks

Administration Overhead	Security Risks
• No centralized user administration process. • Multiple teams are involved in the user administration activities. • Increasing overhead in administration of identities • Administrators spend a lot of time performing routine admin tasks that can be automated • Different administrators often assign different IDs to the same person. This makes it difficult to track activity back to a single source and confuses the customer.	• Potential security risks • Accounts are created with unauthorized system access rights. • Security risks occur when frustrated or overburdened admin staffs may take shortcuts, terminations may not be done as soon as required or permissions granted may be in excess of what is really needed.
Complexity	**Inefficiency**
• The users of the system are located worldwide and can be customers, employees, temporary workers, contractors and external suppliers. • Multiple authentication requirements for applications • Account creation/deletion in repositories is performed by multiple groups • Many systems and applications have different business owners, platforms, administrative tools, and system administrators, leading to slow performance, delayed or unreliable terminations and higher administration costs. • Account creation process requires great coordination, involves many steps, and involves multiple clients which must remain segregated from each other • Support staff requires advanced training to administer accounts on so many varying systems. • Employees and customers require timely access to applications and systems to perform their jobs.	• A high number of calls are made to the support center for user provisioning activities including password resets. • Terminating employee accounts is a manual process • The process for business unit managers and application owners to sign off on the privileges of the users is cumbersome and time consuming. • Proliferation of directories and identities: diverse infrastructure has evolved over time • Redundant identity information • Information inaccuracies • Users wait longer than necessary to obtain IDs • Managers spend time chasing a sequence of events to ensure proper approvals. • Authorizations needed to process a request often slow the process of account creation or update and leads to errors and mistakes.
Poor Compliance	**Lack of Long Term Strategy**
• Untimely response to regulations	• Managing for the moment, but not positioned for the future

2.5 Federated Identity Management

A government organization previously managing access only for its employees now needs to manage access for millions of citizens and a wide range of other agencies accessing information and seeking online services. Federated identity management provides capabilities such as government-to-citizen self-service and federated single sign-on (SSO) support. It allows organizations to centralize fine-grained security policy management to enforce access control across applications, databases, portals and business services. The need for federated identity is thus driven by four major drivers; security, compliance, business agility and operational efficiencies. See also Fig. 4.

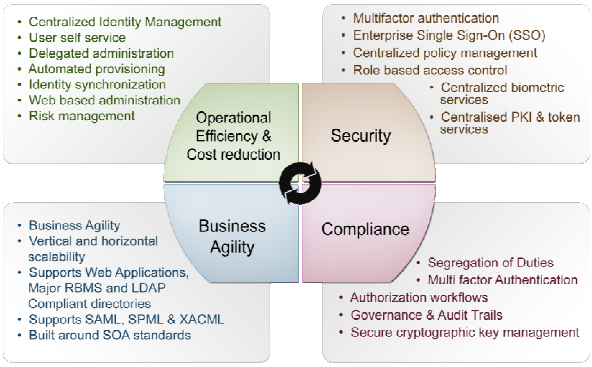

Fig. 4: Drivers for federated identity management

Federated identity is the big move forward in providing an integrated environment for the citizens, service providers and the different government agencies. While a service is delivered to a citizen online, there would be different stakeholders that would be involved in the service delivery cycle. Federated identity provides a very effective solution that obviates the need of repeated authentications and verifications each time a new stakeholder joins the service delivery cycle.

A single credible source of verification can be shared by the different entities which rely on the trust created by the source. This verified identity is then federated to different entities. This leads to uniform security policy enforcement, greater compliance to regulations related to Identification, provides better scalability and responsiveness from different stakeholders ultimately ensuring operational efficiencies and reducing operational costs.

Having said this, the next section looks at the IAM ecosystem that attempts to explain how an integrated architecture can be developed to unify siloed security technologies into a comprehensive, standards-based identity management framework.

3. IDENTITY MANAGEMENT ECOSYSTEM

Identity and access management like many other enterprise solutions cannot add value in a stand-alone mode. The overall value of identity and access management entirely depends on the level and easiness with which it integrates with other enterprise systems. Fig.7 depicts a typical identity and access management ecosystem. On one side, we have different kinds of users like employees, partners, suppliers and customers. On the other side, we have diverse kind of enterprise resources like directories, databases, servers, network resources etc. There exists a complex relation between the users and enterprise resources in terms of identity lifecycle management and access controls. This in turn has to comply with various security standards and guidelines, enabling, at the same time, organizations to achieve their business objectives. It is desirable to have a governance and policy control framework at the heart of the ecosystem that orchestrates the way the whole ecosystem work.

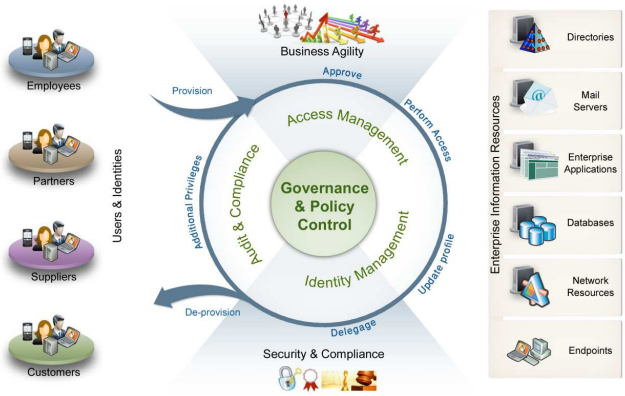

Fig.5. Identity and access management ecosystem

In a step to develop more cohesive identity and access management working models, there is a trend in the industry that is pushing for the convergence of physical and logical access systems. This is likely to enhance the ecosystem as we discuss next.

