IST-Africa 2016 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2016
ISBN: 978-1-905824-55-7

Introducing E-Government in Developing Countries
Analysis of Egyptian e-Government Services

Othoman Elaswad, Christian Damsgaard Jensen
Department of Applied Mathematics and Computer Science,
Technical University of Denmark, DK-2800, Kgs. Lyngby, Denmark
E-mail: {otel,cdje}@dtu.dk

Abstract: Online Identification and Authentication is an essential requirement for providing e-services. Few studies have investigated the challenges facing e-Government and IDM in developing countries and, to the best of our knowledge, none of the existing research has studied the challenges facing online identification and remote authentication in developing countries, such as the North Africa Countries (NAC), where a relatively large proportion of citizens are illiterate. Therefore, the design of a national IDM system in a NAC must explicitly consider illiteracy to allow this group of citizens to benefit from online services. Egypt is one of the NAC, which has implemented online identification and authentication services that are widely recognized as the most advanced among the NAC. This paper analyses the Egyptian digital IDM in order to identify IDM requirements for online identification and authentication services that guarantee equal access to online services and an inclusive society. The study identifies strengths and weaknesses of the Egyptian e-Government and IDM services, which we believe are common to most NAC, since the NAC are quite similar in terms of social culture, citizen's education level and skills, citizen's behaviours, digital infrastructure and legislation, but also common to many other developing countries. Our analysis of the Egyptian e-Government services indicates that the security requirements and principle of equal access are not fully met, which illustrates the difficulty of introducing e-Government in developing countries.

Keywords: Authentication and Identity management.

1. Introduction

The introduction of new technology in the public sector aims to improve public services to citizens and businesses, increase convenience and reduce costs; this is commonly called e-Government [1][2]. Introducing new technology has an impact on the modes of interaction between citizens and the government, e.g. changing public services from face-to-face interactions into online services requires online validation of the citizen's identity and access rights [3][4].

Identity management (IDM) is a complex process that aims to perform online identification and authentication and manage the process of identity creation, registration, and issuing, storing, revocation, recovery and verification of identity based credentials. Each of these processes are exposed to different types of threats if not managed well. The most common models of IDM are Federated Identity Management Systems (FIDMS) and User Centric IDM. The difference between these two approaches depends on the level of user control over the disclosure of sensitive information when a service provider requests information. In User Centric IDM, explicit user consent is required before the IDM discloses any information, while FIDMS allows backend systems to collaborate and disclose identity information based on previously established trust relationships. The permission to release personnel information in the federated model is determined among all parties involved by a business partner agreement, so FIDMS is different from User Centric IDM in terms of the release of personnel information. The main entities in any IDM system (IDMS) are Identity Provider (IP), Service Provider (SP) and the User (U). The IP is responsible for creating and registering identities and issuing credentials that allow identification and authentication. The IP is also responsible for revoking credentials when credentials are compromised or lost or when citizens die. The SP is the entity that provides services to the users. The user is any entity that requests a service from the SP. There are various factors that affect the design of an IDMS, such as legislation and regulation, dependability of the digital infrastructure, cultural norms, social relationships, user's behaviour and skills. Many governments around the world have introduced modern IDMS to replace paper based systems[5]. Various designs of National ID (NID) have been implemented in different ways, e.g. Denmark provides a software solution for online authentication and digital signature called NemID[6][7] and Finland has issued an e-id card with PIN for online authentication and digital signature[8]. The main drivers behind implementing national IDM is to improve the identification and authentication mechanisms to help reduce crime, combat terrorism, eliminate identity theft, control immigration, stop benefit fraud, and provide better service to both citizens and legal immigrants[9]. However, introducing such unique number projects introduces a number of complex risks, such as duplication, impersonation and other ID related crimes. Although the benefits of most national ID schemes are fairly similar, the culture and historical context in terms of digital infrastructure and citizen skills may be quite different in different countries, so those factors must affect the design of a national ID system[10].

The different designs of IDM systems reflect the educational, cultural and technological state of the country in which they are implemented. This means that solutions proposed for developed countries do not necessarily work in developing countries that may have large illiterate populations or where the populations have limited access to a dependable networked infrastructure.

A number of developing countries, such as the Gulf countries and North African Countries (NAC), have recently adopted e-Government projects. For example, one study[11] did a comparative analysis across 16 Arab developing countries to assess the e-Government services provided by those countries. This study shows that Egypt's e-Government portal provides one-way information flows, two-way interaction and E-democracy, while Algeria, Morocco and Tunisia only provide one-way information flows. To provide two-way interaction services, online identification and authentication is required. This paper aims to study the strengths and weaknesses of the Egyptian digital IDM. Egypt is selected because it was identified as the best in class by the previously mentioned study[11]. Moreover, Egypt is similar to other North Africa Countries in terms of culture, social relationship, citizen's skills and behaviours. Egypt has a high population rate, so most of the common social habits and skills will be exhibited in Egyptian society. Therefore, if Egyptian's digital identity management fully meets the requirements of including both literate and illiterate citizen, it may be generalized to other NAC as well. This paper analyses some specific cases, which include the Egyptian online Civil State services and the Egyptian Ahly online National bank to understand the strength and weakness of the Egyptian IDM. To this end, we introduce a simple model that describes the IDM phases and the requirement for each phase.

