Towards Federated e-Identity Management across GCC – A Solution's framework

Ali M. Al-Khouri* and Malik Bechlaghem **

* Emirates Identity Authority, Abu Dhabi, UAE. (ali.alkhouri@emiratesid.ae)
** Logica Limited, London, UK. (malek.bechlaghem@logica.com)

Abstract

Many governments around the world have introduced modern Identity Management systems that utilize advanced and sophisticated technologies. The electronic identity (e-identity) card which is a product of such systems is considered an imperative and binding government-issued document for online and offline identification of individuals. There is a global trend in governments to replace conventional identity cards with the e-identity cards. The new card is seen to be an ideal building block for key strategic initiatives related to developing innovative business and service models. One of the initiatives introduced recently in GCC countries is to stimulate e-identity card applications to allow citizens of the different GCC member states to travel between their countries using the new card. A major challenge facing this GCC initiative is related to the interoperability of the different GCC systems. This article is written to explore this area in more detail. It also attempted to put forward an innovative solution framework to leverage and complement existing GCC infrastructures in order to address the need for cross validation of different identity cards issued by GCC member states.

Keywords: electronic identity, federated identity management, interoperability.

1. Introduction

For the past 10 years, governments around the world have increasingly shown interest in the deployment of advanced technological systems to establish and confirm identities of their population (Duncan and Al-Khouri, 2010; Al-Khouri, 2011). Modern national identity management systems include biometrics and smart crypto cards that provide strong capabilities to link the biographical data to the personal biological characteristics e.g., fingerprints, facial, iris, etc. The smart crypto card on the other hand, is a portable document with digitally embedded information and is considered as a token to tie and confirm a given legal identity. This is envisaged by many researchers and practitioners as a breakthrough enabler to revolutionizing public services and many other sectors (Duncan and Al-Khouri, 2010; Petrovic et al., 2003; Shaw, 2003; Shy, 2001). This is to say that electronic authentication and digital signature capabilities of such systems have the potential to contribute significantly to the effective and secure handling of identification requirements in the electronic world.

It is important to highlight here that government officials' and experts in the field have emphasized the need for a globally verifiable electronic identity systems in light of the ever increasing global migration (Noble, 2011). Global migration is considered as a key contemporary social phenomenon. Over the past 15 years, the number of people crossing borders in search of a better life has been rising steadily (BBC, 2011). At the start of the 21st Century, one in every 35 people is an international migrant. If they all lived in the same place, it would be the world's fifth-largest country. According to Research World (2008) more than 190 million people live outside their countries of birth and migrants comprise more than 15 percent of the population in over 50 countries. These numbers will grow as social, cultural, economic

and demographic factors intensify (BBC, 2011; Gannon, 2001). Figure 1 depicts an interesting global migration map with population movement patterns between countries. The green circles represent places where more people are coming in, and the orange circles show countries where more people are leaving.

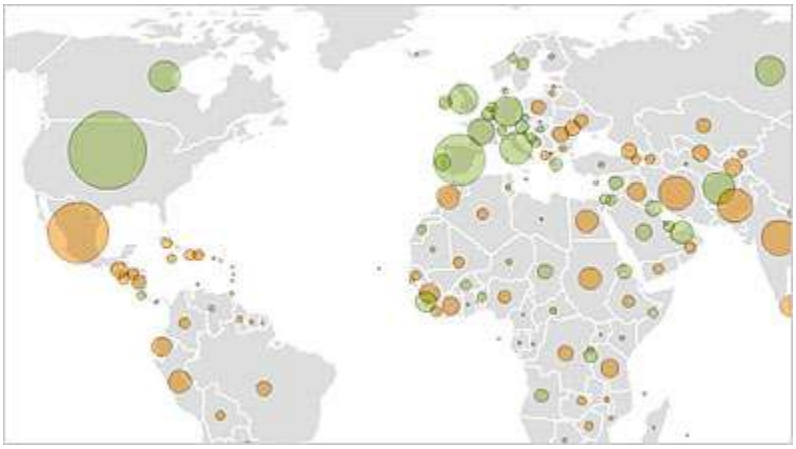

Figure 1: Global Migration
Source: http://southoftheborder.wordpress.com

There a trend in governments to develop a global system that can verify identities of migrant citizens using the same identity document issued by his or her home country. If countries were to issue work and residence permits in an e-identity format that satisfies common international standards, then it is argued that both the migrant workers and the countries themselves would benefit from improved efficiencies and security at the national and global level (Nobel, 2011).

The GCC countries in the Middle East have been among the first implementers of modern identity management systems (Al-Khouri, 2011b). Though with different readiness levels, many of the GCC countries have introduced electronic identity initiatives in public services in the form of e-government projects. One of the recent ambitious projects underway in GCC countries is to enable GCC citizens to cross GCC borders and access local services in member states (also referred to in this article as *domestic services*). In practice, there is a clear need for an interoperability framework to address e-identity requirements at a GCC level. It is the intention of the article to outline the associated challenges and delineate a proposed approach for cross validation of different identity cards issued by GCC member states.

The article is structured as follows. A short introduction is provided about GCC countries. The issue of interoperability is then discussed in detail. Next, the business objectives are presented, and the solution framework is explicated. Finally, the key components of the proposed approach are summarized, and the article is concluded.

2. GCC Countries

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

million people (GCC Portal, 2011). GCC citizens can usually travel freely between member states without the need for visas, and can use either their passports or national identity cards for border crossings.

All GCC countries have initiated a national smart identity card programs with a state of art technologies i.e., smart cards, biometrics, PKI. Although as less as 50% of the population has been enrolled to date for the new ID card, GCC countries are putting in place more strict procedures to ensure the registration of all the remaining population (Al-Khouri, 2011b). The majority of GCC states have developed with varying levels of complexity e-identity service models including Qatar, Saudi Arabia, United Arab Emirates, Oman, and Kuwait. They have recently introduced projects to accelerate the adoption of e-identity in their local societies mainly in the context of e-government.