3.1 CONVERGENCE OF PHYSICAL AND LOGICAL ACCESS

Organizations have long operated, and still many do operate physical and logical access systems as two independent structures, and are typically run by completely separate departments. This is very much evident in current organization structures in the Middle East for example. This is to say that logical access to corporate ICT resources such as e-mail, database permissions, web access, intranet/internet connectivity and database applications are granted and remain the responsibility of ICT departments. The service or facilities departments are responsible to control physical access systems such building doors access, life support systems, etc.

Nonetheless, boundaries between physical access and logical access systems are melting in the current digital world due to several economical and efficiency factors. In fact, identity and access management technology is bringing in a transformation in the way the industry categorizes security and in the development of the primary capabilities of authentication, authorization and administration [24]. This transformation is expected to revolutionize e-business, allowing organizations to use digital identities to contribute real value to their business (ibid).

From one standpoint, combining logical and physical security systems gives a more comprehensive view of

potential intrusions across the physical and IT environments. From another perspective, it is likely to result in significant improvement of the user experience both from administration and end-user perspectives, e.g., cost savings and improving efficiency and enforcing policies throughout the organization. This should provide multilayered security across company networks, systems, facilities, data, intellectual property and information assets.

Fig. 6 shows the convergence of some physical and logical access systems. Physical facilities like office complexes, warehouses, production facilities need to be protected from unauthorized access. Once inside the premises, a person would need access to the network resources like ERP applications, files etc that are stored on a central database. Conventionally these two systems were separate, even though the access and authorization for access were similar, if not the same.

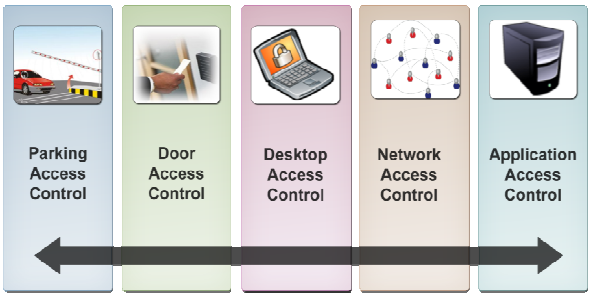

Fig. 6. Convergence of physical and logical access

It is important to refer here that traditional identity and access management architectures focus more on the user provisioning and access management. Today's identities comprise not only of human entities, but also numerous kinds of endpoints such as desktops, laptops, PDAs, smart phone etc. Hence a comprehensive credential management system capable of managing the lifecycle of credentials of these diverse types of entities is a fundamental requirement for today's world. The next subsection looks at how modern identification systems are enabling more robust identity establishment and lifecycle management.

3.2 MODERN DIGITAL IDENTIFICATION SYSTEMS: ENABLERS OF TRANSFORMATION

Critical Infrastructures have long relied on biometric verification and authentication of individuals to provide stricter access to secure locations. Only authorized personnel verified by the biometric data could gain access to secure areas. The file access and network access depends largely on provisioning of users on IT systems like LDAP. Single factor authentication limited the verification of the authorized users by means of passwords. Stronger authentication systems based on biometrics advancements made the biometric data to be available on smart cards enabling what-so-called digital IDs. The same biometric systems that provided physical access could now be utilized for network access. This has made the identity management administration move from facilities management to IT administration.

As authentication remains the mechanism through which access is granted to any corporate resource either physical or logical, identity management systems are forming a primary building block and enabler for such convergence. In other words, modern digital identification systems are facilitating this convergence and unification of identification systems and authorization for access, as they provide identities in digital forms. Smart card technologies are considered to be a key player in this regard. Smart cards use a unique serial number and a Personal Identification Number (PIN) to identify a user, prove identity and grant network access. This 'unified access' token can provide several security-level options ranging from simple access control to complex data encryption. See also Fig. 7.

At the core of all access control is policies, roles and provisioning of users to their roles. Identity establishment is based on the digital credentials backed by strong authentication mechanisms (multi factor authentication) and secure verification of the credentials thus presented. Trust is established by the secure identification that provides assurance to the identity seeker of the genuineness of the identity. The application of identity and access management could vary from one domain to another. Hence it is important to look at the IAM in the context of different domains and their applications, as we outline next.