The structure of the rest of this paper is as follows: Related work will be discussed in the next section and a simple IDM model used in this paper is introduced in the following section. Section 4 describes the Egyptian e-Government services. The case studies and lessons learned are presented in section 5. Section 6 presents the overall conclusions of the study.

2. Related Work

The online environment allows for the collection and interconnection of larger amounts of information than ever before. This may have tremendous benefits to both governments and citizens, but it also creates several risks that did not exist in the more traditional paper-based systems. For instance, one Norwegian study reported that, in 2004, members of the Norwegian Public Service Pension Fund (NPSPF) could apply for loans online by simply entering their social security number (SSN). If the SSN was valid and belonged to an NPSPF's member, then the sender would receive a message containing information, such as the person's name, address and zip code. The author of the Norwegian study showed that it was possible to determine valid SSN using NPSPF's loan web page by implementing a script to build a database containing the previously mentioned information and furthermore, it is possible to classify SSN to a set of people based on specific area using zip code. The author reported that they informed NPSPF, the Data Inspectorate and Independent administrative body under the Norwegian Ministry of Labour and government administration and they showed them SSN and address of both the Norwegian Prime Minister and the Director of the Data Inspectorate. This illustrates the dangers of relying on secret information with low entropy or a limited search space as authenticators and the author concludes that future Internet banking systems must be based on Public Key Infrastructure (PKIs) with client certificates to strengthen customer authentication[12] .

Another study[10] reported that Government identity management can be implemented in different ways, so it is useful to assess these differences against historical, cultural and social backgrounds and these elements can often be as important as technology in determining an approach to identity management. Accordingly, the public and private sectors are now producing a wide range of reference frameworks aimed at achieving consistency in designing privacy and security into identity management systems and as a result, they are gaining greater community acceptance. The authors took New Zealand's identity management as an example case. New Zealand's identity management system is based on a Government Login system to provide both single and multifactor authentication to support services with different transaction values and associated risks, while identification is performed via the Identity Verification Service (IVS). The authors conclude that the New Zealand example demonstrates the value of starting from a sound understanding of the policy environment and a clear vision of what is to be achieved.

In 2004, a research team at Al Akhwayn University in Morocco collaborated with Canadian researchers to implement and deploy a project to transform the Bureaux d'Etat Civil (BEC) in Ifrane, a city in Morocco. BECs are government offices that keep records of citizen's life events such as birth, marriage, divorces and death. The BEC in Ifrane was, as most other public administrations in developing countries, based on paper records. The project aimed to migrate the BEC onto an electronic platform that would provide value to the local community, widen the access, improve usability and support illiterate individuals. The authors reported that they started by installing IT infrastructure such as wired networks, database servers, a firewall and other software. Then they digitalized the information records. As a result, automated service delivery has replaced the paper based system and all citizens can access the new services through various channels including from an employee's desk, an information Kiosk or online through the e-Fez portal[13]. This study illustrates the current poor digital infrastructure of public administration in most of the developing countries and especially in the NAC and the importance of digitalizing Civil State Organization as an essential element of e-Government. The project explicitly considered illiterate individuals who represent a higher rate of citizens in NAC. Team projects of e-governments in NAC should consider this part of the population during early stages of initiatives; otherwise they may have negative effects on the success of projects. The authors did not mention how a citizen's identity is validated online. Moreover, the paper does not specify how the illiterate population will access and benefit from the new system. Another study related the main challenges faced NAC in terms of Information Technology Security into culture and social consideration such as user behaviour and lack of knowledge exchange about computer crimes between police officers in these countries[14][15].

3. A Simple IDM Model for North Africa Countries

The aim of this model is to identify the requirements of each phase of digital identity management. These phases include the registration process, creation of a digital identity, credential issuing and management of credentials as illustrated in Figure 1. We distinguish between National Identity and Digital Identity. All citizens should have a national identity, which is recorded by one of the government authorities, such as civil state registration, whereas a digital identity is only required by a citizen who wishes to access online services. To allow the Identity Provider to validate the citizen's identity online, the first step is, for a citizen to apply to get a digital identity. The Registration Authority (RA) verifies the submitted information to check if the applicant is qualified or not. An applicant is considered qualified if he satisfies the requirements defined in the registration process mentioned later. Step 2−5 in Fig. 1 shows the process of determining whether an applicant is qualified or not. If an applicant is qualified, then the digital identity will be sent to the applicant as shown in step 7 and the issued ID will be stored as shown in step 6. Otherwise, the request will be rejected as shown in step 8. As an applicant gets the digital identity he then needs to apply for a credential that will link to the issued digital identity as shown in step 9. This created credential will be temporary and only used to activate the account. Finally, an applicant needs to activate his/her account by accessing an activation service

