FEDERATED E-IDENTITY MANAGEMENT ACROSS THE GULF COOPERATION COUNCIL

Ali M. Al-Khouri

Emirates Identity Authority

Abu Dhabi

United Arab Emirates

ali.alkhouri@emiratesid.ae

Abstract

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

debate and discussion, opens the door to reflection, and guides international efforts in this eminent domain of practice.

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

1. Introduction

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

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

Governments have been realizing the need to develop interoperable federated identity management platforms to support citizens' mobility cross-borders [Bruegger, 2007; Fleurus et al., 2011; Langenhove et al., 2011; Porter, 2008]. The European Commission is implementing a project to develop an interoperable electronic identification [eID] platform to provide a single, secure, and cross-border infrastructure for the authentication of legal and natural persons across Europe [STORK, 2013]. GCC countries[1] are also working on a similar platform development to facilitate GCC citizens' mobility and to enhance economic cooperation between the six member states. Both

[1] GCC stands for Gulf Cooperation Council, also called the Cooperation Council for the Arab States of the Gulf (CCASG), which was established in 1981 to promote coordination between member states in economic and social spheres. It includes six countries: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. The GCC population is estimated to be around 40 million.

projects aim to allow citizens to access cross-border services securely by using eID credentials issued by their home countries.

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

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

2. Federated Identity Management Landscape

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

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

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

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

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

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

Figure 1. Identity Federation Consideration

2.1. Identity Provider [IdP]

An IdP is an entity that issues an identity to an individual or an entity and manages user authentication and user identity relevant information. It plays a key role in not only

providing a digital identity but also in authenticating the user and storing attributes about the user. Potentially, an identity provider offers the following:

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

2. Authorization data: This is meant to ensure that the user is allowed to perform a specified operation.

3. Personal profile details of the entity: If the identity holder permits it, this is based on a request from a service provider.

2.2. Service Provider [SP]

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

2.3. Service Seeker

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

2.4. Digital Identity

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

2.5. Identifiers

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

2.6. Credentials

Credentials are a set of objects/elements that serve to authenticate an identity by means of the validation of its identifiers. This follows the [1] what does one know? [2] What does one have? [3] What is one's identity? For example, credentials can be a password or a valid response to a challenge, constituting what the individual knows. A credential could be a digital certificate constituting what the individual has. Finally, a credential could be

an inherent characteristic of the entity, such as a fingerprint, eyes, or voice. This defines what the individual is.