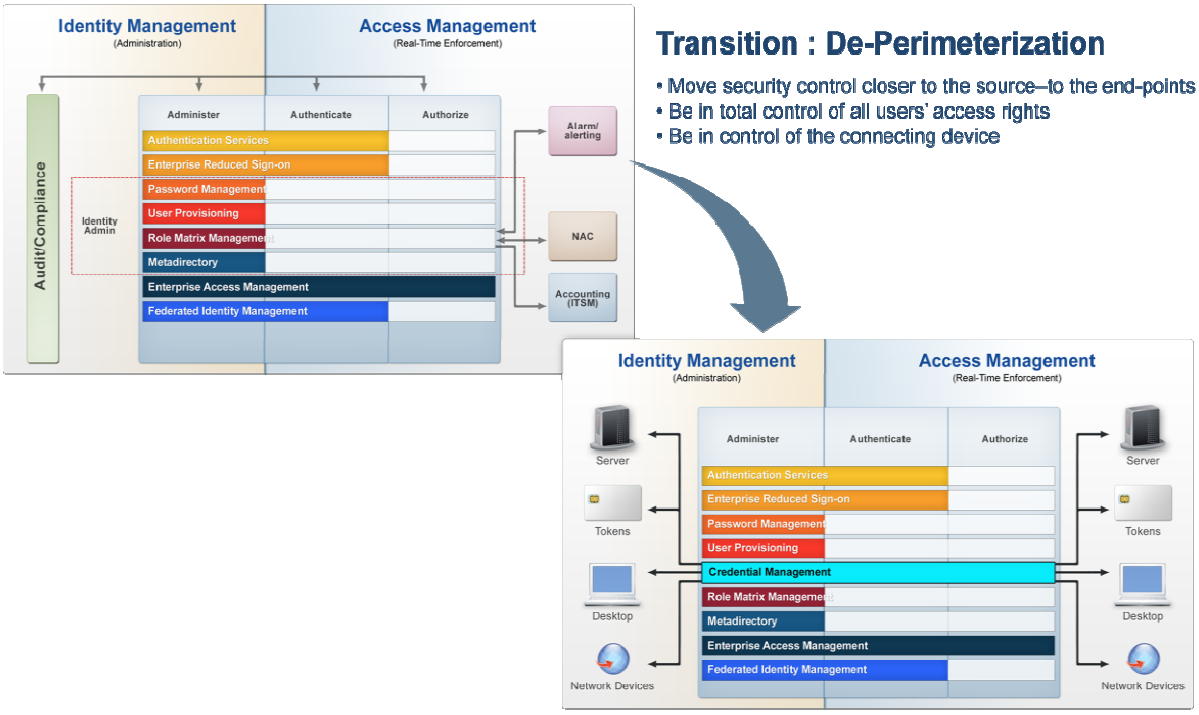

Fig. 7. De-perimeterization of identity and access management (Source: Jerichofurm)

3.3. ENTERPRISE CONTEXT

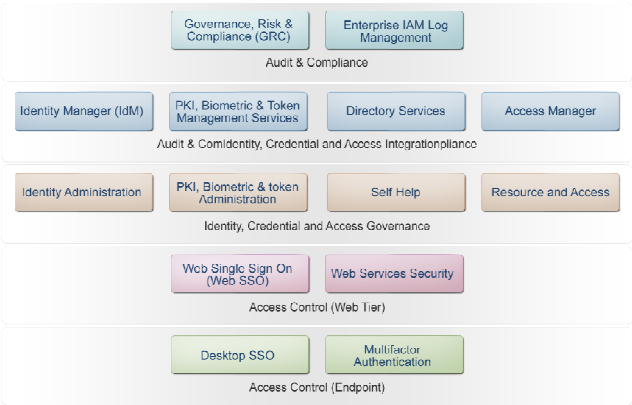

Fig. 8: Layers of identity and access management in an enterprise context

There are typically 5 layers of identity and access management in an enterprise context as depicted in Fig. 8. Using a top-down approach, the first layer integrates business intelligence, process management, and automated controls enforcement to enable sustainable risk and compliance management. It encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.

The second layer deals with identity credentials and access integration. This layer is a result of the identity management polices and the laid down requirements for establishing and verifying an identity. This is a crucial component of the enterprise IAM. Identity can be established by providing an ID number to an individual. To strengthen the identity, digital credentials can be provided as verifiable metadata of the ID. Typically the credentials are issued in the form of a digital certificate from a PKI system and biometric minutiae. A directory service (e.g., LDAP) provides the ability to list and provision an individual's identity for access management. A policy repository with role definition and provisioning of users provides the last component of this layer; i.e., the access management system.

The third layer deals with access governance. This governs the mechanism of defining policies, administration of the identity management system, audit trails, reporting, etc. The remaining two layers are access management component and the application of identity administration and governance components. The Web Tier access management layers allows secure web single sign-on solution that connects remote users to corporate web applications and

systems through a secure portal. The Web based applications can be tied together with the Web SSO enabling centralization of access control and policy enforcement.

The last layer of access control employs multiple factor authentication mechanism to grant access to enterprise systems, platforms and applications. This layer is used for according authorized access to protected resources and prompts strong authentication capabilities. Both access control layers are truly integrated. The same single password (or token) works in both layers as user credentials are managed from a centralized SSO.

Apparently, identity management architecture in enterprises is driven by security needs. There is a colossal difference when we talk about identity management in a government context, as the next subsection outlines.

3.4. GOVERNMENT CONTEXT

A governmental initiative for identity management is typically driven by various factors as in the enterprise context, but the drivers are slightly different. Major drivers for identity management in the government sector are:

- compliance with federal laws, regulations, standards, and governance relevant to identity management;
- facilitate e-government by streamlining access to services;
- improve security posture across the federal enterprise;
- enable trust and interoperability**;**
- reduce costs and increase efficiency associated with identities.

Identity management is largely citizen centric in the government context. Citizens transact with their governments in many ways - to seek information, rightful benefits, business services, legal recourse etc. The interactions of the citizens with their governments are varied and very dynamic. In a federal context, IAM provides tremendous value in the interactions between the government, citizens and businesses. A robust identity management system seeks to make the service delivery more convenient. Consequently, for the government, the core element in providing right content and personalized services is to ensure its citizens are provided with credible and verifiable credentials.

Reliable identification and authentication of entities in an online or over the counter environment is a critical requisite [25]. Fig. 9 below depicts the typical value pyramid for the IAM in government context. Trusted entities can reliably transact in seeking and availing of services delivered remotely or over the counter. Identity needs to be established at every node – i.e., in G2G, G2B, G2C, B2B, C2C and B2C transactions.

