International Scholars Journals

International Journal of Banking, Economics and Finance ISSN: 8201-4728 Vol. 3 (1), pp. 001-011, January, 2019. Available online at www.internationalscholarsjournals.org © International Scholars Journals

Full Length Research Paper

Biometrics and identity management for homeland security applications in Saudi Arabia

Bilal Khan[1], Muhammad Khurram Khan[1]* and Khaled S. Alghathbar[1,2]

[1]Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia.
[2]College of Computer and Information Sciences, Department of Information Systems, King Saud University, Riyadh, Saudi Arabia.

Accepted 14 October, 2018

Identity is the collection of all characteristics related to an entity, be it a person, enterprise or an object. Identities allow entities to be distinguished from each other. This is what makes an identity a key component in several administrative, social and economic transactions. Identity management is important for government, communication, commerce and just about any significant societal activity. Government identity management systems are not usually static and are frequently changed with the change of time and situation. A flexible approach is needed towards the addition of new features in identity management systems. This paper analyzes different identity cards used for different purposes in the Kingdom of Saudi Arabia as a case study followed by their deficiencies. Finally, a biometric based identity management system is proposed referring to the successful and extendible identity management system of developed countries.

Key words: Biometrics, security, privacy, identity management, e-ID

INTRODUCTION

It is expected today that an individual who wants to authenticate himself for a service must have a token and/or password for example identity card, ATM card, driving license, health card etc. Carrying different cards and remembering passwords for different services is a significant issue for individuals and organizations. A vast expansion of identification practices has been observed in citizen -government relationships. These relationships are in the form of social citizenship rights, benefits, education and public health. Furthermore, an increasingly mobile society is also a factor in the expansion of identification practices. The provision of public services is based upon the assessment of paper based request and the final decision made by public officer. Thereby, turning the public service providing organizations into large repositories of stored paper records. In such system

the process of claiming and obtaining benefits is not only time consuming but also costs more and increases the possibility of identity fraud.

A secure and effective identity management system plays an important role in the successful deployment of e-government scheme. This also enables secure and reliable access to online services, hence reducing the cost and improving the quality of the delivered services. In addition, preventing illegitimate use of identification and authentication credentials helps governments in defending national security by combating terrorism, illegal immigration and other criminal activities.

To make the identity management system even more secure and reliable for authentication, biometrics data such as fingerprint are integrated in the national ID card. Biometric based identity management systems are essential to the effective operation of any organi-zational information systems that utilize personal data.

Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification (Ratha, 2007). Biometric based authentication and identification systems are the new

*Corresponding author. E-mail: mkhurram@ksu.edu.sa.

solutions to address the issues of security and privacy. It is being used as the authentication method these days with increasingly high demand for reliable security. The types of biometrics used are fingerprint, face, hand geometry, iris, retina, keystroke, gait, and voice recognition. Using biometrics for identification restrict individuals from access to physical spaces and electronic services. In addition, it stops the potential fraudsters to take more than one identities. Physiological biometrics have being largely used for authentication purposes, however, Moskovitch et al. (2009) propose the use of behavioral biometrics, i.e., keystroke and mouse dynamics to authenticate to devices and websites (Moskovitch et al., 2009).

From the last few years the use of biometric applications is growing rapidly. As shown in Figure 1a, a major part of governmental applications use biometric technology (http://biometrics.org/bc2009/presentations/tuesday/Kwon%20MR%2014%20Tue%20345%20PM%20%20400%20PM.pdf). A 39.3% of the whole biometric applications are used for civil ID applications followed by 24.6% which is used in criminal ID. It means that the combine share of civil ID and criminal ID that uses biometrics is more than 60% of the market volume. Fingerprint and AFIS recognition technologies dominate on other biometrics recognition technologies used in biometric applications (http://biometrics.org/bc2009/presentations/tuesday/Kwon%20MR%2014%20Tue%20345%20PM%20%20400%20PM.pdf). Fingerprint shares the market volume by 36% followed by AFIS which is 38% of the whole biometrics used. The combine share of fingerprint and AFIS is 2/3 of the whole biometrics used as shown in Figure 1b.

A basic biometric authentication system consists of five main components (Anil et al., 2008). These are: sensor, feature extractor, fingerprint/template database, and matcher and decision module (Figure 2). The function of the sensor is to scan the biometric trait of the user. The function of the feature extraction module is to extract the feature set from the scanned biometric trait. This feature set is then stored into the template database. The matcher module takes two inputs, i.e., feature set from the template database and feature set of the user who wants to authenticate himself and compares the similarity between the two sets. The last module, i.e., the decision module makes the decision about the matching of the two feature sets.

Basically there are two factors in measuring the accuracy of an efficient biometric system:

1. False reject rate (FRR): FRR is the rate, usually in percentage at which a true authentic person is rejected during the process of authentication as unidentified or unverified by a biometric system.
2. False accept rate (FAR): FAR is the opposite of FRR.