Among these exciting projects, GCC countries are working to develop a common e-identity infrastructure that will enable the authentication of GCC citizens by any service provider at a member state e.g., border control, public services, etc. In light of the imminent requirement to enable e-identity on the GCC level, a major challenge upraises on the interoperability of these different silo systems. The next section explores this in more detail.

3. Interoperability

Plausibly, service providers cannot be expected to deal with the large number of different, manufacturer-dependent interfaces that are offered by smart card readers and smart card services (Vogt, 2004). Therefore, all GCC countries have developed middleware applications to enable interaction and access to their electronic identity cards. This middleware that sits "in the middle" between the user and service portal, is typically a set of multiple interacting layers of software that serve as a bridge between the card and the service providers to facilitate remote identification and authentication of the card and the cardholder (see also Mayes & Markantonakis, 2010; Rankl & Cox, 2007).

Let us consider a simple scenario to elaborate on some of the main interoperability issues. Citizen A of Member State X uses his electronic identity card to access an online public service offered by another Member State Y. In order to provide access to relevant services, the public service provider in Member State Y requires that the citizen uses his or her electronic identity card as a token for identification and authentication prior to be granted access to any particular service.

An ideal situation would be where irrespective of geographical boundaries within GCC countries, a GCC citizen can deal with any GCC online service provider using his e-identity card. Two possible application scenarios for card and cardholder validation can then be prominent in this GCC cross border scenarios:

- The cardholder, while residing in his home country attempts to perform an e-identity transaction on a foreign (another) GCC country online service provider;

- The cardholder is residing in a foreign (another) GCC member state and attempts to conduct an e-identity transaction to a foreign (another) online service provider.

These scenarios are envisaged to be arduous to endure as they bring about their own set of challenges as we listed them below.

- The identification process takes place typically through a unique identifier stored in the card and sometimes through a combination of attributes. The user's attributes can be stored in several files and in different formats.

- The authentication of the card and the cardholder requires that the domestic public service provider can interact with the backend infrastructure of the card issuer.

- Interacting with electronic identity cards requires the development of specific security modules to interact with the card on the client computer stations e.g., biometric verification, access to private key, etc.

- For the cardholder to perform an electronic transaction in a foreign (another) country, he oor she requires a client computer station equipped with all required pre-requisites of software and hardware.

4. Absence of a generic middleware

Smart card middleware is a software connecting smart cards in readers to applications via standardized or proprietary interfaces. In practice, where a public service provider attempts to communicate with a foreign (another) card, communication would not be possible if there is no common interface through which communication can take place between the foreign card and the domestic (local) public service provider.

While all GCC e-identity cards are ISO 7816 standard compliant, certain characteristics of the GCC cards are issuer or vendor specific. In particular, GCC cards have tailor developed and most of the times proprietary applications (i.e., applets). These applications have their own file layouts and formats that expose a dedicated set of APDUs (Application Protocol Data Units). In the context of smart cards, an application protocol data unit (APDU) is the communication unit between a smart card reader and a smart card itself.

Obviously, the first major issue facing the domestic public service providers is related to the absence of a middleware which can recognize a foreign card and interact with it. Standardization efforts would suffer from their high cost and the rapid change of market needs, and practically interoperability would heavily depend on the environment they are used in (Kehr et al., 2001).

4.1 Complexity of backend validations

Another major challenge faced by the domestic public service providers is related to *"backend validations"* required to complete the electronic transaction. Depending on the business service model defined by the domestic service provider, card or cardholder validation may involve different levels of technical integration. Let us look at each scenario individually.

- If card validation is required, a communication with the card issuer system is required in order to establish that an electronic identity is authentic and valid. Such a validation system has typically a proprietary web interface and requires the public domestic service provider to authenticate itself prior to providing access to the required validation service.

- If cardholder validation is required, a complete revocation path shall be built and validated including the extraction of various CRLs (Certificate Revocation List). While dealing with CRLs may be trivial nowadays, however validating a certification path requires trusting various CAs

(Certification Authority) from foreign countries. Establishing such trust relationships may not be as easy to achieve and to manage for a domestic online service provider standpoint.

Each card issuer would normally define a set of online validation services that will be offered to service providers. Some of the validation services would be insignificant from an integration viewpoint and would for example only require access to an LDAP to retrieve CRLs. Other validation services may require advanced and complex set ups and operations. To deal with a foreign card, domestic service provides need to set up and operate separate system to deal with card issuing authority in each country for which an electronic identity are to be supported. The interoperability of systems here could potentially be a stopper point considering the number of potential proprietary backend validations.

4.2 Dealing with on-card required secure messaging

In order to be resilient to sophisticated threat scenarios, electronic identity card issuers in GCC countries have invested heavily in state of the art security mechanisms to guarantee the security of their systems. In some GCC cards, even reading public data files require the initialization of a secure channel communication with the medium. See also Table 1. Setting such secure channels involves specific cryptographic protocols to secure the messaging as well as having shared cryptographic keys between the domestic service provider, foreign card issuer, and the card itself e.g., PIN verification process as part of a PKI authentication.

From an outset viewpoint, such string-based-security models may well enforce the overall security of the electronic identity systems and may show strong cases for proven resiliency to sophisticated threat scenarios. However, such complex security and trust models may induce fundamental developments and set up requirements on both the infrastructure and on the client side.

Since secure messaging is fundamental prerequisite to perform trusted operations with the card, particular hardware is normally required on client stations. Such hardware is typically referred to as Security Access Module (SAM). SAM is designed to act as a general cryptogram computation module or as a security authentication module for smart cards. It is used to interact securely with the electronic identity cards mainly to perform a mutual authentication to guarantee the authenticity of the terminal and the client card.

For a domestic service provider to offer its service to a foreign card, it may have to consider the deployment of SAM devices that can support secure messaging with different interfaces. The alternative to using SAM devices is to hardcode the *electronic identity issuer* attributes in the software which is an option that may be appropriate within a domestic scheme. However within a GCC interoperability framework, relying on keys in software may go against the interests of some political and technical policies.