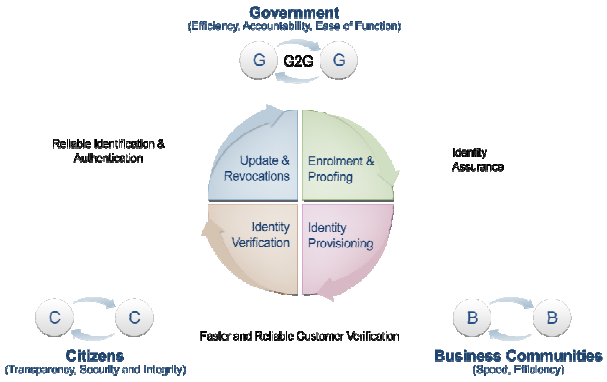

Fig. 9. IAM value pyramid in government context

The identity and access management platform here is very akin in functionality to the one in the enterprise context. The difference is in the application. Herein, the government facilitates the identity issue and provides assurance to the identity by means of strong authentication mechanisms. So at the core of the IAM value pyramid is the "identity issue system". This system allows the government to enroll its citizen and resident population and provide them with identity baselines "proof of identity" that will be used as credible credentials for identity provisioning and strong authentication.

Management of identities is carried out by means of dynamically updating the identity repository for new additions and revocations. As the provider of the identity, the government provides a third party service for reliable identity verification to the seekers of this service. To understand how this pyramid works in practice, let us look at the role of national identity cards and PKI technology in the optimisation of identity and access management systems.

4. ROLE OF NATIONAL ID CARD & PKI IN IAM OPTIMIZATION

Governments and enterprises have always been engaged in providing an Identity to their stakeholders for benefit deliveries and services. Conventionally, identity documents were all paper based (e.g. passports, birth certificate, etc.) which have very limited use in online transactions and incur cumbersome processes to verify the authenticity of these documents. The role of optimization thus gets defined. Identity management optimization includes a re-look at the identity infrastructure, processes involved in determining the authenticity of an identity, parameters to establish the identity and processes for trust establishment and, providing

assurance to the service seekers and service providers of the identity established in the process. Identity management optimization seeks to reduce the time involved in completing the processes of identity and trust establishment between two entities.

In a national context, many governments around the world are issuing national identity cards as a vehicle that carries digital identity credentials. Many of the modern national identity cards are based on smart card technology. It enables faster identification and authentication of citizens and residents. Thus we view a national identity card as an enabler and a means to optimize the identity and access processes across various organizations by eliminating redundant identity infrastructure and providing higher levels of assurance.

Smart cards are an exceptional means to store identification metadata of the card owner securely. The security accorded by the smart cards, backed by a strong and solid multi factor authentication methods allow secure communications with the card. The smart cards provide tamper proof mechanism to store identity data. Table 4 provides an overview of the features provided by smart cards.

Table 4: Smart card capabilities

Security	Protection
• Match on card biometric • Support for RSA (PKI), DES and Hash algorithms • PIN protection to access card information	• Tamper proof protection against forgery • Self locking on brute force attacks • Applications can be protected through SAM
On Card Processing	
• On card cryptographic processing chip • Protection of PKI private keys on Smartcard • Capability to generate PKI key pairs on card • On-card digital signing and encryption	

These features provide an unshakeable trust in the data held in the card [26]. Therefore, any data read from such secure cards provides the means for instant verification of identity. The smart card can store biometric information that can be checked with a biometric device to match the data in the card. Further, any communication with the card itself is encrypted and is carried out only using authorized protocols. Such authorized protocols provide a control on who gets to read the data and use for verification.

In addition to the personal information that can be stored, the smart card can store securely the set of private and public keys that constitute an electronic signature of an individual. The PKI system provides the equivalent of a biometric fingerprint to individuals in the form a digital certificate which is a unique signature that is provided to individuals. This certificate can then be used as credentials from the secure store in the card to establish further trust in the transactions carried out electronically by the individuals. The following diagram provides an overview of key PKI benefits.

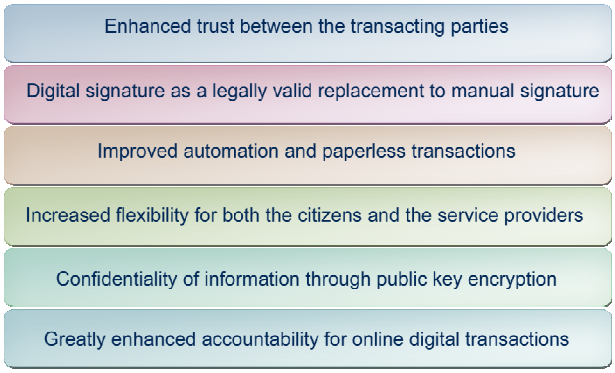

Fig. 10. Key benefits of PKI

Establishing the identity of a person is not sufficient to conduct a transaction. Enhanced mutual trust is needed to be established that assures the stakeholders of the transaction that:

1. the transaction indeed did take place;
2. the stakeholders in the transaction did indeed take part in the transaction and have accepted the transaction as completed;
3. there is irrefutable evidence on the time at which the transaction has taken place;
4. confidentiality of the transaction is maintained; and
5. in case of a dispute, the transaction can be legally upheld.

PKI technology enhances the trust between the parties involved in the transaction. PKI allows digital signing, allowing transactions to be carried out electronically without geographic barriers, providing tremendous ease in the transactions across the globe. Such a transaction obviates the need of paper. And, if the PKI is provided as a service by the identity provider, it provides a third party assurances leading to enhanced accountability in the transaction.

With smart cards, multi factor authentication is possible i.e., biometric, PIN and password can be used since the card can provide such capabilities. Typically two of these three factors can be used by service providers for identity verification. The security on the card ensures strong privacy since unauthorized users cannot read any data from the card. This leads to less fraud since identity is securely established and business can then authorize the authenticated users to

complete the transaction. Being digital, all the transactions, services, verification, etc are audit trailed for a back track check providing very high accountability. No one can deny the usage of the card, if the card has been used in a transaction. Such secure features backed by the ease of implementation allow quick adoption of the card and PKI for rendering services electronically. Such identity systems provide a win-win platform for businesses to enable lower turn-around times in their go-to-market strategies. The following diagram summarizes the benefits accorded by these complementary technologies.