2.7. Domain of Application

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

2.8. Circle of Trust

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

2.9. Single Sign-On [SSO]

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

2.10. Assertion

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

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

3. The Role of Identity Provider in the Federation Ecosystem

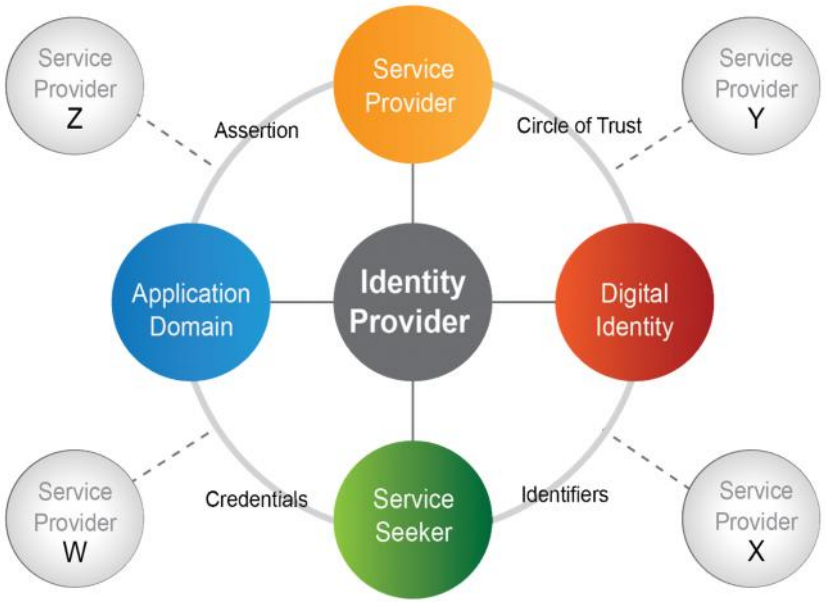

Figure 2. Federated Identity Eco-System

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

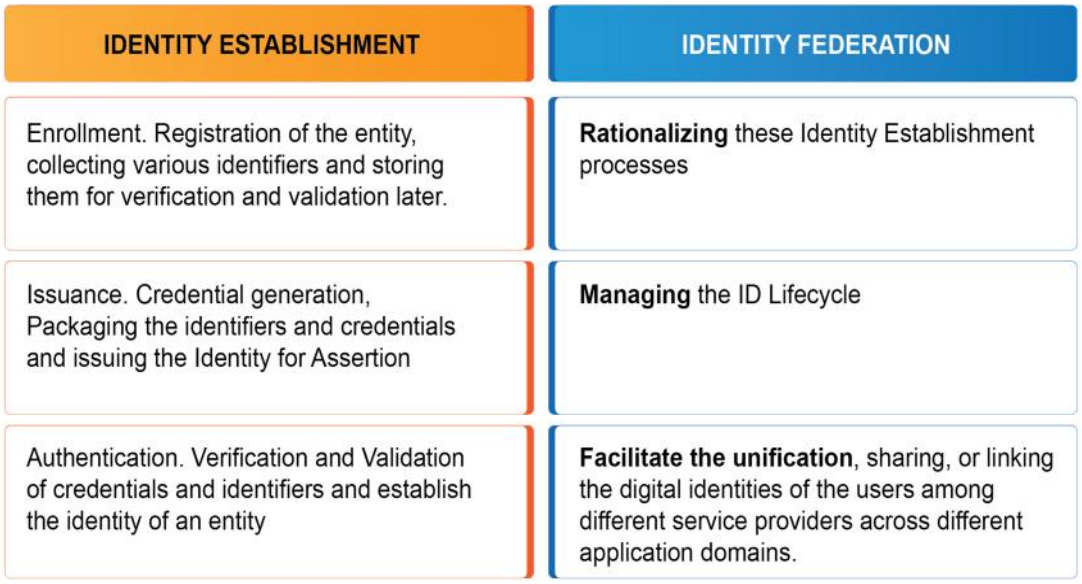

Figure 3. Roles of Identity Providers

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

4. Enrollment Process: Registration of the entity, collecting various identifiers, and storing them for later verification and validation.

5. Digital Identity and Credentials Issuance: Credential generation, packaging the identifiers and credentials, and issuing the Identity for Assertion.

6. Authentication Capabilities: Verification and validation of credentials and identifiers and establishment of the identity of an entity.

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

From a legal standpoint, governments have long been the de facto identity providers through the issuance of identity documents to their citizens and residents—e.g., passports, ID cards, driving licenses, voter registration cards, and more. With the advancement of the Internet and remote service delivery, trust and identity assertion in the digital environment has become an urgent requirement. Coping with such pressing needs, governments, the world over, have realized the need to modernize their identity management systems and initiate technologically-driven, digital identification infrastructure development programs that create digital identity profiles together with various electronic identifiers and credentials.

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

4. Identity Federation in GCC

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

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

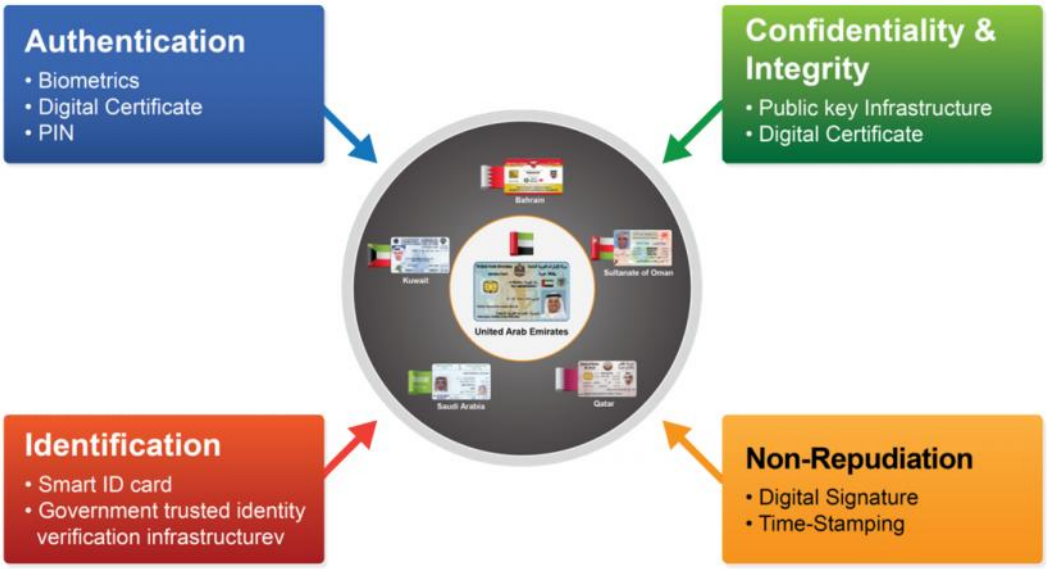

Figure 4. National ID Card as the Enabler of the Digital ID

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

7. Provided with identification parameters stored securely in the smart chip.

8. Establish a person's identity on-site, remotely allowing secure and trusted transactions.

9. Multi-factor authentication capabilities provide both match-on-card and match-off-card features and facilitate validation, verification, and authentication of an Identity.

10. The cardholder is accorded all identity services—validation, verification, authentication, and assertion of identity—from the respective national identity providers.

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

The government is at the heart of the framework—the first, innermost layer—because GCC governments have realized the need to own the development of their digital economies through the development of digital identities. This is also based on the belief that a government-issued digital identity is likely to provide higher levels of trust and assurances, and would have a positive impact on the uptake and usage by service providers. Each of the GCC countries has established independent entities and departments to act as an identity authority [identity provider], which provides the second layer of the framework. These entities and departments are responsible for the development of the infrastructure and provision of identity services [i.e., authentication and validation services].