Table 1: Security Enforcement on GCC ID cards

	What's in the chip?	How is security enforced?
Data containers	Public data including: • Cardholder data (name, unique identifgier, address, sponsor, ...etc) • Card data (card nuber, etc)	• Typically 100 % accurate information contained in files digitally signed by the eID issuer • Organizations can read the data and then validate the signature on to establish that the data is accurate. • In some cases, secure messaging with the eID is required in order to read public data files.
	Private data containers some owned by the eID issuer and some by other organizations, for example: • Family book, eHealth	• Secure messaging with the eID card si required in order for an external entity to conduct operations on the containmer
Authentication	PKI credentials typically contaimed within a PKI applet on the eID card: • Authentication key pair • Authentication digital certificate	• PIN code protection where the cardholder introduces his PIN in order to authorize the usage of his ID card for authentication • In some eID cases, conducting a secure messaging with the eID is a pre-requisite to perform PIN verification by th eeID • The service provider shall validate the authentication certificate prior to completing the authentication process with the cardholder
	Biometric application enabling the verification of holders with biometrics (fingerprints)	In most of the known cases, conducting secure messaging with the eID card is a pre-requisite to conducting biometric verification

4.3 Too many client dependencies

Another important challenge relates to the dependencies required on the client computer station in order for a cardholder to be able to use his e-identity card to access a foreign online public service. The middleware may not support the OS platform or browser available on the client station. In addition to that, the actual middleware itself or some of its software components may require to be pre-installed on the client computer station prior to any e-identity transaction to occur. Last but not least, our experience in GCC countries shows latency and slowness in enabling the download of web components (ActiveX, applet) of the e-identity middleware as part of service provider portal pages.

5. Vision and business objectives

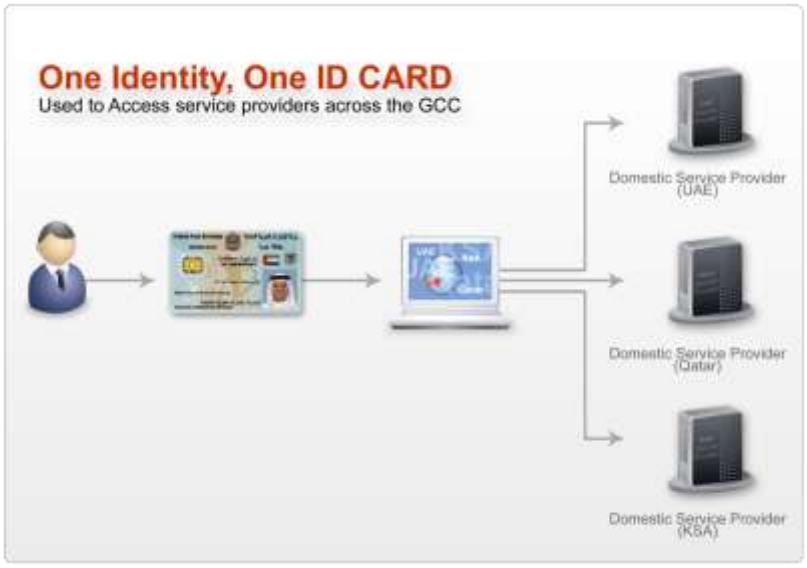

Figure 2: One Identity, one e-identity concept across GCC countries

Having clarified the problem areas, a number of assumptions were laid down to guide the development of the proposed framework and to define its direction. Figure 2 illustrates a graphical representation of the desired project outcome. The following elements were seen as key strategic objectives to implement the common e-identity infrastructure:

- Primarily, and in order for a GCC member state to engage in a common e-identity infrastructure initiative, it needs to have already invested in some form of e-identity validation and authentication services;
- Domestic (local) online services need to be accessible to mobile GCC citizens;
- Building a more citizen inclusive GCC community and enhancing the sense of GCC citizenship through supporting different domestic business service models;
- Improving and combating ID fraud and ID theft across GCC countries;
- Improving the effort related to preventing illegal work, illegal immigration and organized crime.

The proposed development framework is presented and discussed next.

6. The Solution framework – Federated eID management

6.1 Federated e-identity management - Conceptual view

It was envisaged that an interoperable solution would meet public and authorities' acceptance across GCC countries only if it meets some basic requirements as listed below:

- The solution framework shall take into consideration existing GCC members' independent e-identity schemes deployments and technical implementation rather than trying to replace them. GCC states have already invested heavily in building their e-identity infrastructures and it would be impractical to suggest an approach that induces fundamental changes on existing infrastructures.

- The solution framework shall not disturb domestic online service providers dealing with foreign e-identity cards. The best solution framework shifts the entire card transaction from the domestic service provider to the issuer of the foreign e-identity card. The domestic service provider would only need to redirect the cardholder to relevant online services offered by the e-identity issuer where card interaction is going to take place. At the end of an e-identity card transaction, the domestic online service provider receives an assertion from the eID issuer on the result of the card/cardholder transactions.

- Any proposed solution framework shall be user centric. While the user would be conducting transactions with a foreign service provider, the user should still have the perception that he or she is being validated by his own e-identity issuer. He would as such still be in control of the information that is revealed to the foreign online service provider. In addition to this, the solution framework shall guarantee user mobility by enabling e-identity card transactions with minimum dependencies on the client computer stations. The best solution framework shall guarantee that e-identity transactions on a client computer station have no dependencies apart from the availability of a smartcard reader.

- An interoperable solution framework shall support at minimum PKI authentication where the cardholder can be authenticated within any GCC member state using his e-identity card PKI capabilities. In addition, the solution framework shall offer the means for online public service providers to identify the cardholder via proper identifiers.

Looking at the above requirements, a Service Provider (or Identity Provider) implementation model is recommended where every e-identity scheme owner would make available e-identity validation services for online service provider within GCC countries. From a conceptual standpoint, this would enable the implementation of a federated e-identity infrastructure across the GCC countries where a domestic online service provider would redirect a cardholder to the e-identity validation services of the e-identity scheme owner as depicted in Figure 3.