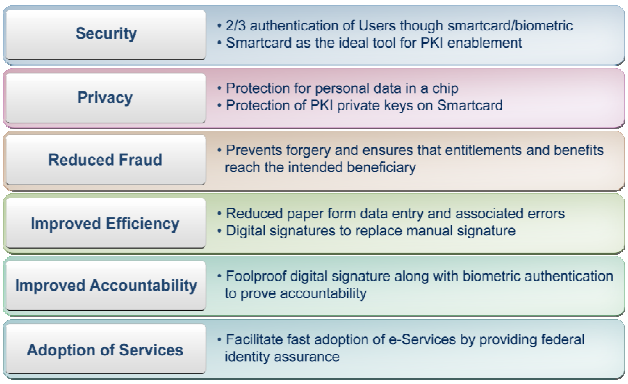

Fig. 11. Smart card and PKI benefits

The next section looks at one of the pioneering government implementation programs in the Middle East to setup and provide reliable identification and verification mechanisms to enable digital identities with the aim to support e-government and e-commerce initiatives.

5. IDENTITY INITIATIVE: THE CASE OF THE UNITED ARAB EMIRATES

Globally there are a few countries that have successfully adopted digital identity systems. Belgium, France, Finland, Malaysia, South Korea, Singapore remain some of the successful examples. In the Gulf region, there are appealing initiatives in the digital identity front. United Arab Emirates, Oman, Bahrain and the Kingdom of Saudi Arabia have launched in the last five years modern identity management programs. Due to the current role of the author in the UAE program, and lack of information about other governments' practices, the discussion in this section will be limited to only the UAE project.

United Arab Emirates has taken the lead in the Middle East to implement a modern national identity management infrastructure with smart card, PKI and biometric technologies and in promoting digital identities to its citizen and resident population – estimated around 9 million people in 2011. The government established an independent federal agency named Emirates Identity Authority in 2004, to become the sole identity provider in the country. The organization introduced lately a "4E Strategy" to promote the application of digital identities. This strategy is envisaged to support and play a key role in the transformation of service delivery infrastructure and in enabling e-government and e-commerce initiatives in the country.

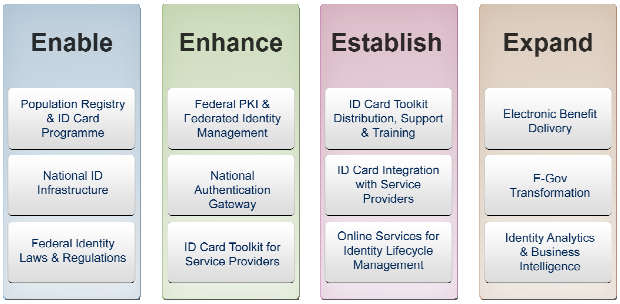

Fig. 12. UAE "4E Strategy" implementation framework

As depicted in Fig. 12, the first phase of the strategy relates to the setup of a national identity infrastructure to (*enable*) and empower citizen and the resident population digitally by enrolling them in a state of art and technologically sophisticated population register. The registration process includes the capturing of biographical data, personal portrait and ten rolled fingerprints. A robust identity verification process takes place to perform biographical and biometrics checks against the population register and other forensic systems, to ensure that the person has not been enrolled previously and/or is needed by the legal authorities for criminal charges.

After passing through this stage, each individual is then assigned a unique identification number, which is linked to his or her biometrics. A smart card is issued to each individual that contains multiple credentials including unique RFID, MRZ barcode, photo ID, two best fingerprints for authentication purposes. The ten prints taken at the enrolment stage is stored in the population register database. The UAE smart card, which is considered the highest in specification worldwide in government application to-date, is a combi- microprocessor-card, with both contact and contactless capabilities. To *enable* digital identities, the card also contains crypto keys and digital certificates.

The UAE government invested heavily in PKI technology to support e-government and e-commerce initiatives. PKI is seen as an important trust anchor, as it will determine compliance to defined criteria of trustworthiness of online identities. The government is working on crafting a legal framework and policy structure to provide the legal grounds

and promote the adoption of digital identities in all walks of life in the country.

The government has shown particular effort to further *enhance* the digital identity infrastructure through the development and setting up of a federated identity management system and a national authentication gateway. The government aims to integrate multiple authentication capabilities provided by the new smart ID card and access channels to diverse resource interfaces in e-government and e-commerce environments. In an attempt to demystify the application of smart cards, a tool kit has been developed to allow service providers to seamlessly integrate the digital identification solution with their service delivery chain systems [27].

Managing the lifecycle of a digital identity presents significant business challenge i.e., the processes and technology used to create and delete accounts, manage account and entitlement changes and track policy compliance, etc. From this perspective, the government is working on *establishing* and providing managed identity services to both government and private sector organizations. This will provide a service level-based identity lifecycle management solution that is designed to offer authorization services only to individuals with valid ID cards. Indeed, a government based certification authority that issues and manages the lifecycle of digital identities is likely to acquire higher levels of trust.

The government is currently working to develop an integration platform to integrate the population register database with multiple government organizations involved in the identity lifecycle management related processes i.e., ministries of interior, health, justice, labour, and education who are responsible for civil incidents of the individuals related to (residency details, birth, marriage, divorce, death, education and health register). This will support organizations to better define and automate the processes and policies related to the authorization of digital identities and associated entitlements.