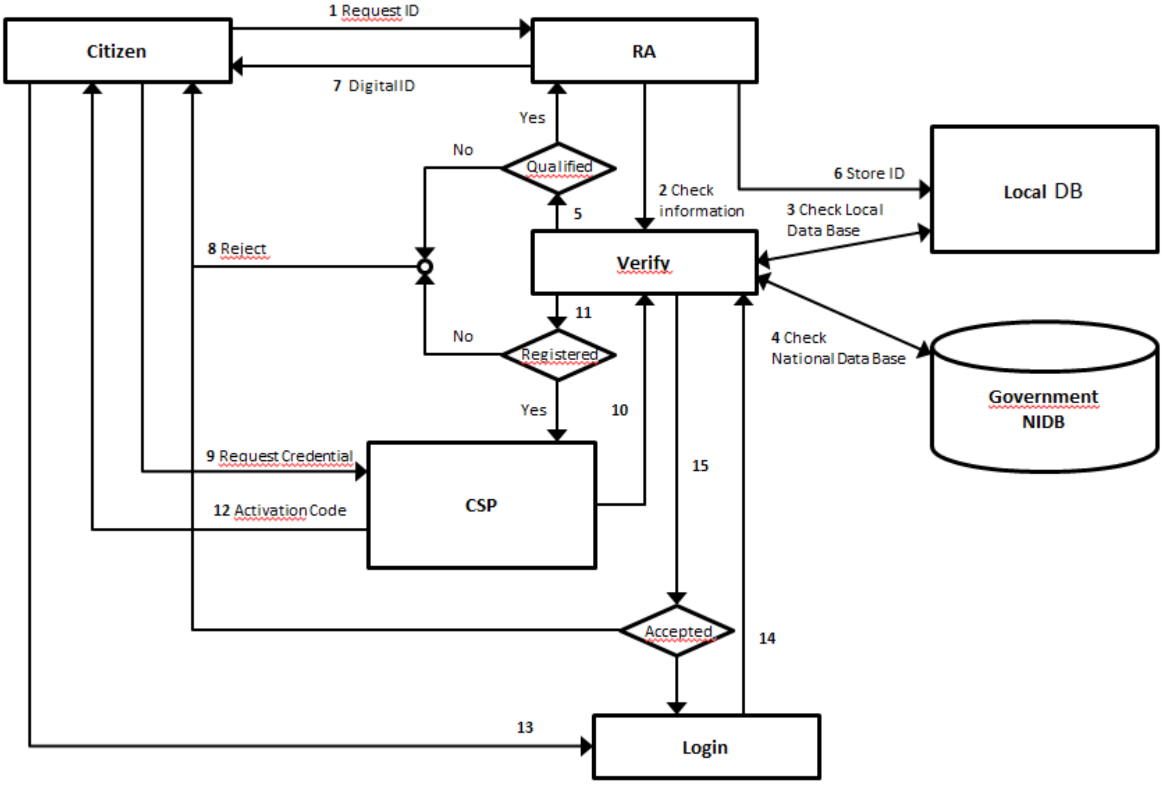

Figure 1A simple Model of Online Authentication.

and entering the digital identity and the temporary credential to create his secret that will be associated with his digital identity for subsequent access online services. Later, when a citizen requests online service using his/her digital identity and the associated secret, the identity provider will validate the entered identity before providing the requested service. The following sub sections will describe each phase of the model in more detail.

3.1 Registration Process

The first step of IDM process is the registration process, where an applicant may either show up in person or register remotely. In both cases, the Registration Authority (RA) must verify the authenticity of the applicant, i.e. it must protect against the main threats to the registration process, which are fabrication, impersonation and repudiation of registration. This translates into the following operational goals that the RA must ensure: the applicant's National ID number is registered in the National Database, the number belongs to the applicant and it is difficult for the applicant to repudiate the registration later. Another requirement is to ensure that the applicant has not been issued with a digital identity before, this may require a national search if the RA is a regional authority. The RA must identify mechanisms that satisfy the above requirement to avoid such threats.

3.2 Credential Issue

When an applicant has been identified and authenticated, a Credential Service Provider (CSP) is responsible for issuing credentials and associating necessary secrets, such as passwords, with the proven identity. The first requirement in this phase is to verify digital identity of the applicant and ensure that it belongs to that applicant. It is also required to ensure uniqueness of the issued credentials, by ensuring that each digital identity only have one credential associated with it. Then, the CSP needs to protect the channel used to deliver the issued credential to the applicant against modification or disclosure. For example, the average citizens in NAC have limited computer skills, so email is often not a secure way to send secrets to the applicant. This requirement aims to ensure the integrity and confidentiality of secrets during transportation. The final requirement in this phase is to ensure that secrets have been received by the right applicant.