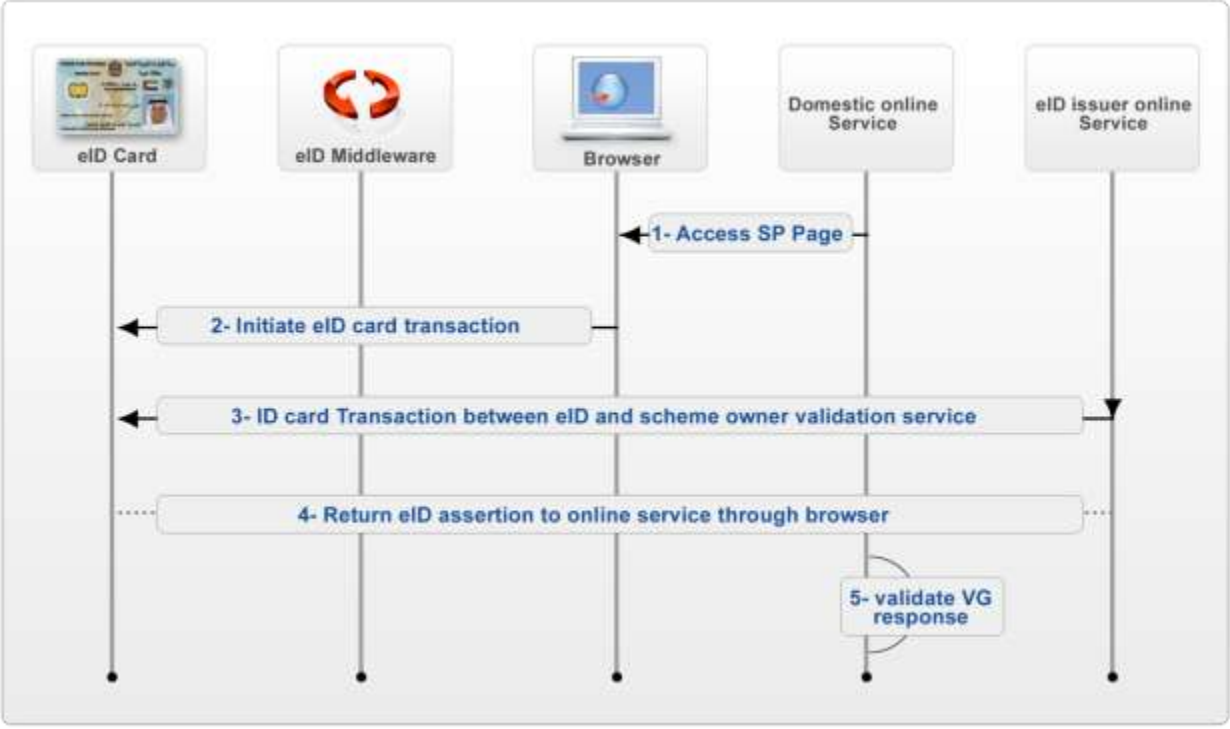

Figure 3: Federated e-identity management concept

The overall flow of an e-identity transaction in the proposed model is as follows:

1. The e-identity cardholder visits the website of the domestic online service provider. This would require the e-identity issuer middleware to be loaded on the end user browser.

2. The e-identity transaction is triggered from the browser using one of the middleware functions.

3. An end-to-end card transaction occurs between the e-identity card and the backend validation services of the e-identity scheme owner. This communication happens through the middleware and the service provider is not involved at this stage.

4. A validation response is returned to the browser. This response would be an assertion from the e-identity scheme owner validation service to confirm or reject the transaction. It indicates the status of the validation (success/failure) as well as relevant attributes such as cardholder unique identifier and card number. This request is typically signed and timestamped. The browser returns the response to the domestic online service provider.

5. The online service provider validates the response and provides or denies the access to the service accordingly.

The above approach allows implementing the concept of federated e-identity management between e-identity scheme owners within the GCC countries. The e-identity scheme owner acts as an identity provider exposing e-identity validation services that deal with all backend interactions such as interacting with the CA to perform certificate validation, accessing backend directory/database services for

card/cardholder validations, etc. Such approach enables each e-identity scheme owner to keep control of their existing backend infrastructure with minimum disturbance. On the other hand it guarantees minimum integration requirements on domestic online service providers as illustrated in the above figure where the actual card interaction is completely shifted from the service provider to the e-identity scheme owner. Last but not least, the desired level of security is met assuming that all e-identity cards and schemes offer at minimum two-factor authentication of the cardholder with PKI.

6.2 Federated eID management – Common eID interfaces

The concept of cross GCC e-identity federation services presented above addresses some important interoperability requirements. It guarantees minimum impact on e-identity scheme owners' backend infrastructure as well as low integration requirements for domestic online services providers.

In order to ensure a full interoperable solution, adequate formats must be agreed between e-identity scheme providers that would allow domestic service providers to support multiple e-identity schemes each having its own client middleware. At minimum e-identity scheme owners shall agree on a common e-identity client middleware as well as on common e-identity validation (assertion) mechanisms.

6.2.1 Common e-identity client middleware interface

While each e-identity scheme would have its own client middleware, a common interface shall be agreed between the e-identity scheme owners. Each e-identity scheme owner would provide an implementation of such interface so that a service provider would use the same interface regardless to which e-identity card is used.

The common middleware interface would specify a set of business functions such as:

- PKI Authenticate: functions that perform cardholder verification with PKI.
- Certificate validation: functions that perform the online validation of the cardholder certificate using standard protocols such as OCSP (Online Certificate Status Protocol).
- Card Status: a function that performs card status validation. It indicates whether the e-identity card is genuine and returns its status (revoked/active).
- Biometric verification: a function that performs cardholder verification with fingerprint validation. Match-Off-Card or Match-On-Card could be implemented by the e-identity scheme owner depending on the e-identity capabilities and technical constraints.