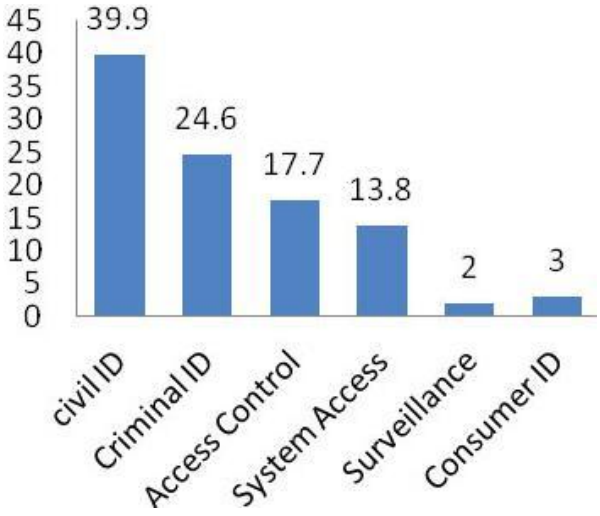

Figure 1a. Market volume by application (%) in 2009.

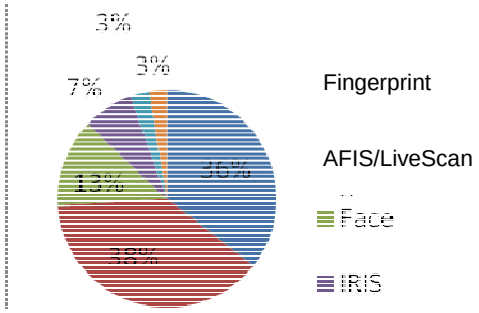

Figure 1b. Market volume by biometric technology (%) in 2010.

FAR is also measured in percentage. This is the rate at which an un-enrolled or an imposter person is accepted as a true authentic by a biometric system.

Related work

The United Kingdom recently launched identity card scheme which has been analyzed by Shaikh and Rabaiotti (2009). They approach the scheme from the perspective of high volume public deployment and described a trade-off triangle model. They have found that there is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other (Shaikh and Rabaiotti 2009).

The requirements, design and application scenario of The Netherland's biometric passport has been discussed by Schouten and Jacobs (2009). They con-cluded that the success of a biometric system highly

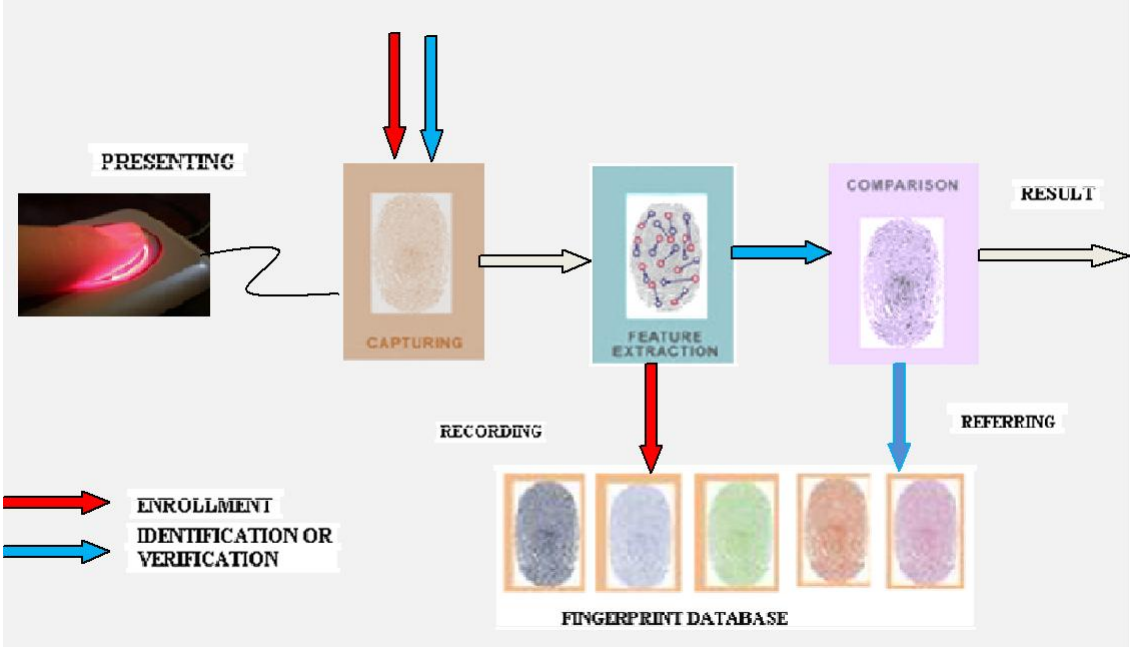

Figure 2. A basic biometric authentication system

depends on its security and design.

The development and deployment phase of Belgium e-ID card has been discussed by Marein and Audenhove (2010). It has been argued that the pre-existence of national register was one of the factors that have helped in the development of the Belgium e-ID card. So far eight million cards have been provided to Belgium citizens mentioning the process was smooth and straightforward (Marein and Audenhove, 2010).

A discussion on security and design of the Malaysian identity card, i.e., Mykad has been done by Raphael et al. (2003). Mykad integrates ID card, driving license, passport and ATM. As Mykad is used for various sensitive purposes, therefore, it is stated that its security features should be analyzed before it is deployed.