The integration platform and the national authentication gateway being designed and implemented are expected to completely transform the nature of business and government transactions in the country. The government *expansion* plans focus to provide the foundation for secure government communications and transactions and identity business intelligence for e-government transformation. This infrastructure provides a key building block to defend against security threats and identity fraud and at the same time enhancing resource utilization, improve productivity, and maximize ROI. Expansion of the online identity services and continual improvement to the identity infrastructure is envisaged to greatly support national and individual security, as well as building the country's new digital economy [28]. So to clarify how the national identity framework adopted in the UAE government is designed and implemented, we attempt to outline in the following subsections its primary components and how they work.

5.1. UAE National Identity Framework

The national identity and access management in government context as we explained earlier differ vastly in the objectives and the expected outcomes of identity management from enterprise perspectives. Identity management in enterprises is driven by their security needs. And in this context, enterprise investment in identity management is dictated by the criticality of their internal data and the exposure they need to service their clients. At a national (government) level, identity management takes a different connotation altogether. The UAE government is assuming the role of an identity service provider to provide identity credentials to entities.

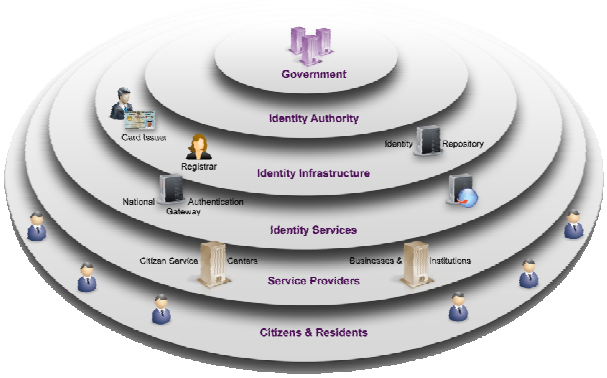

Figure 13: Government identity and management layers

As depicted in Figure 13, the adopted national identity framework in the UAE consists of many layers to enhance its reach and to improve the identity assurance levels. It assumes the role of providing the necessary credentials to provide baselines for provisioning and authenticating identities. The credentials are packaged in a secure system and delivered to the citizen. At this stage, smart cards act as the vehicle for such credentials to be delivered to the citizens.

An identity infrastructure is currently being setup in the UAE to contain various identity repositories along with the verification mechanisms to enable identity establishment and verification on demand. This then should form a credible identity service provided by the government that can be used by the different service seekers and service providers alike. Let us take few examples.

Banks and financial institutions are classic examples of service providers. Banks invest heavily in securing their financial systems. Conventionally, customers need to carry out their financial transaction with their banks by physically visiting one of the bank branches, where a teller agent verifies the customer in a "face-to-face" approach. With the increase in online banking facilities and in attempt to provide convenience, banks currently resort various identity establishment mechanisms ranging from interactive tokens with one time passwords (OTP), virtual keyboards, PIN verification and biometric verification. Now, with the government stepping in, to securely verify the credentials and to stand to guarantee online identities, electronic banking and e-business models are expected to flourish and support the country's economy.

Let us consider another scenario where a government agency needs to deliver a service to a citizen. As part of the service delivery, the government employee needs to verify the credentials of the citizen. During the process of service delivery, the government employee needs to access different applications, databases – sometimes cutting across different departments and different government agencies. Current conventional processes depend on time consuming manual tasks that necessitate communication going back and forth to access data, verify identity, seek and get approvals and so on.

The new government federated identity architecture provides online credentials to both employees and citizens. This allows employees' identities to be established and trusted to accord access across different systems in the government. The same identity management system would ensure verification of the citizen's identity and allow the right services to be delivered to the right entities in the right time. This is expected to supporting the government's strategy to revolutionizing public services and e-government transformation. Let us see how the national identity authentication is architected in the next subsection.

5.2. National Authentication Gateway

Fig. 14 provides an overview of the national authentication architecture in the UAE and its key components. At the heart of the architecture is the identity gateway.

As the national identity provider, the UAE government relies primarily on the digital identity it issues in the form of a smart card as a vehicle for authenticating physical or virtual users. All requests for verification of an identity would have to be ported through an electronic system that acts much like a gatekeeper for the requests. Valid requests are entertained and sent to the identity verification systems managed by the identity provider. These are web based systems that provide the front end access to submit a request for identification and identity verification using defined industry standard protocols.

The requests are redirected to the gateway which in turn communicates with the identity management system. PKI systems provide the ability for transactions in real time using online certificate status protocol (OCSP). In transaction terms, a citizen is served by a service provider remotely. The citizen tries to access the services through a secure web site. The service provider needs to identify the citizen. The citizen submits his identity card with his credentials. The service provider's application on the web reads the cards, collects the credentials from the card and refers the data with a verification request to the identity service provider. The identity provider validates the request coming from the service provider as a valid request and allows the request to be processed. The identity provider verifies two main components of the ID data submitted by the service provider:

1. the Card itself to check the genuineness of the card; and
2. the Certificate data in the card.

Optionally, the service provider could also request for the verification of the biometrics. Secure communication is established between the card and the service provider's application. This is provided by an Active X control component running on the browser or by the authentication gateway. The architecture is designed to handle millions of identity validation requests on daily basis and is expected to scale based on requirements. Having said this, the following section summarizes and concludes the article.