These are layers three and four. Service providers and citizens make up the fifth and sixth layers, respectively, as beneficiaries and users of the identity services. Identity lifecycle management creates the seventh layer and represents the integration platform with other government organizations in order to maintain automated data updates in those cases involving changes to personal data.

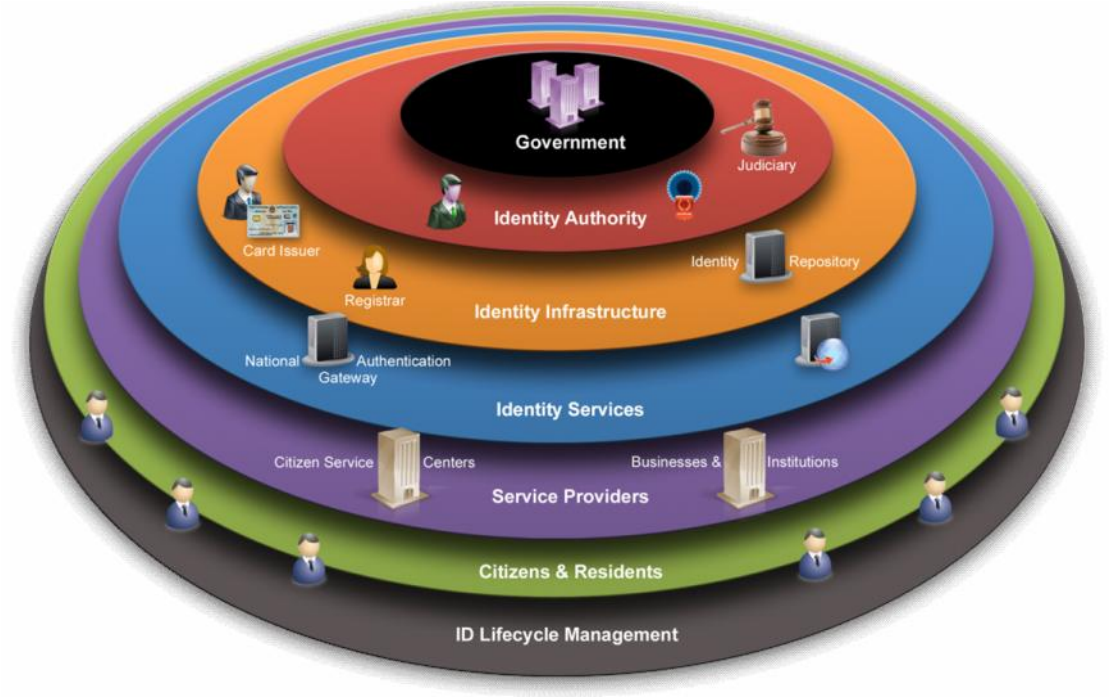

Figure 5. National Digital Identity—the GCC Context

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

Each of the GCC countries has set up a national validation gateway to provide authentication and validation services to both public and private sector organizations in their own countries. These gateways are designed to provide a federated identity for government-to-government and government-to-citizen transactions. For instance, when a user moves from one service provider to another, the *assertion token* is released to the second service provider, who trusts the authentication token generated in the first place. This ensures that, across multiple service providers, the same authentication token can be used to trust the service seeker/user without the need for the user to login or self-authenticate multiple times.

In the e-government context, this token could be handed over to the e-government portal, and the e-government entity acts as the *identity proxy*. Figure 6 depicts how the national validation gateway has been set up in the UAE.