It is important to consider the perceptions and responses of end users while developing and analyzing biometric based identity management systems (Laurie et al., 2007). Surveys and interviews have been conducted to understand the employee's perception on the use of biometric authentication system in the Kingdom of Saudi Arabia (Alhussain and Drew, 2009). It has been found that there is a significant resistance from employees in implementing a biometric based identification and authentication system. They finally suggested that awareness programs should be introduced before the implementation of such systems in organizations.

Gronlund has described the previous identity management and the current e-ID system in Sweden (Gronlund, 2010) His work is based on the official policy documents, technical documentation, comments from the government and other experts. It is concluded that the proposal presented by e-delegation in October 2009 will be a major step towards the successful implementation of e-ID system (Gronlund, 2010).

Emphasizing on the need for identity management system, Al Tawil, the former Director General of national information center Saudi Arabia, said, "providing a secure authenticated identity for every citizen will help us provide better, faster and more reliable secure governmental and non-governmental services and thereby enhance global security" (http://www.ameinfo.com/179613.html).

Although identity management has been given a strong attention in the research community but the emphasis was mostly on the issues of its implementation in European and other countries (Shaikh and Rabaiotti 2009; Schouten and Jacobs 2009; Raphael et al., 2003; Marien and Audenhove, 2010; Gronlund 2010). On the other hand, only one attempt has been made to address biometric based identity authentication issues in the kingdom of Saudi Arabia (Alhussain and Drew, 2009). Therefore, we consider our work a significant progress in the identity management system in the Kingdom of Saudi Arabia.

METHODOLOGY

To find out the best solution for Saudi Arabia, we explored the e-ID systems of different countries and did a comparative study.

Many of these countries are from Europe, which are believed to be in the advanced level with respect to e-ID systems imple-mentation and research. The study also included countries other than European, e.g. UK, Malaysia, Japan, Korea and Singapore.

Regarding the use of identifiers to avail different services under the e-government, the following three types are typically used (Modinis, 2006);

Type 1: all public sectors use same identifier. Type 1 is also called *Flat model.*
Type 2: different public sectors use different identifier, derived from the base identifier. Type 2 is also called *Sector Specific model*.

Type 3: every public sector uses its own separate identifier. Type 3 is also called *Separate model*.

Every model has its own benefits and drawbacks in terms of security, privacy and usability. In this paper, we present different tokens used by individuals in the Kingdom and their purposes and the technology they use. Moreover, some features some features of the European electronic identity management systems will be highlighted. The integration of such features in the e-ID system makes the system unsecure and complex. It has been found that such features are unnecessary for the Kingdom and the elimination of those might facilitate the implementation of e-ID card system and increase the security of the electronic identity management system.

IDENTITY MANAGEMENT WITH BIOMETRICS

National identity is a set of attributes defined by a state to create and assess the citizenship of individuals in most cases registered in a national citizen's register and proved by a national ID card (Kubicek and Noack, 2008) . National ID card could be used by the nationals of the country as a proof of age, authentication of right to vote, public health programs, and in addition, can provide privacy by granting control over data. However, some countries use national ID cards as a travel document; for example, EU nationals can travel within EU using national ID card (Gronlund, 2010). Apart from national ID card, EU uses e-passport compliant with the ICAO (International civil aviation organization) standards to travel outside EU. (ICAO), an agency runs under the United Nations (UN) is responsible for setting international passport standards. The number of the ICAO contracting states is 190 and Saudi Arabia
is also one of them
(http://www.icao.int/cgi/statesDB4.pl?en)

The ICAO has specified facial images as standard to be used in e-passports, whereas the use of fingerprints and iris biometrics is optional (http://www2.icao.int/en/mrtd/Pages/default.aspx). Passport is basically a travel document, which is also used as an identity document while abroad.

The use of biometric technology increases the security of the e -ID system. From the study, it is found that while some countries are considering the inclusion of biometric technologies into their e-ID systems, e.g., France and Spain, others consider the use of biometric technology as the invasion of privacy, e.g., UK. In Saudi Arabia, the reason for the user's negative perception on the use of biometrics in the e- ID system, if implemented, will not be privacy rather the digital and cultural gap (Alhussain and Drew, 2009).

PRIVACY AND SECURITY PROBLEMS RELATED TO ID THEFT

Identity theft is a crime of obtaining another person's personal information for financial gains by posing as that person (http://www.electronic-identity.org/what-is-identity-theft). Identity theft resource center (ITRC) Moskovitch et al., (2009) has categorized identity theft from the consumer point of view into four categories namely financial identity theft, criminal identity theft, and identity cloning, commercial or business identity theft. The main causes of identity theft are when the individual lose control over his identity or when the information about the individual is already available at different places. A name, date of birth and photograph is enough for a potential criminal to commit identity theft and build a fake identity.

Identity fraud continued to rise in 2009 (www.javelinstrategy.com/research/Brochure-170). According to Javelin 2010 identity theft report, the number of identity theft victims and the amount of fraud increased by 12 and 12.5% respectively, the highest rate ever issued by the company.