3.3 Recovery of Secrets

The aim of this phase is to help citizens in case they lose or forget the secrets. There are different mechanisms that can be used to recover secrets, e.g. challenge-response questions and one time password are examples of mechanisms that could be used for recovering secrets. Each of these mechanisms has different design options. In a Challenge-response question mechanism, which is the most common mechanism, a user selects a question or an answer given a system generated question that the user must answer during the registration phase. Later on, when a user has forgotten or lost his credential, the user can use a recovery feature to reset his secret, which is associated with his digital identity. In the recovery phase, a system submits the registered question to the user and the user must provide the registered answer to that question. If the answer is easy to guess by others, then it will be easy for an attacker to perform an impersonation attack. Therefore, the vulnerability of the recovery system will affect the security of the whole system. Recovery systems rarely used, as we mentioned above, so some users may forget the appropriate answer related to the recorded question. Therefore, a balance between security, privacy and usability measures must be considered by satisfying the following requirements. The system should ensure difficulty of guessing answers and difficulty of getting answers from public sources. The system should be limited to collect non-public information. The system should give sufficient retry attempts to give a user more chance to remember the appropriate answer to a challenge-question.

3.4 Policies and Strategies

An organization should identify its own security policy regarding the type of tokens to be used in terms of the required security level, lifetime of credentials, procedures for renewal/reissuance, revocation and destruction. The stored data, such as digital identity information and the information used by a user to prove his identity during registration, requires guaranteeing confidentiality and integrity. Furthermore, a system should ensure that, provided services such as activation processes and validation processes, are always available to legitimate citizens. A system should have mechanisms for renewal/reissuance of secrets and credentials based on the organization's security policy. A system should be able to retrieve information in case of failure. Any vulnerability in management of credentials and stored records will violate the security of the system.

3.5 Online Identification and Authentication

The strengths of verifying a citizen's identity and remotely authenticating citizens is based on the strengths of the previous processes including the registration process, issuing credentials and strengths of secrecy recovery. Another requirement is that the communication channel, during online transaction, should be secure. Uniqueness and accuracy of stored data is also required to enable a verifier to accept or reject the request. Finally, the number of retries should be limited, or an increasing delay should be introduced after each failed attempt, to prevent the authentication service acting as an oracle.

4. The Egyptian e-Government Services

Egypt is one of the North Africa Countries, with a population of 75 Million. It has an illiteracy rate of about 45% and 23% of all Egyptians live under the poverty line[16]. During the past decades, the Egyptian government has carried out various reforms of the civil services. In 1985, the information and decision support center was formed to support government initiatives that support public access to government information[17][18]. In 1999, the Ministry of Communication and Information Technology was formed to facilitate Egypt's transition into the global information society[19][17]. In 2004 Egyptian's portal pilot project started to provide some online services, such as access to telephone bills. The vision of e-Government in Egypt is to provide public services in a way that suits all citizens[19]. The Ministry of State for Administrative Development (MSAD) has initiated a number of projects aimed at building and integrating an Egyptian Citizens National Databases. Also, the MSAD has reviewed all public services and identified the most frequently requested public services, in order to unify the decrees governing service delivery and minimize the required documents and procedures. This has resulted in public services provided through the Internet or telephone services, thus serving as a one-stop-shop[16]. Some of these services target citizens while others target the business community. Examples of citizen services include birth certificate/National ID replacement services, the college enrolment guide, car license renewal, tourism complaints, Egypt Air flight services, electricity bills inquiry, and online public libraries. Examples of business services include customs services, online banking, export guide, and registration for a commercial license[16][19]. One study reported that more than 70% of public services are provided on the Egyptian government's portal and that the Egyptian e-Government initiative has achieved the stage of allowing online transaction[20].

This paper aims to study the security strengths and weaknesses of Egypt's online identification and authentication. To achieve this goal, we need to consider some scenarios of Egyptian online services to identify security issues. The Civil State Organization is one of the most important services. It is responsible for registration of Egyptian citizens. Civil state issues essential documents that are used by other e-Government services. For example, a citizen needs: a NID to open a bank account and a birth certificate to apply for a driver's license. Online financial services also need to deal with sensitive information that must be protected, and such services require authentication of citizens' identity before any transaction takes place. In the following section, we describe Egypt's civil state registration services and Ahly net banking scenarios.

5. Case Analysis

5.1 Case 1 Egypt's civil state registration

The main online services provided by the Egyptian Civil State Organization include issuing of NID, Birth Certificates, Death Certificates, Marriage Certificates, Divorce Certificates and Family Certificates. The process of obtaining any of these documents requires an applicant to access the Egyptian e-services portal and choose the Civil State Organization service. Then the citizen needs to select the requested type of document and go through three steps. First, the applicant must fill in his/her own personal information including relationship to the applicant if the applicant applied on behalf of a relative; this information include name of the applicant, mother's name and NID number. The second step is to fill in the same information for the person to be issued the document if applying for a relative. Finally, an applicant selects the payment method. An applicant may either pay online or when receiving the required certificate. Within 72 hours, an applicant should receive the requested document by mail. There is no process that verifies the link between the entered national number and the applicant at the time of application, the verification is mainly through the postal services.

In the following, we analyse the security of the Civil State Organization e-service transactions to identify possible risks that might affect the organization as well as the citizens. We use the CORAS approach for Risk Analysis. It consists of three parts including Language, Tools and Methods[21]. The CORAS language uses a graphical editor that produces risk diagrams that are often used during brainstorming session.