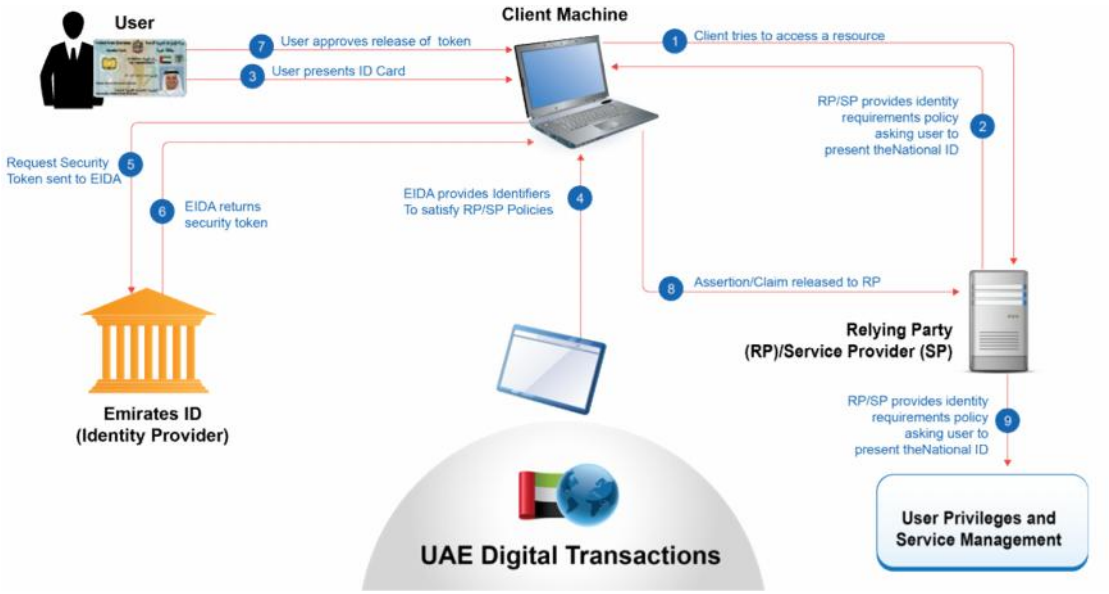

Figure 6. National ID Card and Federated Identity

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

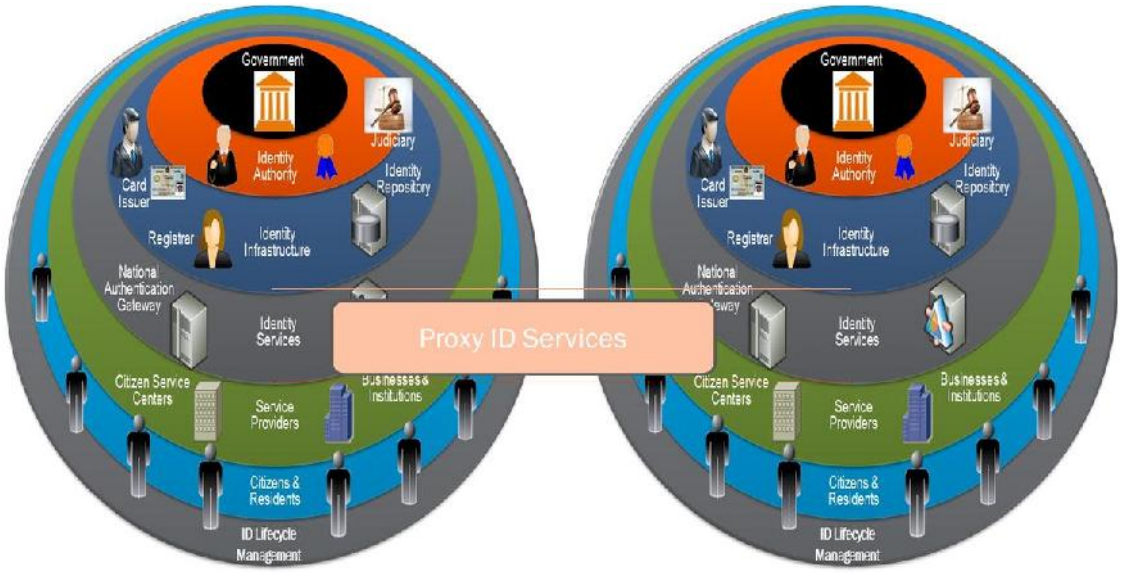

Figure 7. Federated Identity in the GCC Context

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

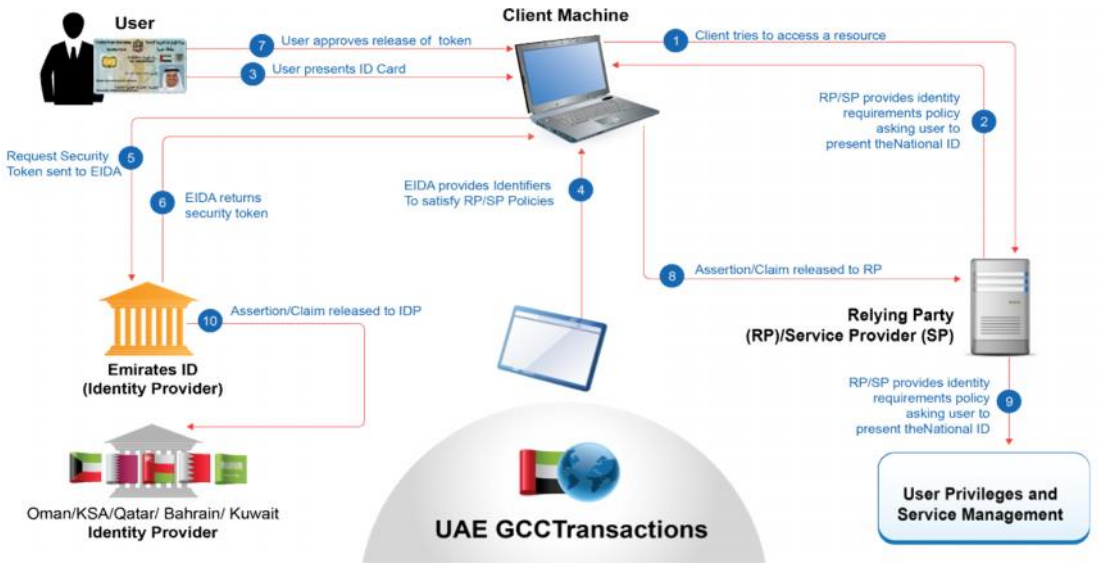

Figure 8. GCC Federated e-ID

Efforts are already underway and the GCC countries have conducted multiple workshops on interoperability. Pilots are in the planning stage to ensure "recognition" of the ID cards using Web services. In fact, a common API was developed in 2011 to read public data, in offline mode, from the GCC smart identity cards and this has been implemented at borders [airports and land and sea ports] in each of the six countries.