A recent incident of identity theft, which shocked the world, is the stealing of the identities of British, European and Australian citizens by a group of killers (http://www.allaboutidentity.com/content/eu-condemns-identity-theft-dubai-assassination). The group used the forged passports in the assassination of a senior militant in Dubai. It is worth mentioning that all the passports forged were of different countries and must have different security mechanisms implemented. It can be said that the current security measures in e-passports are not adequate and poses a potential challenge for security experts. However, building a robust identity system with data protection act can provide security and privacy to individuals.

EXISTING ID SYSTEM IN SAUDI ARABIA

This section illustrates the various identity tokens used in Saudi Arabia, their attributes and the purposes they are used for.

National ID card

The Kingdom of Saudi Arabia is using a wallet sized national identity card for its citizens that have replaced Civil Affairs Card. The card is using smartcard technology provided by Lasercard Corporation

Figure 3a. Front of National ID Card of Saudi Arabia (http://www.lasercard.com/files/casestudies/LaserCard_case_study_Saudi_Arabia.pdf).

Figure 3b. Back of National ID card ((http://www.lasercard.com/files/casestudies/LaserCard_case_study_Saudi_Arabia.pdf).

(http://www.allbusiness.com/law-legal-system/immigration-law-national-identity-cards/11746173-1.html). The ID card contains two biometric identifiers, i.e., fingerprint and facial photograph. The front of the card carries the photo of its holder, in addition to full name, number, expiry date, address, and date of birth and national ID number of the card holder (Figure 3(a)). While the back of the card features optical memory security and a contact chip (http://www.lasercard.com/files/casestudies/LaserCard_case_study_Saudi_Arabia.pdf) as shown in Figure 3(b). All the details provided on the card are in Arabic language.

According to Lasercard Corporation, the digital security of the card has never been compromised and is durable for 10 years ((http://www.lasercard.com/files/casestudies/LaserCard_case_study_Saudi _Arabia.pdf). The national ID card makes the individual for secure personal identification and to achieve the benefits as a citizen. The authorities say that the new card protects cardholder against identity theft and fraud. In addition, this card is also used as a travel document to travel to GCC (Gulf Cooperation Council) countries without the need for visa on the passport.

However, the new card can only be used for a few government services and is unable to authenticate an individual to perform bank transactions and cannot be used for online services.

E-Gate card

E-gate card is a facility developed by the ministry of interior, Kingdom of Saudi Arabia under the e-government initiative (http://www.moi.gov.sa/wps/portal/; http://www1.elm.com.sa/Portal/En/Topics/Services/eGate/default.htm). The card carries the name, photograph, and date of birth, place of birth, validity of the card and biometric information of the card holder.

The card is used by those Saudi nationals who frequently travel using airport. To obtain e-gate card, the individual has to enroll for the e-gate card by registering its fingerprint, facial biometrics and other identification details. Figure 4a shows the enrolment for e-gate card, whereas Figure 4b shows authentication before departure http://www1.elm.com.sa/Portal/En/Topics/Services/eGate/default.htm. The primary advantage of this card is to reduce the queuing time and efforts during arrival or departure in airports. The holder of this card does not have to interact with the human immigration official, rather to use an automated terminal during the arrival and departure process (Figure 4b). A similar system has been deployed between USA and Canada for the citizens of both countries, who frequently travel (Shaikh and Rabaiotti, 2009; http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/) . Fingerprints and iris images are used as biometric identifiers by the system.

Health card

Health card in the kingdom of Saudi Arabia is a simple plastic card. The card carries the name, date of birth, nationality, gender, national ID number and six digit patient number of its holder. In contrast to other identity cards, the health card does not have the photograph of its holder and does not mention the dates of validity and expiry. It is worth mentioning that the card does not store any health information about the cardholder. Moreover, each hospital has its own health card so the health card of one hospital is not

Figure 4(a). Enrollment for e-gate card (http://www1.elm.com.sa/Portal/En/Topics/Services/eGate/default.htm).

Figure 4(b). Authentication and departure (http://www1.elm.com.sa/Portal/En/Topics/Services/eGate/default.htm).

Figure 5. Health card in Saudi Arabia.

acceptable in other hospital. Figure 5 shows the health card used in one of the hospital.

Health insurance card

Apart from the health card, there is a health insurance card in Saudi Arabia. The card uses optical memory technology. The health insurance card carries the name, year of birth, scheme, membership number and the validity of the card. Although, it is mentioned on the card that the card is only valid for the named insured person, however, the cardholder is not authenticated in practice while receiving the health service.

Driving license card

Saudi Arabian driving license card uses optical memory card technology. The card is issued by the traffic department, ministry of interior. The card bears the photograph, name, date of birth, place of birth, driving license number, date of expiry, in addition to blood group, restriction and phone number. The card is issued to only 18 years old or over and is valid for 5 years.

Discussion

Problems of multiple identity management increase with the increase in the interaction with public sector services. Multiple identity cards are not only inconvenient but also costly for both individuals and government agencies. Hence one embedded identification management system is needed.