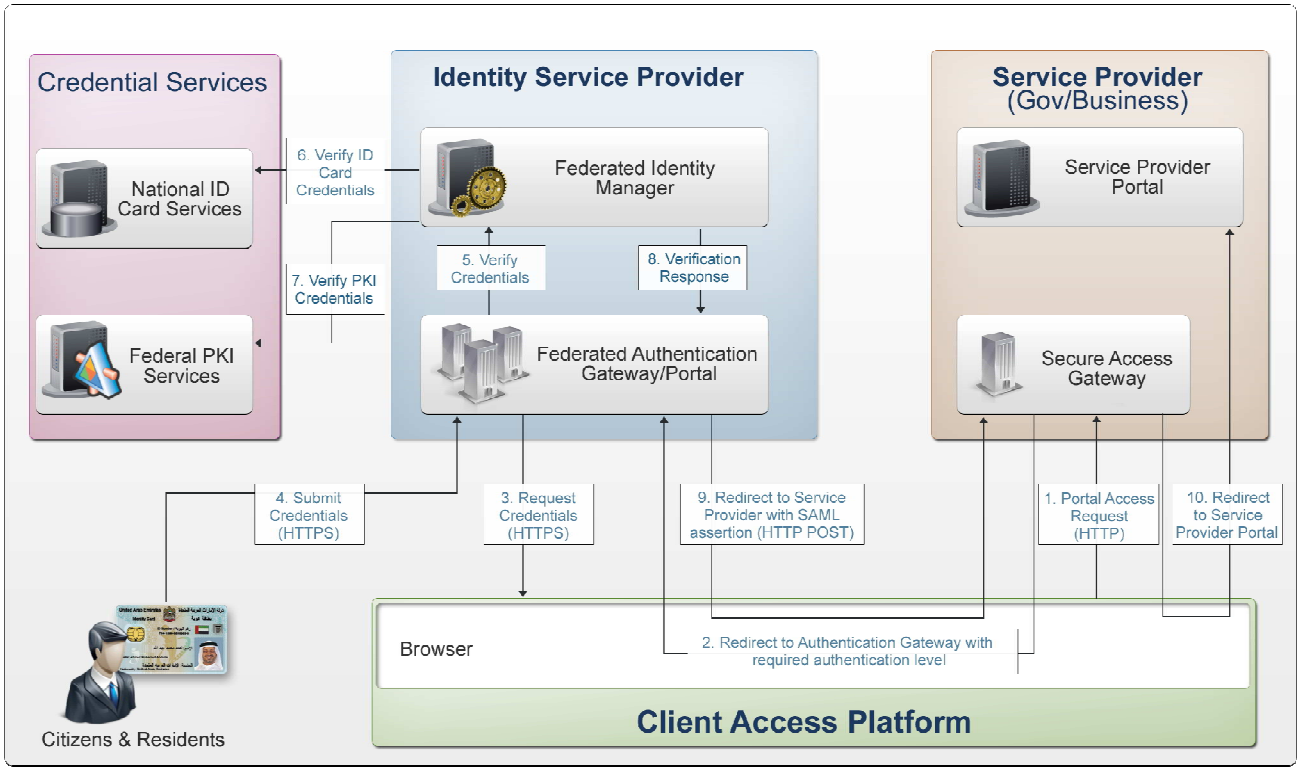

Fig. 14. National authentication gateway architecture

6. CONCLUSION

We presented in this article how identity and access management technology can provide a framework for (1) simplifying the management of access to services, (2) implementing policy, (3) increasing transparency, and (4) enabling scalability in operations to integrate identity management infrastructure with services provided by both central and distributed ICT systems.

We believe that the scope of identity management is becoming much larger in today's organizational context, and its application more critical. They indeed provide new levels of trust and confidence to identification systems. The role of the government is seen to play a major role in setting up a trusted identity management system and addressing the entire identity lifecycle of establishment, management and usage. The case of the UAE government is worth to be further examined and evaluated to measure its success, and most probably other cases from other countries.

It was not in the scope of this article to discuss the case of the UAE government in detail. The author just presented it for the purpose of referring to one of the very ambitious government initiatives in the field. The existing literature lacks such references from government implementations as it merely focuses on private sector and commercial cases.

In summary, the following key points discussed in this article, are likely to have a high impact on governments and public services in the near future:

- With the growing needs of Identification and rapid growth in information technology, the manner in which physical access and logical access requirements are met show a high degree of convergence. A digital identity issued to a person serves to provide access control to physical areas controlled for secure access as well as access to secure logical information.
- As the needs of remote (online) transactions grow, the identity and trust management between stakeholders becomes a key issue. Trust is accorded in identities by the assurance of the Identity provider. This makes the government, as indicated above, a key player in identity management by becoming the de-facto Identity provider to the citizens of the nation. System deployed by governments to provide identity assurance services are likely to evolve in the coming few years to address identity assurance requirements i.e., complete identity services from identity issuance, credentials management, verification services and identity assurance;
- National identity frameworks are characterized by a national authentication gateway will provide standards based, reliable identification and verification requirements of e-government service providers and businesses;
- Enterprise IAM implementations are growing towards maturity and we will see federated identity management integrating government, businesses and citizens at a national level; and
- Smart cards and PKI technologies will play a central role in optimizing the identity services, being the enablers and the vehicles of identity management.

REFERENCES

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

[2] Whitman, M.E. and Mattord, H.J. (2011) Principles of Information Security (4th edition). Course Technology.

[3] Stamp, M. (2011) Information Security: Principles and Practice (2nd edition). Wiley.

[4] ABA Report (2011) Trust Framework, ABA Federated Identity Management Legal Task Force [Online]. Retrieved from: http://www.fips201.com/resources/audio/iab_0211/Draft_Trust_Framework-6.pdf. Accessed: 13 June 2011.

[5] Choi, H., Kruk, S.R., Grzonkowski, S., Stankiewicz, K., Davis, B. and Breslin, J.G. (2006) Trust Models for Community-Aware Identity Management [Online]. Retrieved from: http://www.ibiblio.org/hhalpin/irw2006/skruk.html. Accessed: 2 July 2011.

[6] Aberdeen Group (2007) Identity and Access Management Critical to Operations and Security. Communication News. Retrieved from: http://www.comnews.com/WhitePaper_Library/Managed_services/pdfs/Quest_Software_Aberdeen_IAM_Critical_to_Operations_and_Security.pdf. Accessed: 1 June 2011.