Figure 2 uses a CORAS Risk Diagram to show possible threat scenarios that may lead to unwanted incidents and cause risks. As the citizens' education level limits the access to e-services, we classify citizen into citizens and illiterate citizens (those who cannot read and write). Employees of the state organisation are also considered a type of citizen that may accidentally or maliciously initiate a threat.

The first class of citizens is an educated citizen who has sufficient knowledge to enable him/her to interact with the system. This type of citizen may initiate one of the two threats shown in Figure 2. A literate citizen may have limited computer skills, and be unfamiliar with online attacks and malicious software. All these vulnerabilities, and others, will make different type of threats, such as phishing attacks, possible. Phishing attacks will lead to unauthorized access incidents, where both the citizen's record and the organization's reputation may be harmed. A literate citizen may also share or record confidential information, e.g. users often record their passwords on a piece of paper. Such actions initiate a threat of disclosure of information, which makes additional privilege escalation threats possible. These types of threats will lead to unwanted incidents including loss of reputation and abuse as shown in Figure 2. Reputation incidents will harm the organization’s finances, while abuse incidents will harm the citizens as well as the organization’s reputation.

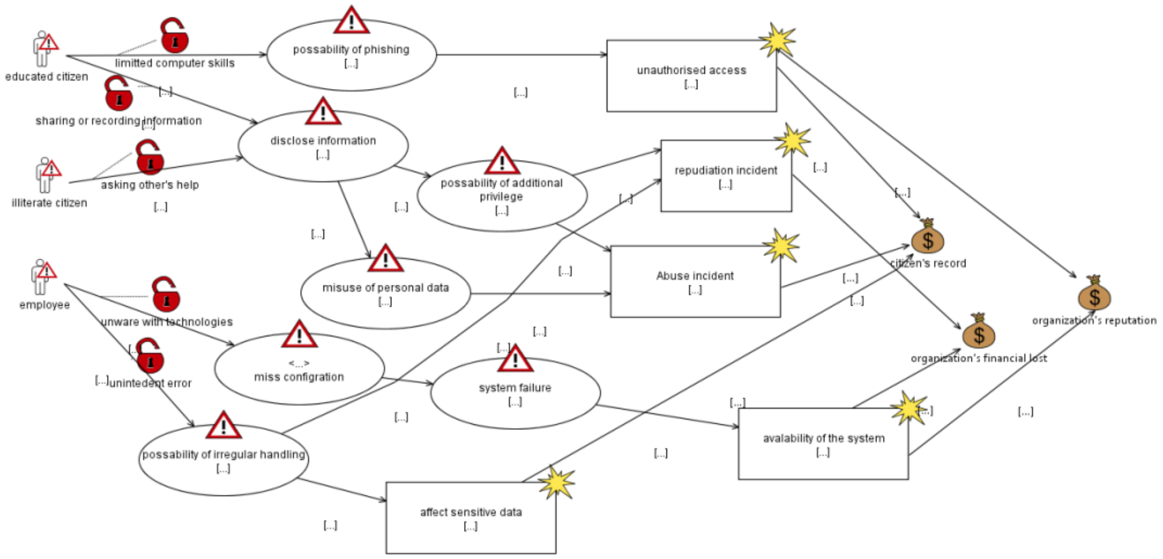

Figure 2: CORAS Risk Diagram for the Egyptian e-Governement Services

The second class of citizen is the illiterate citizens. These are unable to interact directly with the system due to inability to read or write, they normally ask literate people for help to apply on their behalf. This means that some risks identified above may also be initiated by illiterate citizen.

The third class of citizens is government employees, e.g. Civil State Organization employees. If employees are untrained in the technology adopted by the Civil State Organization, then the risk of misconfiguration is possible. Misconfiguration may result in system failures as shown in Figure 2. System failures may lead to unavailable services, which is an unwanted incident. Unavailability will prevent authorized citizens from accessing services, which will affect the organization’s reputation. The other possible threat initiated by an employee is unwitting such as input errors. Such errors will affect the integrity of data and as a result harm to the citizen’s information record as well as the organization’s reputation.

There is no identity verification to prevent unauthorized access, so any citizen who has an NID or knows another citizen’s NID can access the Egyptian civil state e-services and apply for a document using that NID. There is also no access control mechanism implemented to prevent unauthorized access. Moreover, the disclosure of a citizen’s sensitive information may lead to risks of identification from aggregated data. Illiterate citizens are unable to interact with web portals since she cannot read and write. Literate users with limited technology skills may also be unfamiliar with new technologies, so both this group and disabled citizens have unequal access opportunity compared to literate citizens who have experience with the existing technology. Disabled citizens and illiterates may disclose their information to others when they ask for help and this leads to disclosure of sensitive information, which as a result may create various types of unwanted incidents.