Table 1 shows countries with electronic ID cards, the attributes they have and the purposes they are used for. Many countries are reluctant to adopt e-ID system as the addition of extra features, i.e., e- voting, tax-on-web, and citizenship for foreigners, not only makes it technically unfeasible but also insecure. Before we discuss the motives and driving forces behind the implementation and adoption of e-ID card in Saudi Arabia, it will be beneficial to have a brief overview of the successful biometric based electronic identity management system in Malaysia.

Malaysian government has introduced multipurpose smart identification card with an embedded chip in September 2001 and was named 'Mykad' (http://www.rogerclarke.com/DV/MyKad.html). Mykad incorporates the national identity card, driving license, health information, ATM access as well as PKI feature for online transaction.

Mykad carries the name, date of birth, place of birth, photograph of the holder in addition to date of validity and date of expiry of the card, whereas the chip holds information on race and religion, biometric information, i.e., thumbprint. Health information in Mykad is stored in the form of blood group, allergies etc.

Personal information on Mykad can be accessed on

Table 1. The information about e-ID cards of different countries collected from different websites.

S/N	Country	ID	Attributes	Uses
1	Austria	E-ID (2004)	Photograph, name, id code, date and place of birth, sex, card number and validity.	e-Government and e-services.
2	Belgium	E-ID (2003)	Photograph, place of birth, date of birth, sex , address, issuing authority, digital signature.	e-Services, e-portal, online tax declaration, home banking.
3	Estonia	E-ID Card (2002)	Name, national id code, date and place of birth, sex, card number and validity.	Official identity document, European travel document, e-services, e-ticketing
4	Finland	E-ID	Photograph, name, id code, date and place of birth, sex, card number and validity.	Tax services, health insurance, social security services.
5	France	E-ID (2006)	Personal data.	e-Government and e-services
6	Slovenia	E-ID (2002)	Name, place and date of birth, sex, validity.	e-Government and e-services
7	Spain	E-ID (2004)	Photograph, place of birth, date of birth, sex, address, biometric data, handwritten signature.	e-Government , e-banking, e-services
8	Hong Kong	ID (2003)	Embedded microchip, photograph, name, birth date, fingerprints.	Travel document, immigration.
9	Malaysia	Mykad	Photograph, fingerprint, name, date and place of birth, card number.	ID card, driving license, travel document, e-cash, touch n go
10	Pakistan	NIC	Photograph, name, date and place of birth, address, biometric data, card number.	Government procedures, commercial transactions.
11	Singapore	NRIC	Photograph, name, race, date of birth, sex, country of birth, card number, issue date and finger print.	Government procedures, commercial transactions.

government kiosks and offices after the authentication of their fingerprints (http://www3.austlii.edu.au/au/journals/MULR/2004/15 html). So far, no vulnerability in MyKad has been notified in publications except Raphael et al. (2003), who pointed out the problems of the limited memory capacity and security weaknesses. Due to the advancement in cryptographic techniques and memory technologies, these issues have been solved. Particularly, the use of smart card has avoided the problem of limited storage memory. In some countries providing e-government services securely to native citizens only is not acceptable, rather the focus is shifted on the interoperability in the design of e-ID system, which is an open issue in European Union (https://www.cosic.esat.kuleuven.be/modinisidm/twiki/bin/view.cgi/Main/WebHome).

Driving forces for the proposed e-ID card

In case of Saudi Arabia there are basically three driving forces behind the proposed e- ID card system, these are e-government, low cost of implementation and mobile society (Figure 6).

With the growth in the number of services provided by e-government, the need for reliable, secure and efficient electronic identity cards becomes more and more. E-government refers to the use of information and communication technologies, and particularly the internet, as a tool to achieve better government (http://www.oecd.org/dataoecd/60/60/2502539.pdf). The Saudi government launched its e-government program in 2005 (http://www.yesser.gov.sa/english/default.asp). The electronic government or e-government project serves