[7] Benantar, M. (2005) Access Control Systems: Security, Identity Management and Trust Models. Springer.

[8] Baker, W.H., Hutton, A., Hylender, C.D., Novak, C., Porter, C., Sartin, B., Tippett, P. Valentine, J.A. (2009) Data Breach Investigations Report - Verizon Business [Online]. Retrieved from: www.verizonbusiness.com/resources/.../reports/2009_databreach_rp.pdf. Accessed: 2 July 2011.

[9] Deloitte-NASCIO (2010) State governments at risk: A call to secure citizen data and inspire public trust. The 2010 Deloitte-NASCIO Cybersecurity Study. A publication of Deloitte and the National Association of State Chief Information Officers [Online]. Retrieved from: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_state_2010DeloitteNASCIOCybersecurityStudy_110910.pdf. Accessed: 4 August 2011.

[10] Keeney, M., Cappelli, D., Kowalski, E. and Moore, A. (2005) Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors [Online]. Retrieved from: http://www.secretservice.gov/ntac/its_report_050516.pdf. Accessed: 23 May 2011.

[11] Randazzo, M.R., Cappelli, D., Keeney, M. Moore, A. and Kowalski, E. (2004) Illicit Cyber Activity in the Banking and Finance Sector [Online]. Retrieved from: http://www.secretservice.gov/ntac/its_report_040820.pdf. Accessed: 13 June 2011.

[12] Forrester Report, "Twelve Recommendations For Your 2011 Security Strategy." Forrester Research [Online]. Retrieved from: http://www.forrester.com. Accessed 18 June 2011.

[13] Cser, A. and Penn, J. (2008) Identity Management Market Forecast: 2007 to 2014. Forrester. Retrieved from: http://www.securelyyoursllc.com/files/Identity%20Management%20Market%20Forecast%202007%20To%202014.pdf. Accessed: 1 June 2011.

[14] Trigoso, C. (2010) Thinking of the Future: Identity and Access Management. Retrieved from: http://carlos-trigoso.com/2010/12/22/thinking-of-the-future-identity-and-access-management. Accessed: 13 June 2011.

[15] FIDIS (2006) D5.2b: ID-related crime: Towards a common ground for interdisciplinary research. Retrieved from: http://www.fidis.net. Accessed: 1 June 2011.

[16] KPMG (2008) KPMG's 2008 European Identity & Access Management Survey - Status and maturity of identity and access management projects in European organizations [Online]. Retrieved from: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/European-identity-access-management-survey.pdf. Accessed: 23 May 2011.

[17] Aldhizer III, G., Juras, P., & Martin, D. (2008) Using Automated Identity and Access Management Controls. CPA Journal, 78(9), 66-71. Retrieved from Business Source Complete database: http://0-search.ebscohost.com.maurice.bgsu.edu/login.aspx?direct=true&db=bth&AN=35654420&loginpage=login.asp&site=ehost-live&scope=site. Accessed: 1 June 2011.

[18] Reymann, P. (2008) Aligning People, Processes, and Technology for Effective Risk Management [Online] Retrieved from: http://www.theiia.org/intAuditor/itaudit/archives/2008/january/aligning-people-processes-and-technology-for-effective-risk-management. Accessed: 13 June 2011.

[19] Rai, S., Bresz, F., Renshaw, T., Rozek, J., and White, T. (2007). Global Technology Audit Guide: Identity and Access Management. The Institute of Internal Auditors. Retrieved from infotech.aicpa.org/NR/rdonlyres/...9CE1.../GTAG9IdentAccessMgmt.pdf. Accessed: 2 July 2011.

[20] Engelbert, P. (2009) 5 Keys to a Successful Identity and Access Management Implementation [Online]. Retrieved from: http://www.ca.com/files/whitepapers/iam_services_implementation_whitepaper.pdf. Accessed: 8 April 2011.

[21] Links, C.H. (2008) IAM Success Tips: Identity And Access Management Success Strategies.

[22] IDG (2009) As hyper-extended enterprises grow, so do security risks. IDG Research [Online]. Retrieved from: http://www.rsa.com/innovation/docs/IDGResearchWhitePaper_Final_060409.pdf. Accessed: 23 May 2011.

[23] Egan, M. and Mather, T. (2004) The Executive Guide to Information Security: Threats, Challenges, and Solutions. Addison-Wesley Professional.

[24] McQuaide, B. (2003) Identity and Access Management: Transforming E-security into a Catalyst for Competitive Advantage. Information Systems Audit and Control Association [online]. Retrieved from: http://kuainasi.ciens.ucv.ve/cisa/articles/v4-03p35-37.pdf. Accessed: 13 June 2011.

[25] Al-Khouri, A.M. (2010) Supporting e-government, Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.

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

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

[28] Emirates Identity Authority's 2010-2013 Strategy [Online]. Retrieved from: http://www.emiratesid.ae/en/eida/eida-strategy.aspx. Accessed: 1 June 2011.

ABOUT THE AUTHOR

Dr. Ali M. Al-Khouri is a senior government official in the United Arab Emirates. He is currently holding the position of a Director General at Emirates Identity Authority; a federal government organization established in 2004 to develop and implement a national identity management infrastructure in the country. This multi-billion dollar government program is expected to revolutionize public services and e-government initiatives. He holds an engineering doctorate in the field of "large scale and strategic government programs management" from Warwick University in UK, M.Sc. in Information management from Lancaster University, UK, and B.Sc.(Hons.) in Business IT Management from Manchester University, UK. He has been an active research in the field of e-government and identity management for the past 12 years. He has published more than 40 articles in the past 5 years in different knowledge domains.