It would be at the discretion of the e-identity scheme owner to implement a subset or all of the interface functions. However, the minimum requirements for the e-identity scheme owner would be to offer an implementation of the cardholder verification with PKI as well as the card status validation. The following Figure 4 illustrates the components of the common e-identity middleware interface and how it could be used.

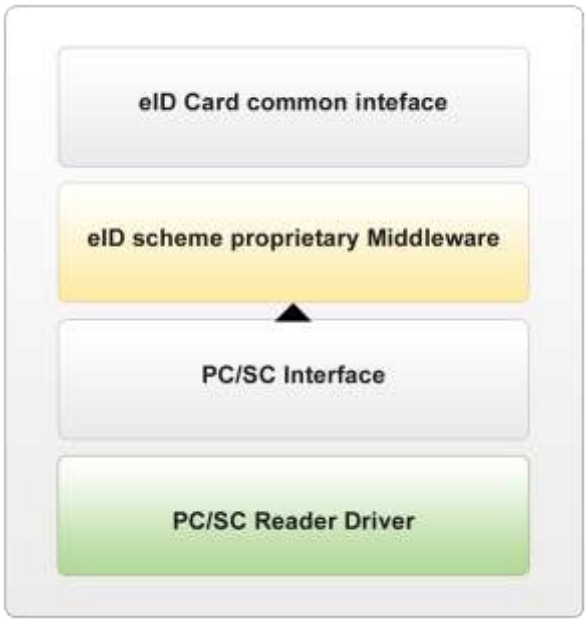

Figure 4: Common e-identity interface

6.2.2 Common eID validation assertion

The federated e-identity management concept relies on an e-identity validation assertion that is returned by the e-identity scheme owner validation server. An adequate format for the validation assertion shall be agreed by GCC e-identity scheme owners. It shall incorporate the minimum card and cardholder attributes in a manner that is clear and understandable by domestic online public service providers. The minimum attributes to be returned in the validation assertion should be as follows:

- Cardholder unique identifier: an identifier uniquely identifying the cardholder as read from the e-identity card;
- Card number: indicating the unique identifier of the e-identity being processed;
- Validation request type: indicating the type of request processed by the e-identity scheme owner validation service (card validation/cardholder verification with PKI, etc.);
- Validation status: indicating whether the validation succeeded of failed;
- Validation time: timestamp indicating the time at which the validation service performed the validation and created the validation assertion; and
- Validation period: duration (in seconds) of validation of the assertion.

The agreement on a common validation assertion format is considered to be a breakthrough capability for e-identity interoperability across the GCC countries. It guarantees a common format for the domestic online service providers for all GCC e-identity schemes.

6.3 Federated e-identity management – Formats and standards

6.3.1 Common e-identity client middleware interface

The common e-identity interface as described earlier in this article is implemented by the e-identity scheme owner on top of the proprietary/legacy e-identity middleware. It is assumed that the existing e-identity middleware covers online web scenarios and as such it integrates web components in the form of an ActiveX or Applet or both. Within a domestic scenario, these web components are used by domestic online service providers and embedded within its web/portal pages. Typically, functions of the web component (Activex/applet) are triggered through Javascript code that may be produced by the online web service provider.

An important principle of the federated e-identity management solution framework is that it takes into consideration existing e-identity schemes infrastructure and should induce as minimum impacts on these as possible. Therefore, an interesting approach to implement the e-identity common interface would be to use a common Javascript specification on top of the existing e-identity schemes web components (Activex/applet). This would mean that each e-identity scheme owner would provide a set of Javascript functions for the e-identity business function it exposes.

A simple scenario is presented to elaborate further the suggested e-identity middleware common interface. The e-identity scheme owner of GCC member state X has an Applet part of his existing e-identity middleware. The Applet exposes a PKI authentication function called "PKI authentication()". On the other hand, the eID scheme owner of another GCC member state Y has an Applet part of his existing e-identity middleware that exposes a PKI authentication function called "CardholderAuthenticate()". In order to illustrate the common e-identity interface concept, a domestic online service provider from a GCC member state Z is introduced. The e-identity common interface would include a set of Javascript functions to be implemented by each member state. For example, the PKI authentication Javascript function would be referred to as "PKI Authenticate". E-identity scheme owners from member X and Y would provide an implementation of this Javascript function "PKI Authenticate" that would be used by the domestic online service provider depending whether he or she is dealing with an e-identity from state X or Y. Figure 5 below illustrates this simple scenario.

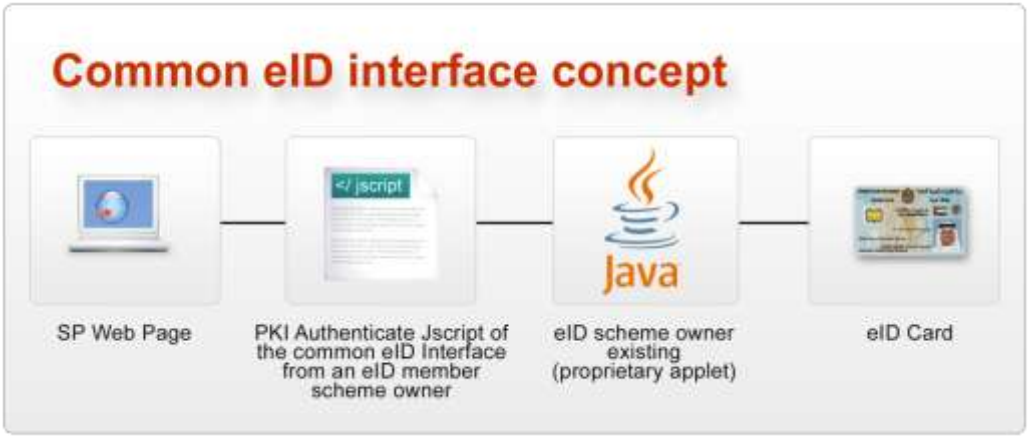

Figure 5: Common e-identity middleware interface implementation concept

It is noted that other options to implement a common e-identity middleware interface are possible and discussing them is not part of the scope of this article. It seems however that the approach suggested is quiet innovative and induce minor impacts on e-identity scheme owners existing investments in their e-identity front-end (client) and backend interfaces.