5.2 Case 2 National Bank of Egypt (NBE)

NBE developed its services and products to provide the bank’s customers with remote banking services and the bank has introduced a phone cash service that is independent of any mobile network in Egypt. Customers can use such services to pay phone bills, book airline tickets and transfer cash in a safe way. In 2002, the bank introduced online bank services including Ahly net Retail, Ahly net Corporate, Ahly E-shopping and Mobile payment services. This service has been added to Egypt's portal. To benefit from such services a customer needs to register online with Ahly net service (www.alahlynet.com.eg/eBanking). The registration steps are:

- An applicant needs to show up in person to one of the bank's branches.
- An applicant needs to bring proof of his/her identity attributes.
- An applicant fills in two application forms, one for updating personal information and the other for requesting to subscribe to the Ahly net service.
- The bank issues a National Bank of Egypt Identity number (NBEID) that consists of 8 digits.
- The NBEID will be sent to the applicant through the applicant's email.
- The bank issues a passcode consisting of 4 digits and sends it to the applicant's mobile phone.

As an applicant receives those credentials, the activation process starts by contacting a call centre. The applicant is directed to enter both NBEID and passcode. The call centre system will automatically validate the entered credentials. If the verification of the entered credentials fails, the applicant will be transferred to the bank's customer service for help, but if the verification succeeds, the applicant will be asked to enter a new passcode (TPIN) consisting of four digits, which will now be used as a password when the applicant accesses the system online. The applicant will also be forced to provide answers to three secret questions that will be used in case the password is later forgotten. These questions are:

- The applicant's mother's middle name
- The applicant's preferred color
- The applicant's preferred sports team.

5.3 Password recovery

If a customer forgets his/her password, the system allows three attempts to answer one of the security questions that were set during first time login. If a customer answers the question correctly within three attempts, then the old password will be reset and a customer needs to create a new password. If he fails to answer the security questions correctly, then a customer can enter the TPIN instead of the challenge questions. If the verification of TPIN succeeds then the customer can create a new password. If verification of the TPIN also fails, then the customer needs to contact the bank's customer service.

5.4 NBE Password policy

The IT department of the National Bank of Egypt has issued a number of password policies to strengthen the customer's password against attacks such as guessing attack. The main password policies of NBE are that passwords cannot consist of all characters or the applicant's user name, the password length should be between 8 and 28 characters and the password should use a mixture of numbers and characters. Every three months the password must be changed.

Due to the registration requirement, it is difficult, if not impossible, for someone to impersonate another customer during the registration phase, e.g. an applicant is required to show up in person and prove his identity. Moreover, an applicant needs to fill in forms to ensure non-repudiation of registration later. These requirements fulfill the requirements identified in the registration process of our model. On the other hand, there are a number of weaknesses that may possibly impact the security of the system. Figure 3 shows a few scenarios that may cause unwanted incidents. Some of these vulnerabilities arise because of weaknesses in password recovery and the password policies. Other vulnerabilities relate to the bank's customer. As we mentioned in the section above, a bank will send the NBEID to a customer through the customer's email and send the TPIN to the customer's mobile phone. The average customer has limited computer skills, so they may be unable to protect their computers from malicious software, such as key-loggers, spyware and viruses, and they do often not know how to handle phishing emails. Therefore, if a customer's email is hacked, the NBEID will be discovered. If a hacker obtains the NBEID, then the features of password recovery can be used to get the password belonging to the customer's ID. This may result in unauthorized access to the system, which leads to harm to the customer's account as well as impact on public image of the Bank. The security requirement of password recovery has failed to fulfill the identified requirement of a recovery system as well as the management of credentials as defined in our model. The bank's security questions are fixed and easy to guess. As a result, it may be possible to violate the security of the whole system. Also, the password policy of the bank requires customers to change their password every three months, so every three months a customer needs to remember a new password with a length between 8-28 characters. This requirement leads to issues of forgotten passwords, poor passwords chosen primarily because they are easy to remember and it may also force some users to write down their password, in order to remember them. Forgotten passwords prevent customers from accessing bank services for a period of time. Moreover, poor passwords allow hackers discover credentials and enable them to access the customer's account and also to change the password, which prevents the legal customer from accessing the service. Hackers might violate recovery system and reset customer's password and as a result prevent a customer from accessing services. Some of the bank's customers are illiterate so they may ask others for help, which forces them to disclose their credentials to others, which may lead to additional privilege incidents as well as repudiation incidents. All these issues arise because of poor identity management.