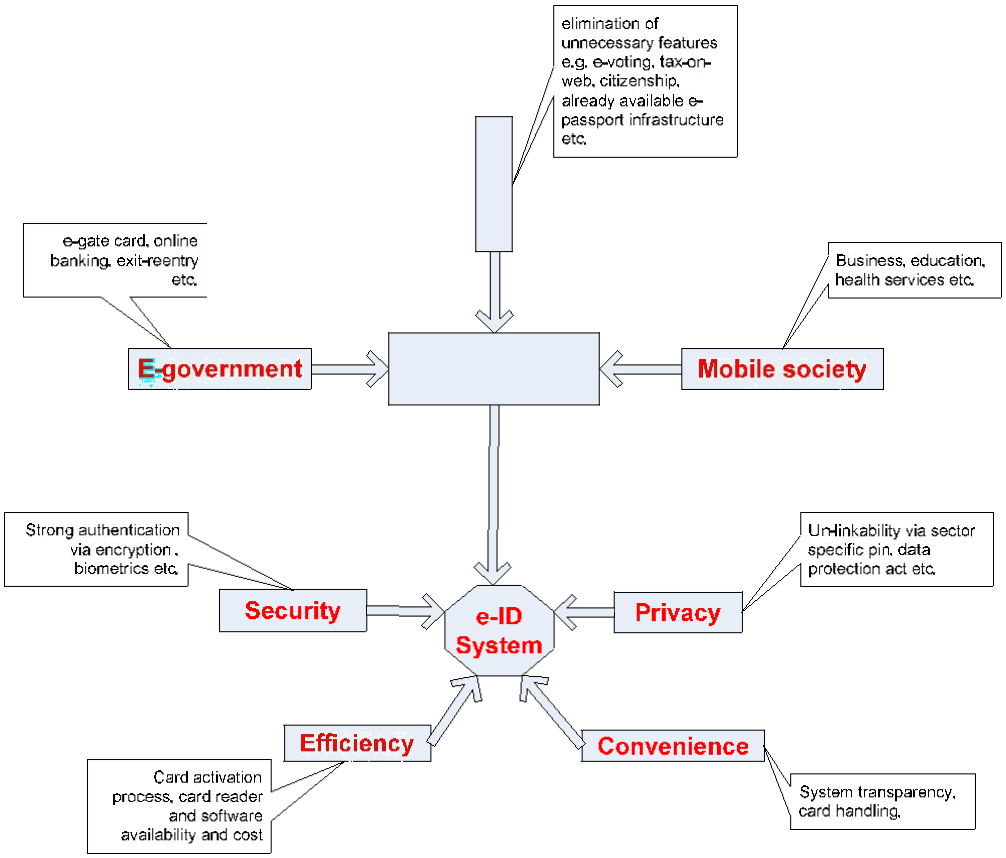

Figure 6. Driving forces for the proposed e-ID design and its usage and acceptance.

the Saudi government's goal of using electronic technology to help making the public sector more efficient. Through this program the Saudi government has implemented e-gate card, online banking, exit-reentry facility for experts and many other electronic services are expected in the near future (http://www1.elm.com.sa/Portal/En/Topics/Services/eGate/default.htm). In order to obtain an e-government service the individual needs to provide the same personal details which he/she has provided to obtain national ID card or driving license. Obtaining an additional service in this way not only increases the number of tokens for individual to carry but also the unnecessary efforts of enrolment. The e-ID card would avoid the need for an individual to provide the same personal information to different government depart-ments repeatedly. As evident from Figure 7, a person needs to enroll for each and every service and shall carry different tokens to authenticate for different services in the Saudi society. The need for e-ID card will increase with the increase in the remote interaction between individuals and organizations. Hence it can be said that for the success of e -government in Saudi Arabia, the implementation of a national e-ID card is necessary.

In addition to the unnecessary efforts made by the individual to enroll separately and carry separate cards for different services, cost is also the driving force behind the implementation of e-ID card. The Kingdom spends money on setting up separate centers for different services, deploying and maintaining IT infrastructure, hiring and training employees. All these expanses can be eliminated by adopting one system that integrates all other identity systems, i.e., e-gate card, driving licenses and health card etc. This would also reduce costs incurred by the individual in paying for each and every token separately. So it is argued that building National e-ID card is a cost effective solution.

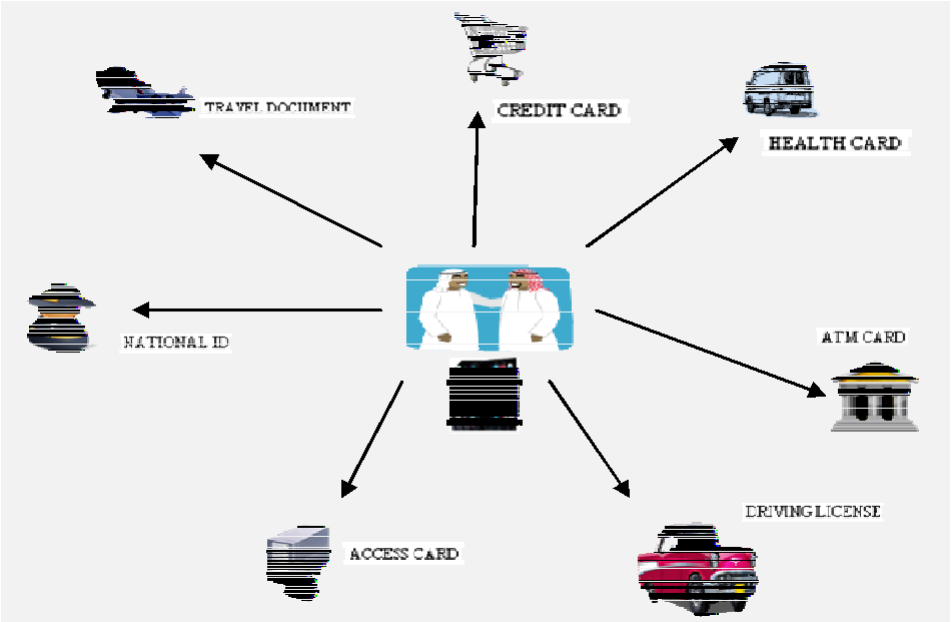

Figure 7. An individual authentication for different services.