6.3.2 Common e-identity validation assertion

The federated e-identity management concept relies on an e-identity validation assertion that is returned by the e-identity scheme owner validation server to the domestic online service provider. The online service provider validates the assertion and completes the e-identity transaction.

The first observation here is that the assertion shall be of a common format and that there shall be means for the online service provider to validate the assertion that originates from a trusted e-identity scheme and that it has not been tampered with during its transport over the network. It is therefore suggested that the common e-identity validation assertion is a signed XML document that incorporates three types of data as follows:

- Data identifying the e-identity scheme member;
- Data identifying the e-identity card including cardholder unique identifier and e-identity card number;
- Data identifying the transaction status including validation status, validation timestamp and assertion validation period.

The federated e-identity management concept is recommended to implement a Service Provider – Identity Provider (SP – IdP) model based on SAML standard (Security *Security Assertion Markup Language*). This is considered to be a contemporary practice in the field of Identity Management. SAML is an XML-based open standard for exchanging authentication and authorization data between entities from different security domains. In particular, SAML is well suited for Service Provider (SP) that decides to offload the whole authentication process to a trusted Identity Provider (IdP) which is also referred to as SP-IdP model.

Looking at the federated e-identity management concept, the domestic online service provider acts as a Service Provider (SP) relying on an e-identity scheme owner to validate an e-identity card transaction and that is therefore acting as an IdP. Therefore, SAML appears to be an obvious option for the common e-identity validation assertion format. SAML assertion may allow the minimum data attributes for the e-identity validation assertion listed above.

As a conclusion, the e-identity validation assertion format should at least comply with SAML format. As a means to support service providers that have not invested in a SAML infrastructure, a dedicated XML schema (format) for the common e-identity validation assertion across GCC should be specified and used. Depending on the transaction context, the e-identity scheme owner validation service will return an e-identity validation assertion in either SAML or any other specified GCC format.

6.4 Federated eID management –eID scheme discovery in a mobile GCC environment

The discussion so far on the federated e-identity model can be summarized as follows:

- A common e-identity middleware is used by the domestic service provider to interact with a foreign e-identity card. This middleware is used as a bridge between the e-identity card and the target e-identity scheme owner validation services.

- The e-identity scheme owner validation services execute an end-to-end transaction with the e-identity card through the common e-identity middleware software components. It then responds with a proper e-identity validation assertion that can be conveyed to the service provider who will validate it.

The fundamental issue that is remaining is how the domestic service provider would recognize the e-identity card as coming from a specific GCC country member so that it can then call and use the proper e-identity middleware for that target e-identity scheme owner. There are three possible options to circumvent this challenge. All options assume that the e-identity card scheme can be identified using the e-identity ATR (Answer To Reset) that can be read from the e-identity. The possible options are discussed below.

1. In the 1st option, all the different common middlewares implementations from various Member States are put together as one module that can be installed on the service provider site. This can then be downloaded as part of the initial steps of the e-identity card transaction. Once the service provider page recognizes the origin of the e-identity card (i.e. its ATR), it can then invoke the proper e-identity common interface for the target eID scheme owner.

2. In the 2nd option, each e-identity scheme owner may build the support in its e-identity middleware for foreign GCC e-identity cards. This would result in a large e-identity middleware to be distributed by the e-identity scheme owner to online service providers within the same country. Once the service provider page recognizes the origin of the e-identity card (i.e. its ATR), it can then invoke the proper e-identity function calls from the e-identity middleware augmented with the support of all e-identity schemes.

3. In the 3rd option, the domestic service provider relies on a discovery service that is part of the overall federated e-identity management solution. The discovery service is used to discover where the e-identity card is originating. It then has the capability to download in real time the e-identity middleware of the target e-identity scheme. Once loaded on the browser, the target scheme e-identity middleware is used to initiate the relevant e-identity transaction with the e-identity scheme owner validation services.

Options 1 and 2 seem to be impractical to implement. They go against one of the main objectives of GCC interoperability which is ensuring minimal impacts on existing e-identity schemes. Moreover, they would involve large e-identity middleware components that impact end user experience and the overall e-identity transaction performance.

The 3rd option involves a new building block for the federated e-identity management solution framework which is the e-identity discovery service. This option copes with all interoperability requirements and is therefore the option recommended to be part of the federated e-identity management solution framework. Figure 6 illustrates how the discovery service is used.