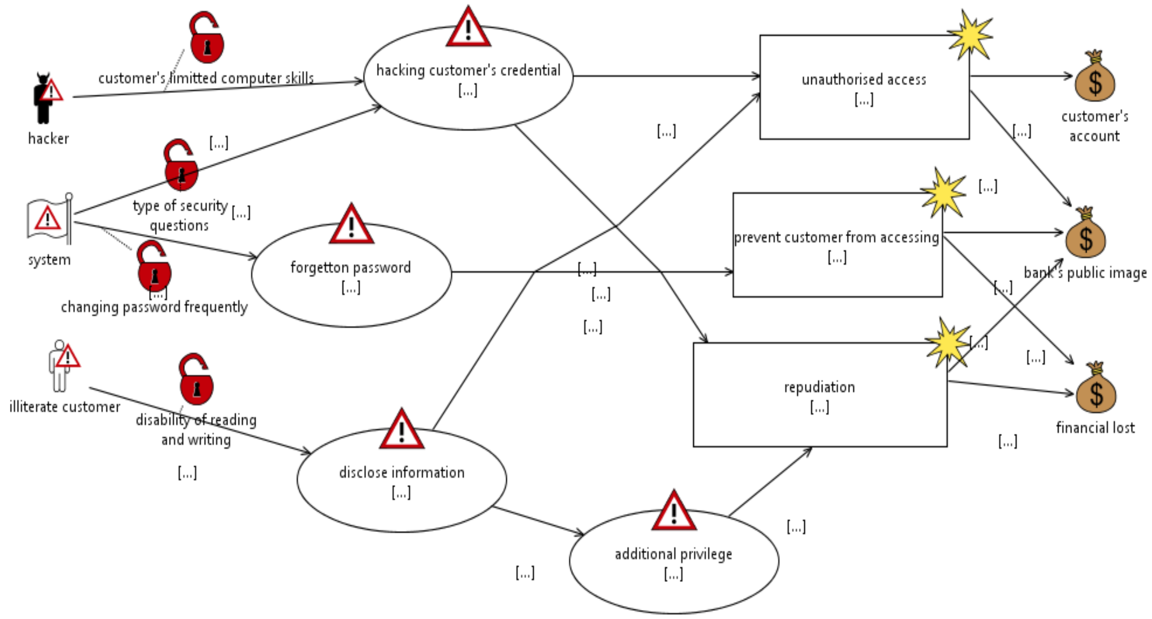

Figure 3 shows possible threats against National bank of Egypt

5.5 Lessons learned and recommendations

The Egyptian case illustrates that some developing countries may provide online services before implementing online identification and authentication systems. The fact that some organizations consider something that is not secret, e.g. an applicant's favourite football team, as an authenticator exposes systems to various online attacks. There is a failure to achieve the vision of equal access, e.g. illiterate people are not considered and, as a result, they are likely to circumvent the system by performing illegal delegation to benefit from the online services. Some organizations implement poor online authentication and force users to carry the risk. For example, Ahly net bank's policy mentions that a customer is responsible for all transactions carried by the bank based on the customer's credentials until the bank receive written declaration from a customer to indicate that credentials are stolen, while the bank's security questions are vulnerable to various attacks such as guessing attack. Selection of authentication method should match the citizen's skills and abilities as well as societal culture. For example, user name/password is not a suitable authentication method for Al-ahly bank, because some of its customers are illiterate, so they will reveal their passwords to others when they are asking for help.

To resist online attacks and achieve the stated objectives of e-Government in NAC, as well as other developing countries, we propose the model defined in Section III, which is based on the requirements to help NAC transition from paper based systems to online systems securely. Before providing online services to its citizens, a country must design and implement online identification and authentication systems. The first steps to introduce digital IDMS start by digitalizing the citizen's record in the Civil State Organization or similar government authority that record citizen's information. The process of digitalizing citizen's record is not just creating a digital database and transferring all records into digital form. It also needs to sanitize all the information stored in the paper based system to ensure the uniqueness, accuracy, completeness and consistency of the information. It must also introduce digital legislation and regulation that specify the accountability of each entity in the digital transactions and identify activities that are considered as digital crimes. It must organize the interaction between government bodies, citizens and businesses using digital documents and media. After that, a government needs to identify the goals of electronic IDM, e.g. will it be used to identify citizens online applications or for both offline and online transactions. All these considerations impact on the shape of electronic identity management. The following requirements to be considered to provide e-services that support majority of citizens:

- Implementing online Identification and authentication is a precondition for provisioning e-services.
- Provide a wide range of access means to support a large portion of society including illiterate individuals.
- An identity provider is responsible for the entire identity management process, including issuing, activation, revocation, renewing and performing online identity verification as the model explained in section III.
- A system should be able to prevent illegal activities such as illegal delegation.
- A token should be composed of more than one authentication factor. This requirement is aimed to make sharing or describing secrets more difficult while using them is easier.
- The communication channels between parties should be reliable and secure.

6. Conclusions

Digital Identity management (DIDM) is an essential component for secure provision of e-Government services. Designing and implementing DIDM systems in developing countries is a complex process caused by human factors, such as limited supply of technology experts and generally limited IT-skills by citizens, but also by technology factors, such as lack of reliable IT-infrastructure. Understanding the human factors, such as citizen's behaviors based on social culture and the citizen's IT-skills are as important as the technological factors of DIDM. This paper introduces a simple model that illustrates e-DIDM process including registration process, issuing of digital identity, association of secrets and digital identity and finally login of citizens to e-Government services. Security abstractions and technology for e-Government services are typically developed for developed countries, with good basic education (i.e. high literacy rates) and high degrees of digital inclusion. In this paper, we have focused our study on North African Countries (NAC), where literacy rates and basic IT-skills are generally lower. In particular, we studied the design and implementation of Egypt's digital IDM as a case study for all the NAC. Egypt was chosen because it has a larger population than the other NAC, which includes many of the different cultures and social behaviors prevalent in the region. During the past 2 decades, the Egyptian government has reformed and initiated many e-government projects, e.g. the Egyptian e-portal has existed for more than 10 years, and Egypt is generally considered as one of the most IT-advanced countries among the NAC.