Moreover, the current system is time wasting and inconvenient to individuals as well as to agencies. Figure 7 shows the existing scenario of an individual for enrolling and authenticating for different services.

Saudi Arabia is economically a stable and geographically a very important country. It is an attractive place to stay and work, therefore the adoption of a national e-ID card will be helpful to thwart illegal immigration and combat terrorism. With the implementation of the e-ID card, all the information about the individual is made centralized. To interact with any public or private sector, e-ID card is required whether it is driving li-cense department, health department, education, bank or acquiring the service of a cellular network. Hence the illegal immigrant will be unable to get benefit of any government services and unable to authenticate to the authorities. Apart from illegal immigration, e-ID card will be helpful against criminal elements who pose a serious threat to the national security of the Kingdom.

Finally, the list of the ICAO contracting states includes Saudi Arabia. There is legal and political pressure to implement e-passport system that is compliant with the standards specified by ICAO 9303 (http://www.icao.int/cgi/statesDB4.pl?en). One advantage of implementing ICAO compliant Saudi e-passport is that national e-ID card scheme can be run alongside e-passport scheme. While using the same infrastructure, data capture, IT network, PKI and access control systems for the implementation of e-ID card resulting in secure and cost effective system.

Acceptance and usage

Although it seems feasible for the government to implement e-ID card keeping in view the above driving forces, however, for such systems to be adapted, security and privacy should be the major aspects in the design as shown in Figure 6.

It can be presumed that the infrastructure of the e-ID card developed for the Kingdom will be secure and efficient as compared to that of European and other developed countries which are very complex. For example, the concept of e-voting is emerging in many countries and some countries have already adopted such systems i.e. Estonia (Kalvet, 2009). To make e-ID card capable of supporting e-voting an additional feature needs to be added in e-ID card. In other words, the e-ID card provides the base for e-voting. Using e-ID card let the voter access online ballot. To cast the vote electronically, the voter has to authenticate itself through a reader using his/her e-ID card. It means additional features have to be added into the e -ID card system to make the e-voting system working (Kalvet, 2009). It has been found that such systems are highly unsecure and technically complex. Since there is no voting system in the kingdom of Saudi Arabia, so developing e-ID card system without making it capable of authenticating individuals for e-voting system is not only technically feasible but cost effective and secure.

Apart from e-voting some countries have provided tax-on-web service to citizens (Marien and Audenhove, 2010). Tax-on-web is an application that enables citizens

to submit their tax declarations online. Like e-voting, tax-on-web works on the basic infrastructure of e-ID card. Tax-on-web system has numerous security vulnerabilities. Since Saudi Arabia is tax free country, so its e-ID card does not need to be integrated with any tax system.

There are various device options for the e-ID system to be implemented on, e.g., national ID card, health card, ATM card, USB, mobile phones but national ID card will be a better option as it is used widely for identification in Saudi Arabia. Unique identifier is a threat to privacy which can be used for linking databases and making profiles on personal data (Aichholzer and Strau, 2010). In order to ensure privacy, linkability should be avoided by the use of sector specific pins.

In contrast to European and other developed countries, Saudi Arabia does not offer citizen ship to foreigners. Countries with e-ID cards systems have to integrate foreigner's ID with e- ID card (Marien and Audenhove, 2010) . From technical point of view, such integration makes the system complex. Since Saudi Arabia is not offering citizenship to foreign nationals so this is another ease in the implementation of e-ID card system.

CONCLUSION AND FUTURE WORK

This paper favors the biometric based national e -ID card system to be implemented in the Kingdom of Saudi Arabia. In this paper, the current identity ma-nagement system of Saudi Arabia has been analyzed. It further looks at the national e-ID programs of other countries and particularly keeping the Malaysian 'Mykad' as a model for the proposed biometrics based e-ID management system for Saudi Arabia. It is found that several tokens are being used in the Kingdom followed by a discussion on their purposes. It is predicted that the number of tokens could increase with the growth in the services provided by the Saudi e-government initiative resulting in inconvenience and cost to the citizens as well as to government and non-government agencies. So it can be said that e-government is a significant driver behind the develop-ment of the proposed e-ID system. In contrast to the current ID system, the national e-ID card will be an efficient solution in terms of security, privacy-protection, cost and convenience.

The Kingdom of Saudi Arabia provides an ideal environment for the e-ID card to be implemented by eliminating unnecessary features. These features are e-voting, tax-on-web and citizenship for foreigners, which are the requirements of EU countries and the adoption of which may compromise security and privacy.

It is believed that there is more work to do in the area of electronic identity management system in Saudi Arabia. Our future research plan includes the privacy and security concerns about the personal data collected for different purposes in the Kingdom and the data protection act regarding personal data.

REFERENCES

"Case Study: The Kingdom of Saudi Arabia National ID Card". Source [online]: http://www.lasercard.com/files/casestudies/LaserCard_case_study_Saudi_Arabia.pdf (Accessed: 5th march, 2010).