The current working phase links the national validation gateway systems in all countries to provide online validation and verification services across borders. Figure 9 depicts a high level, tentative implementation plan of the GCC eID interoperability project.

Figure 9. GCC Interoperability plan

5. Reflection

5.1. GCC e-ID Interoperability Platform vs. European STORK 2.0

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

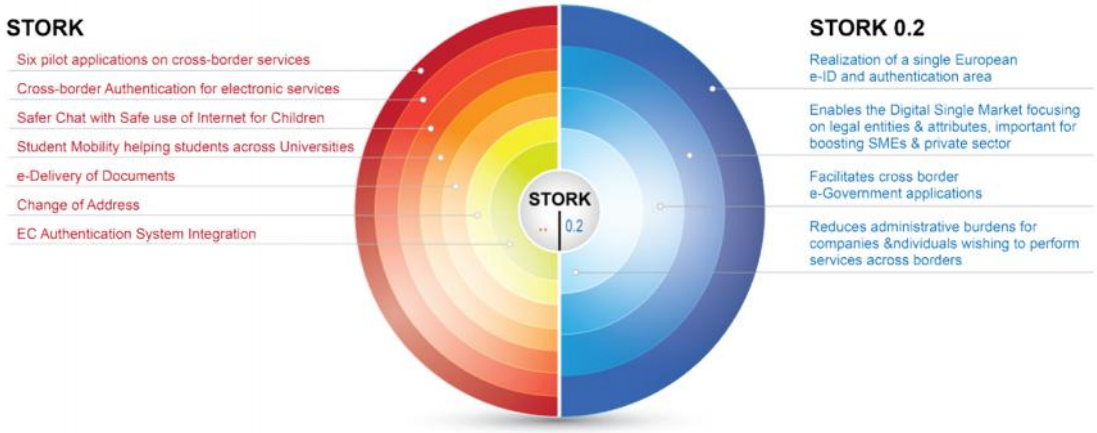

Figure 10. Key Objectives of STORK and STORK 2.0

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

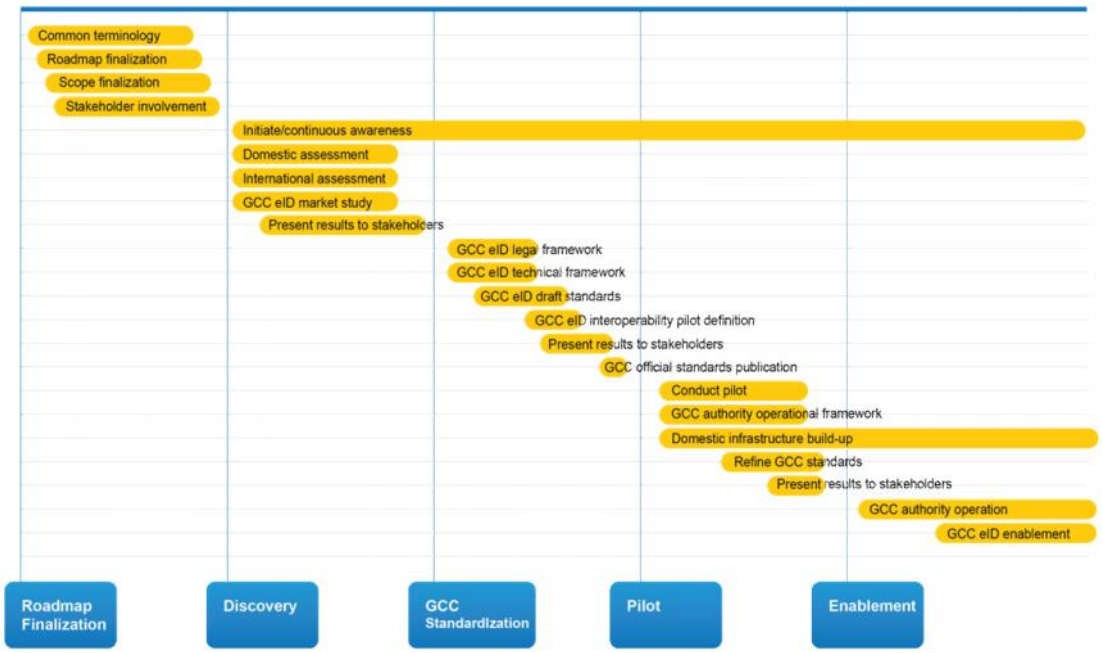

Figure 11. GCC interoperability schema

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

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

5.2. Addressing the User Spectrum

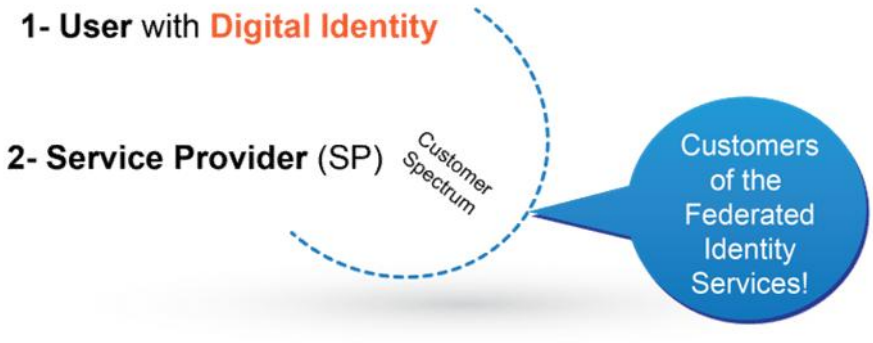

Figure 12. Pillars for successful federated identity management systems