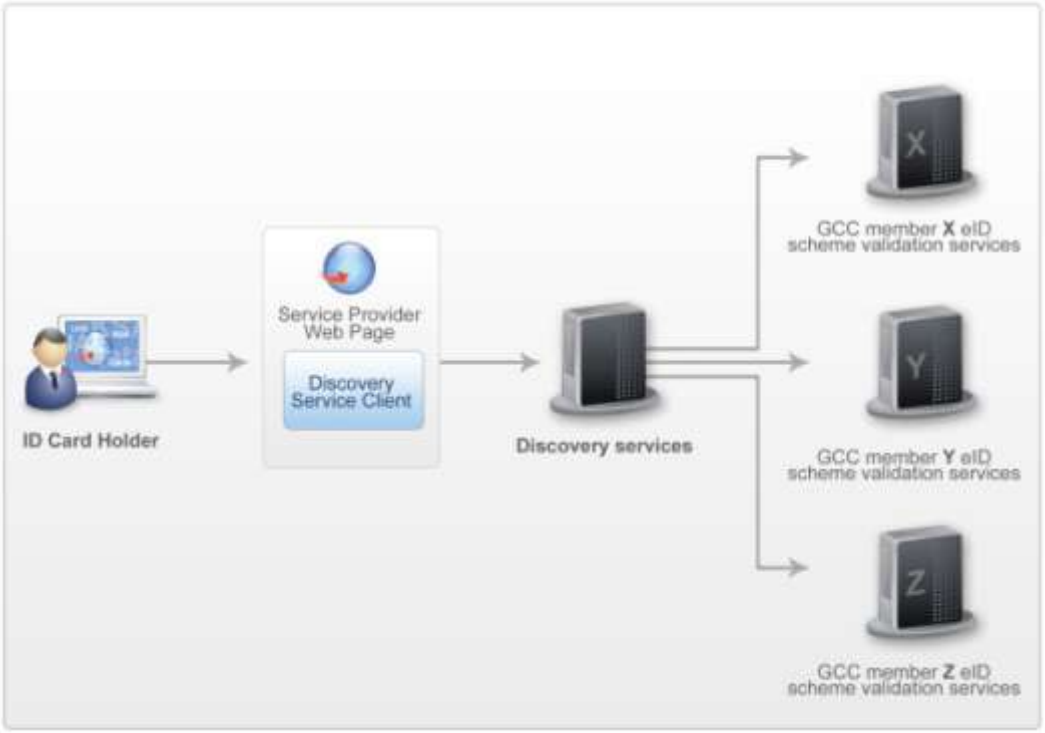

Figure 6: e-identity discovery service

The discovery service would provide a lightweight web component (Applet/active X) that is loaded with the domestic service provider page visited by the e-identity cardholder. This web component will then read the card ATR through a standard APDU command.

The discovery service web component will then query its discovery service that is configured with details of each GCC member state e-identity scheme owner. The discovery service will query a dedicated service from the target e-identity scheme owner validation services that will return data to be used by the discovery web component to load the e-identity middleware. This data consist mostly in HTML tags and file paths that would enable the discovery service web component to download the target e-identity scheme owner e-identity middleware.

The discovery service web component loads the target e-identity scheme middleware that will then take control of the card transaction. Figure 7 below illustrates the discovery service web component and e-identity scheme owner middleware.

Figure 7:Discovery service and eID scheme owner middleware

Depending on the agreements between GCC member states, there could be one discovery service across GCC with its mirror site. These would be used by service providers from all GCC countries. Another approach would be to have one discovery service within each GCC country that could be hosted within the domestic e-identity scheme owner infrastructure. Opting for one of the options would be dependent on the logistical and political reasons but implementing either option is equally possible.

7. Solution's building blocks and functional summary

The earlier sections of this article attempted to present the proposed federated e-identity management framework, its guiding principles and an overview of the building blocks of the approach. The following components were introduced as important building blocks and their role and potential implementation were discussed:

1. **e-Identity Validation Gateway (VG)**: a Server exposing the e-identity scheme owner card validation services as web services available over the cloud. At minimum, the VG shall expose a reliable cardholder authentication method using his or her e-identity. The recommended minimum services to expose on the e-identity VG are as follows:

    - PKI Authentication: a service that interacts with the e-identity card and performs an end-to-end PKI authentication protocol. This involves PIN verification, challenge-response protocol certificate validation using CRLs or OCSP depending on the local scheme PKI infrastructure.

    - Verify Card Status: a service that interacts with the e-identity card and performs card validation. It indicates whether the card is genuine and returns its status (revoked/active).

    - Biometric verification: a function that conducts cardholder verification with 1-to-1 fingerprint matching to relevant ISO/IEC 7816 biometric standards.

2. **e-identity discovery service**: a server dedicated to discovering the target e-identity VG to query the client terminal in order to execute a specific card transaction.

3. **e-identity common middleware**: set of software libraries exposing the e-identity card business functions to service providers. In a web environment, the e-identity common middleware consists in the e-identity VG applet which interacts with the VG in order to conduct an end to end e-identity card transaction.

Figure 8 illustrates the above three components that are jointly involved in an eID card transaction.