"Citizen ID Forum" [online], available from: http://www.ameinfo.com/179613.html [accessed on: 20th march, 2010]

"E-Gate Project", Source [online], Available from: http://www.moi.gov.sa/wps/portal/ [accessed: 1st march, 2010]

"ID Theft Statistics: Javelin (2010). Identity Theft Report" [online], available from: https://www.javelinstrategy.com/research/Brochure-170 [accessed on: 12th march, 2010]

"International civil aviation organization" [online], available from: http://www2.icao.int/en/mrtd/Pages/default.aspx [accessed on: 18th march, 2010]

"Mykad: the Malaysian ID card" [online], available from: http://www.rogerclarke.com/DV/MyKad.html [accessed on: 22nd march, 2010]

"Saudi e-government program" [online], available from: http://www.yesser.gov.sa/english/default.asp [accessed on: 5th march, 2010]

"The ICAO contracting states" [online], available from: http://www.icao.int/cgi/statesDB4.pl?en [accessed on: 15th march, 2010]

Aichholzer G, Strau BS (2010). "The Austrian case: multi-card concept and the relationship between citizen ID and social security cards", Identity in the Information Society, March, 2010, Springer Netherland.

Al-elm website, "A Passage to the world: E-gate" [online], available from:http://www1.elm.com.sa/Portal/En/Topics/Services/eGate/default.htm. [Accessed: 28th February, 2010].

Alhussain T, Drew S (2009). "Towards user acceptance of biometric technology in E-Government: A survey study in the Kingdom of Saudi Arabia." IFIP International Federation for Information Processing 2009, pp.26-38, Springer Boston.

Anil KJ, Karthik N, Abhishek N (2008). "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January 2008.

Electronic Identity Website, "What is identity theft?" [Online], available from: http://www.electronic-identity.org/what-is-identity-theft [accessed on: 28th February, 2010].

EU condemns identity theft in Dubai Assassination. [Online], available from: http://www.allaboutidentity.com/content/eu-condemns-identity-theft-dubai-assassination. [Accessed on: 25th march, 2010].

Gronlund A (2010). "Electronic identity management in Sweden: governance of a market approach", identity in the information society, March 2010, Springer Netherland.

Kalvet T (2009). "Management of Technology: The Case of e-Voting in Estonia", International Conference on Computer Technology and Development, Malaysia. 2: 512-515,

Kubicek H, Noack T (2008). "Comparing electronic identities in Austria, Belgium, Germany and Spain cases of path dependencies", DEXA/EGOV 2008, Torino, Italy.

Kwon YB (2010). "Biometrics in Asia" [online], available from: http://biometrics.org/bc2009/presentations/tuesday/Kwon%20MR%2014%20Tue%20345%20PM%20-%20400%20PM.pdf [accessed on: 10th march, 2010].

Lasercard Corporation [online], available from: http://www.allbusiness.com/law-legal-system/immigration-law-national-identity-cards/11746173-1.html. [accessed on: 23rd march, 2010].

Laurie AJ, Annie IA, Julia BE (2007). "Towards Understanding User Perceptions of Authentication Technologies", WPES07, Oct 2007, Alexandria , Virginia, USA. pp. 91-98.

Marien I, Audenhove LV (2010). "The Belgium e-ID and its complex path to implementation and innovational change", Identity in the Information Society, March, 2010, Springer Netherland.

Melbourne University Law Review, "Technical Operation of Mykad" [online], available from: http://www3.austlii.edu.au/au/journals/MULR/2004/15.html [accessed on: 23rd march, 2010]

Modinis-IDM, "study on identity management in e-government: identity management issue report, D.3.9 June 2006".

Modinis-IDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome Moskovitch R, Feher C, Messerman A, Kirschnick N, Mustafic T, Camtepe A, Lohlein B, Heister U, Moller S, Rokach L, Elovici Y (2009). Deutsche Telekom Labs., Ben Gurion Univeristy, Beer-Sheva "Identity theft, computers and behavioral biometrics" ieee international conference on intelligence & security informatics, pp. 155-160, Dallas Texas.

Nexus Program, [online], available from: http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/ [accessed on: 5th march, 2010]

Organization for Economic Cooperation and Development (2010) "The e-government imperative: main findings", [online], available from: http://www.oecd.org/dataoecd/60/60/2502539.pdf, [accessed on: 3rd march].

Paul Benyon-Davies (2006). "Personal identity management in the information polity: the case of the UK national identity card" Information Polity, January 2006, Netherlands. 11(1): 3-19

Raphael C, Phan W, Lawan A (2003). Mohammed "the security and design of Mykad", Proceedings of the 9th Asia pacific conference on communication (APCC 2003), September 2003, pp.142-145, Malaysia.

Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007). "Generating Cancelable Fingerprint Templates", IEEE Transaction on Pattern Analysis and Machine Intelligence, 29, (4) April 2007.

Schouten B, Jacobs B (2009). "Biometrics and their use in e-passports", Image and Vision Computing 27 (2009) p: 305-312, USA.

Shaikh SA, Rabaiotti JR (2009). "Characteristic trade-offs in designing large-scale biometric-based identity management systems". J. Netw. Comput. Appl., Dec 2009 (In Press).