Key to the development of a workable federated identity management system is in meeting the needs and expectations of the customer spectrum—i.e., users and service providers, who are the ultimate beneficiaries of such systems. One of the creative, yet simple, models that we recommend is Kano's Model, also depicted in Figure 13. The main objective of this model is to assist organizations to understand the three categories of customer needs and attributes so that new products or services can be launched successfully. The model classifies product attributes based on how they are perceived by customers and their effect on customer satisfaction [Kano et al., 1996]. These classifications are useful for guiding design decisions in that they indicate when good is good enough, and when more is better [ibid.].

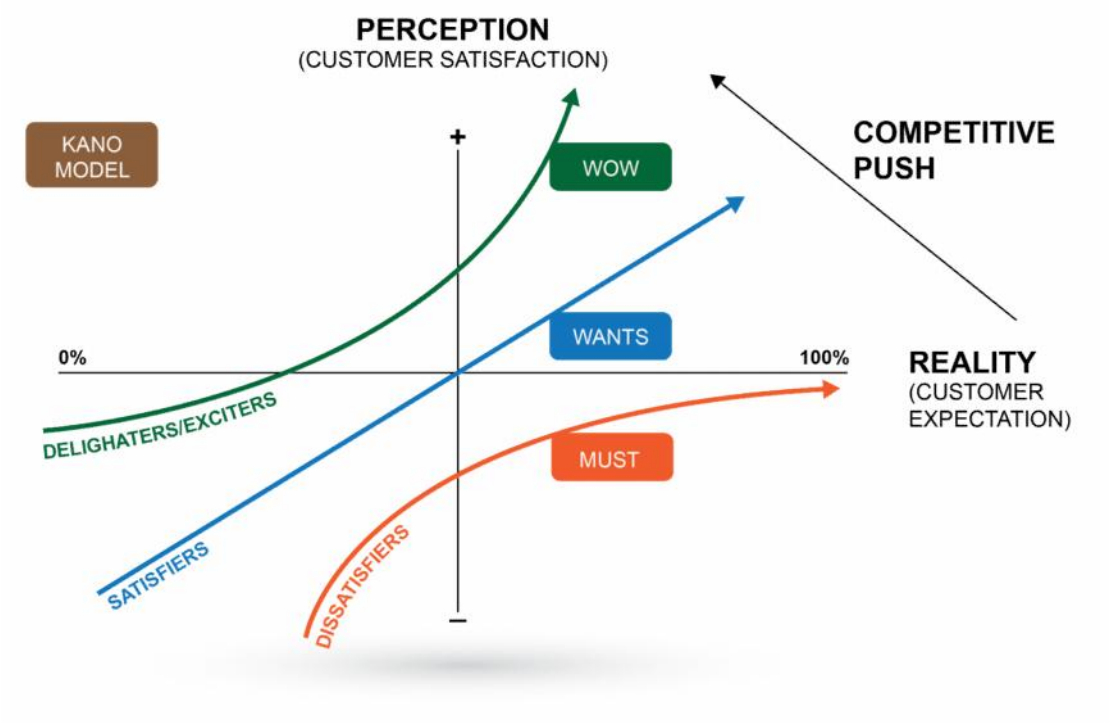

Figure 13. Kano Model of Customer [Consumer] Satisfaction

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

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

See also Figure 14.