The Egyptian online services were analyzed using the CORAS risk analysis tool, which helped us identify possible threats that could lead to disclosure of personal information, escalated privileges and unauthorized access. Some of these issues relate specifically to citizens' with limited skills and abilities while others relate to more general problems with poor identity management. For example, we have seen, in the scenario section that it may be possible to hack a citizen's email, which is generally easier in populations with low IT-skills, and then exploit the feature of forgotten password to reset the password. Exploiting password recovery mechanisms indicate poor management of identity and credentials. This emphasizes the need to implement online identification and authentication that support the majority of citizens including disabled individuals and illiterate citizens. Absence of online authentication that supports these groups raises the issues of excluding a large portion of citizens from the benefit of e-Government service. A redesign of the existing online authentication schemes, which considers illiterate individuals as well as disabled groups, is therefore needed. Studying and simulation of how such groups interact with government services in offline environments; will help understand the possible channels to deliver online services. One possible way is to implement one time delegation of online authentication. The Egyptian e-Government, as well as other developing countries, needs to identify citizen's requirements as well as the technology and digital infrastructure to resist cybercrimes which has not previously existed in their society.

References

[1] T. Rössler, "Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government," Comput. Law Secur. Rep., vol. 24, no. 5, pp. 447–453, 2008.

[2] I. A. Alghamdi, R. Goodwin, and G. Rampersad, "E-Government Readiness Assessment for Government Organizations in Developing Countries," Comput. Inf. Sci., vol. 4, no. 3, pp. 3–17, 2011.

[3] A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Establishing and protecting digital identity in federation systems," Proc. 2005 Work. Digit. identity Manag., vol. 14, no. 3, pp. 11–19, 2005.

[4] G. Aichholzer and S. Straub, "The citizen's role in national electronic identity management: A case-study on Austria," 2nd Int. Conf. Adv. Human-Oriented Pers. Mech. Technol. Serv. - CENTRIC 2009, pp. 45–50, 2009.

[5] S. Khan and A. Hayat, "A Trustworthy Identity Management Architecture for e-Government Processes in Pakistan Categories and Subject Descriptors," pp. 1–6.

[6] J. V. Hoff and F. V. Hoff, "The Danish eID case: twenty years of delay," Identity Inf. Soc., vol. 3, no. 1, pp. 155–174, 2010.

[7] I. T. Management, H. Work, and I. Design, "A HUMAN WORK INTERACTION DESIGN (HWID) CASE STUDY IN E- GOVERNMENT AND PUBLIC," vol. 2011, pp. 105–113, 2000.

[8] T. Rissanen, "Electronic identity in Finland: ID cards vs. bank IDs," Identity Inf. Soc., vol. 3, no. 1, pp. 175–194, 2010.

[9] A. M. Al-Khouri, "PKI in Government Digital Identity Management Systems," Eur. J. ePractice, vol. 4, pp. 4–21, 2012.

[10] R. McKenzie, M. Crompton, and C. Wallis, “Use cases for identity management in e-government,” IEEE Secur. Priv., no. 2, pp. 51–57, 2008.

[11] A. T. Chatfield and O. Alhujran, “A cross-country comparative analysis of e-government service delivery among Arab countries,” Inf. Technol. Dev., vol. 15, no. 3, pp. 151–170, 2009.

[12] K. J. Hole, V. Moen, and T. Tjøstheim, “Case study: Online banking security,” Q5Rhg r gpsutcgvg whRxiqyqTuX6TuwxRxi V gr TH e6T t R $ C S xi ug tcX ie TYdf e! gptcsdgp hgj i5Tut2k5Vv lYmdmon, p. 121, 2006.

[13] D. Kettani, B. Moulin, M. Gurstein, and A. El Mahdi, “E-government and local good governance: a pilot project in Fez, Morocco,” Electron. J. Inf. Syst. Dev. Ctries., vol. 35, 2008.

[14] M. Elbasir, “Challenges of Computer Crime Investigation In North Africa ’ s Countries,” 2013.

[15] S. Alfawaz, L. May, and K. Mohanak, “E-government security in developing countries : A managerial conceptual framework,” Inf. Syst. Manag., 2007.

[16] F. H. Sayed, “Innovation in Public Administration : The Case of Egypt,” Europe, no. April, 2004.

[17] P. Mohamed, H. Mubarak, and T. C. Information, “The Egyptian Information Society Initiative,” 1999.

[18] S. Kamel and M. Hussein, “The emergence of e-commerce in a developing nation: Case of Egypt,” Benchmarking An Int. J., vol. 9, no. 2, pp. 146–153, 2002.

[19] “EISI-Government The Egyptian Information Society Initiative for Government Services Delivery Abstract,” Technology, no. 202.

[20] L. El Baradei, H. M. Shamma, and N. Saada, “Examining the marketing of e-Government services in Egypt,” Int. J. Bus. Public Manag., vol. 2, no. 2, pp. 12–22, 2012.

[21] M. S. Lund, B. Solhaug, and K. Stølen, Model-driven risk analysis: the CORAS approach. Springer Science & Business Media, 2010.