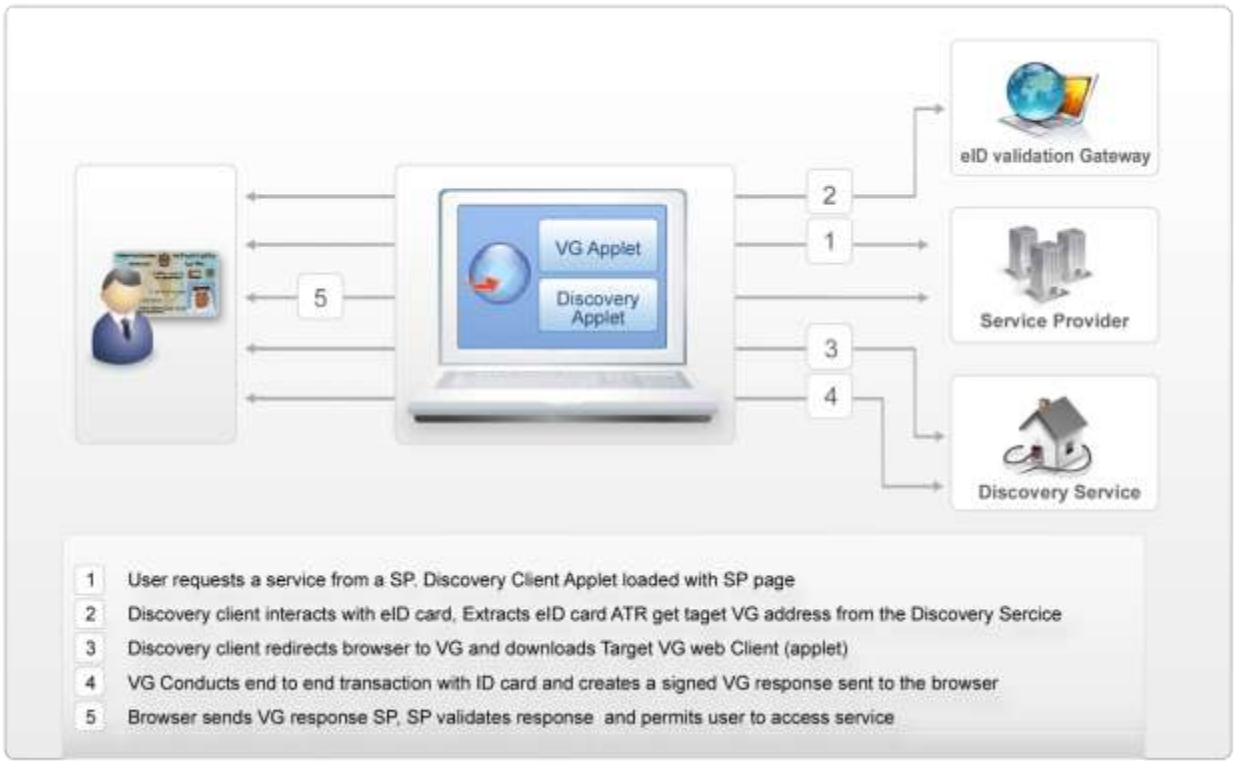

Figure 8: Federated eID management solution framework summary

8. Conclusion

Electronic Identity (e-identity) cards are being issued across the world. These are seen as enablers for secure online services in general and in particular as the enabler of smart societies where the citizen is closer to his or her local authorities. Electronic identity cards are also seen to be the ideal tool to build a more inclusive and secure communities.

GCC countries have initiated multiple projects related to advanced applications development of their e-identity schemes. GCC countries are currently working on developing a unified e-identity infrastructure to enable identification and authentication of GCC citizens at any of the GCC member states. This raises serious interoperability issues due to the different and complex infrastructure setups at each member state and would likely challenge such a project.

This article attempted to outline the challenges related to offering cross GCC e-identity transactions. An innovative solution framework has been presented that leverages and complements existing investments in e-identity schemes and infrastructure. The framework referred to in this article as the federated e-

identity management relies primarily on three key enablers: (1) domestic Validation Gateway (VG) put in place by domestic eID scheme owners; (2) Discovery Service that enables real time discovery of a target eID scheme owner by a domestic online service provider, and (3) a common Middleware to enable interaction with the VG and end-to-end transaction.

We do note that other options to implement a common e-identity middleware interface were possible however, discussing these were not part of the scope of this article. Nonetheless, the suggested overall approach is believed to be quiet innovative and induce minor impacts on e-identity scheme owners existing investments in their e-identity front-end (client) and backend interfaces.

The proposed framework supports the concept of coherent distributed and interoperable architectures development, which in turn should enable and simplify complex distributed applications. The approach should enable service providers to securely verify, certify and manage identification and access of citizens seeking physical or logical access.

The proposed approach was at the discussion stage between the GCC member states at the time of writing this article. Once agreed on the underlying guiding principles a better understanding will evolve of the roadmap to implement the solution across GCC. The next steps should include detailed GCC e-identity schemes survey, development of Validation Gateway and Discovery Service Specifications, and the launch of a pilot implementation.

References

- Al-Khouri, A.M. (2010) "Supporting e-Government," Journal of E-Government Studies and Best Practices, Vol. 2010. pp.1-9.
- 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.
- Al-Khouri, A.M. (2011b) Rethinking Enrolment in Identity Schemes, International Journal of Engineering Science and Technology, Vol. 3, No. 2, pp. 912-925.
- BBC (2011) Migration Boom [Online]. Available from: http://news.bbc.co.uk/2/shared/spl/hi/world/04/migration/html/migration_boom.stm
- Gannon, J.C.(2001) 2001 Growing Global Migration and Its Implications for the United States.
- GCC Portal: http://www.gcc-sg.org/eng/index.html)
- Kehr, R., Rohs, M. and Vogt, H. (2000) "Issues in Smartcard Middleware." In: Attali, I. and Jensen, T. (Eds.): Java on Smart Cards: Programming and Security. LNCS, Vol. 2041, Springer-Verlag, pp. 90-97.
- Mayes, K. and Markantonakis, K. (Eds.) (2010) Smart Cards, Tokens, Security and Applications. Springer.
- Noble, R.K. (2011) Interpol chief calls for global electronic identity card system. Available from: http://www.net-security.org/secworld.php?id=10860.
- Petrovic, O., Ksela, M., Fallenbock, M., & Kittl, C. (2003) Trust in network economy. New York: Springer.

- Rankl, W. and Cox, K. (2007) Smart Card Applications: Design models for using and programming smart cards. Wiley.
- Research World (2008) More than 190 million people live outside their country of birth. [Online]. Available from: www.esomar.org/uploads/pdf/.../RW0807_MakeYourselfAtHome.pdf
- Shaw, M. (2006) Commerce and the digital economy. Armonk, NY: Sharpe.
- Shy, O. (2001) The economics of network industries. New York: Cambridge University Press.
- Vogt, H., Rohs, M. and Kilian-Kehr, R. (2004) Middleware for Communications. John Wiley & Sons.

About the Authors

Dr. Ali M. Al-Khouri

Dr. Al-Khouri is the Director General of Emirates Identity Authority, in the United Arab Emirates. He is also the Head of the UAE Technical Committee representing the UAE government in the GCC ID Cards Steering Committee. He holds an Engineering Doctorate from Warwick University in UK in the field of Large Scale and Strategic Program Management in Public Sector. He is an active researcher in the field of management practices, and advanced implementations of modern technologies.

Malik Bechlaghem

Malek Bechlaghem is a senior PKI specialist at Logica. He has 15 years in designing and implementing PKI and e-Identity projects. His research interests are around the design of zero-footprint PKI and e-Identity frameworks focusing on Identity Federation. He also has a heritage of practical design and implementation of large programs involving technologies like PKI, Access Management and SSO, and Strong 2-Factor Authentication. His mission and ambition are to contribute to the deployment of added value e-ID and PKI usage in public and private sectors.