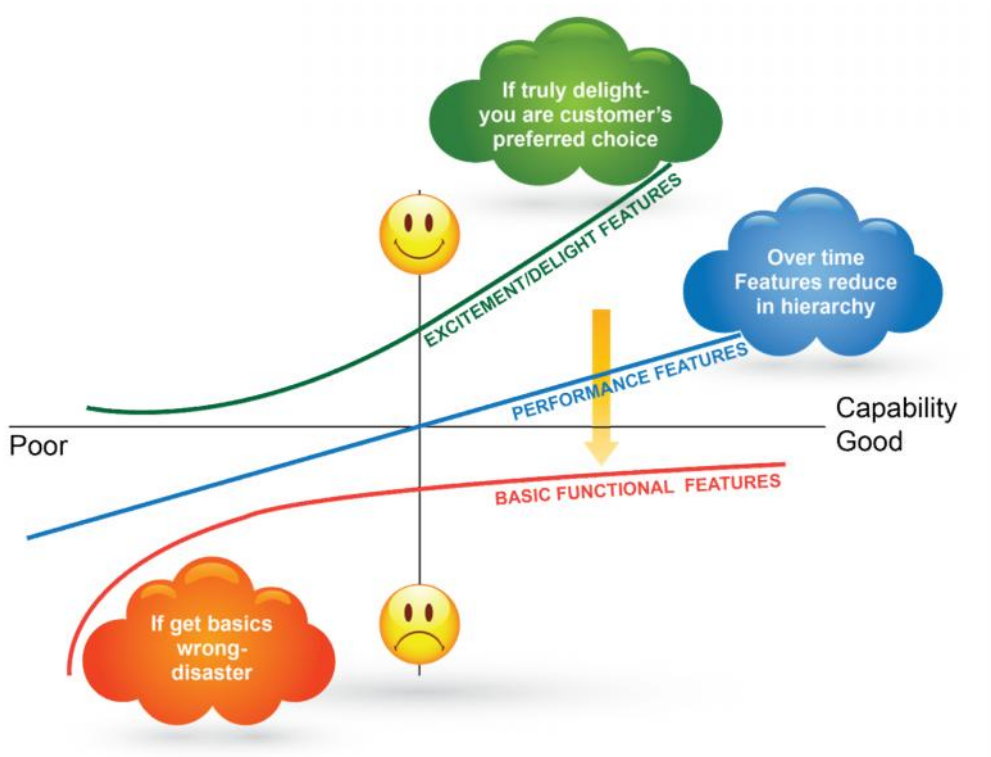

Figure 14. Kano Model

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

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

6. Conclusion

As indicated, it is certain that the benefits of a single PAN GCC digital identification and authentication area scheme are legion and will require the current economic cooperation between GCC countries to reach new and higher levels. A GCC eID interoperability platform should allow citizens to establish and conduct e-transactions across borders, merely by presenting their national eID issued to them from their own home countries.

Cross border user authentication has the potential to create benefits in different sectors and enhance access to educational resources, commercial transactions, and banking transactions. The possibilities are endless.

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

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

Acknowledgment

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

References

Al-Khouri A M. 2012. Emerging Markets and Digital Economy: Building Trust in the Virtual World. *International Journal of Innovation in the Digital Economy* 3[2], pp. 57-69.

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

Baldoni R 2012. Federated Identity Management Systems in e-Government: the Case of Italy. *Electronic Government International Journal* 8[1], pp. 64–84. http://www.dis.uniroma1.it/~midlab/articoli/EG6642.pdf

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

Bhargavan K, Fournet C, Gordon A D and Swamy N. 2008. Verified implementations of the information card federated identity-management protocol, Proceedings of the 2008 ACM symposium on Information, computer and communications security, March 18-20, 2008, Tokyo, Japan.

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

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

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

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

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

Chadwick D. 2009. Federated identity management, in Aldini A & Barthe G & Gorrieri R [eds.], *Foundations of Security Analysis and Design V*, Lecture Notes in Computer Science, 5705, p. 96-120.

CNIPA. 2008. D2.3 Overall European Regulations and Standarisation. European Civil Registery Network. http://www.ecrn.eu/docs/standard_repository.pdf

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

Digitome. 2011. Telemedicine. http://digito.me/telemedicine/

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

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

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

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

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

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

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

Landau S and Moore T. 2011. Economic Tussles in Federated Identity Management. In: 10th Workshop on the Economics of Information Security, June 14{15, 2011, Fairfax, VA. http://weis2011.econinfosec.org/papers/Economic Tussles in Federated Identity Management.pdf

Langenhove P, Dirkx M and Decreus K. 2011. European Interoperability Architecture [EIA]. European Commission- Interoperability Solutions for European Public Administrations Work Programme. http://www.difi.no/filearchive/eu-common-vision-for-an-eeia-final_1.pdf

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

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

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

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

STORK. 2013. What is STORK 2.0?. https://www.eid-stork2.eu

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

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

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

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

Annex-1: Identity Management Frameworks

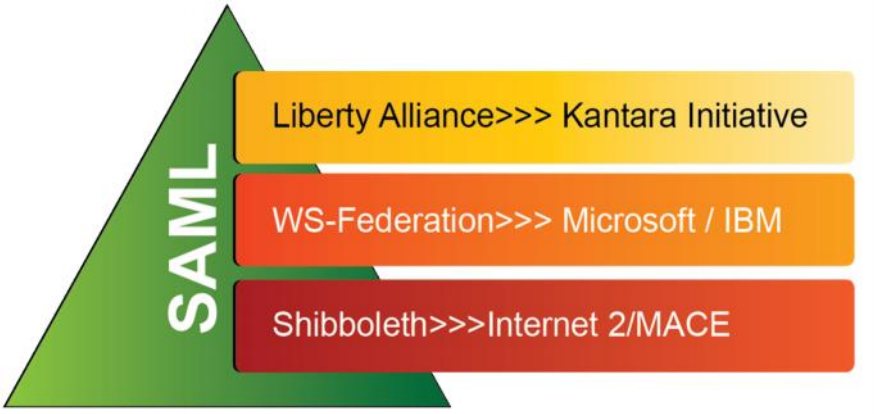

Figure A-1: Identity federation concepts and frameworks

Liberty Alliance, WS-Federation, and Shibboleth are three well known ID management frameworks based on this principle of collaboration and the sharing of identity information. Their initiatives are aimed at establishing trust between different service providers [relying parties]. All of them utilize the identity verification/authentication

methods based on open standards and use the SAML Assertion. The following is a brief description regarding each of the three frameworks.

- **SAML** is the foundation for all of the current identity federation mechanisms. It has passed through three releases: 1.0, 1.1, and [the most recently ratified] 2.0. SAML 2.0 is seen as a point of convergence as it incorporates **Liberty Alliance**'s ID-FF 1.1 and 1.2 specifications as well as **Shibboleth** version 2 functionalities.

- **Shibboleth** is a 'single-sign in' or logging-in system for computer networks and the Internet. **Shibboleth** is a project of Internet2/MACE and seeks to develop the architecture, policy structures, technologies, and open source implementation to support inter-institutional sharing of Web resources. This is, of course, subject to business rules and access controls that will allow inter-operation. This initiative seeks to provide peer-to-peer collaboration using a federated identity infrastructure based on SAML. Shibboleth has been largely adopted by university and research communities around the world. Shibboleth 2.0, which was released in March 2008, is based on SAML 2.0.

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

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

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

Some of these protocols, such as WS-Security, have been submitted to and ratified by existing standards organizations, such as Organization for the Advancement of Structured Information Standards [OASIS]. WS-* can be thought of as a suite of specifications for enabling secure Web services. This collection of specifications, including WS-Trust, WS-Federation, and WS-Policy, is an evolving set of mechanisms for layering authentication, authorization, and policy across both single and multiple security domains.

Open ID

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

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

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

- **Healthcare Management:** Providing access to healthcare services and insurance with a single identification and authentication. Healthcare has a huge potential when viewed in terms of electronic health [e-Health] [World Health Organisation, 2010; see also Linkous, 2009]. Telemedicine, as a concept, necessitates remote access and authentication. This is virtually non-existent today. Major healthcare centers, such as existing government hospitals in GCC countries, can potentially

associate with American/European partners in providing telemedicine facilities that can be driven by the identification and federated authentication of the patients [e.g., in accessing patient records]. The global growth rate in telemedicine is estimated at 19% [Digitome, 2011]. A population of over 380 million in the MENA region in 2013 [two thirds of which is rural] at a cost of $385 per patient per year translates to $97.5 billion. Only 10% of this population is taken in relation to telemedicine— working out to nearly $10 billion. There are many other economic impacts that Telemedicine could create: e.g., saving on transportation costs, time, and manpower, none of which have been considered in the calculations. Telemedicine will be extremely useful and cost effective when applied to the correctional institutions for the inmates. In terms of security, no transportation means no potential jail breaks, and secure identity ensures the prevention of fraud in health. There are many advantages.

- **Online Education:** Enhancing access to educational materials for students across universities. Online education is expected to grow at a healthy rate of 26% annually [at a conservative level]. Considering the growth in population and the skill sets required, very few universities are available and online education is even lower, at the present time. If we consider that the Middle East will require 55 million skilled employees in the next 10 years, even if only half of these are catered for, the current education facilities will not be sufficient. The opportunity window, in this case, is huge in terms of providing quality education online, and this requires strong identity management—specifically, identity federation—so that students are able to gain access to worldwide resources. Thus, American universities, for example, can provide access to the learning material based on enrollment at local universities [see, e.g., European Commission, 2005; Kapoor, 2011].

- **Government Services**: Improve access to government services. Digital signature services for remote transactions are expected to exceed $15 billion in the immediate future [with land deals and property transactions and e-enabled goods and services]. Regarding e-Government services, with consideration only being given to the UAE and KSA, the e-Government payment transactions were published at a value of 4.7 billion AED and 2.8 billion SAR for 2012 and 2011 [Dalakian, 2012; Rorissa et al., 2010]. Estimates of G2G, G2B, and G2C can be facilitated by using the national ID card. The potential is huge.

- **IT Transformation:** Identity As A Service [IdAAS] will be the cornerstone of IT transformation across the region, enabling the migration of conventional IT systems to cloud computing. The value of this transformation, in pure economic

terms, is estimated at $5 billion globally in the next five years. Cloud services are on the rise in the Middle East. As per market estimates, cloud services are valued at a staggering $462 million in 2013 in the MENA region and are estimated to grow at 18% annually [Gartner, 2013]. The world market today is estimated at $131 billion [Whittake, 2013].