A proposed Security Model for E-government Based on Primary Key Infrastructure and Fingerprints

Jaafar.TH.Jaafar[1], Nermin Hamza[1], Bahaa Eldin M.Hassan[2], Hesham .A. Hefny[1].

[1] Department of Computer and Information Sciences , Institute of Statistical Studies and Research, Cairo University

[2] Chairman of Arab Security Consultants

Jaafar_jaafar2000@yahoo.com

Abstract

Securing services of E-government receives an increasing interest in recent years. It is quite important for any E-government services to maintain a sufficient level of security for protecting personnel information of millions of citizens who call such services. Public key infrastructure (PKI) is widely used by many researchers to develop various security models for E-government services. In this paper, we make a forward step to improve such a security methodology by introducing Fingerprints as an additional biometrics means to enhance both authentication and non-repudiation security services. The analysis of the proposed model is promising and provides encouraging signs in terms of acceptable response time and higher security level.

Keywords*:* E-government; Security models; Authentication; Non-repudiation; Fingerprints.

1. Introduction

Using E-government services increases the needs for the user privacy. To accomplish E-government security there are two security issues that must be considered, namely, authentication, and non-repudiation. Applying Public key Infrastructure (PKI) is the main methodology for building security models for E-government.

Ali Shayna et al. (2008) explained the importance of information security requirements during each stage of the e-government. They used twenty selected items dealing with some limited aspects for information security management. However, their approach depends on the experts' opinions at each stage and generally is not applicable for all governmental organization [1].

Phi1D'Angio et al. (2012) began in the analysis of the characteristics of successful as well as not successful projects based on PKI led by government organizations. Examining E-Government project based on PKI suggested the approach for Government PKI programs that emphasize strong collaboration Use Cases. However, such a recommendation has not appeared in practical E-government application [2].

Ali M. Al-Khouri (2012) discussed the Multi-Factor Authentication approach which supports various aspects of authentication with different strengths e.g. pin code, biometrics, digital certificates. The multi-factor authentication feature is a major capability that the ID card provides for e-government applications. For example, Abu Dhabi e-government portal uses the UAE smart ID card to provide higher levels of assurance and confidence in the digital identities that interact with the portal. A two factor authentication (PIN and

Offline Certificate validation) capability of the ID card has been integrated to support and enhance the security for different e-service access models [3].

DaeyoungHeo and Suntae Hawng (2012) proposed some protocols and showed some challenges that came as an alternative certificate validation method, which translates the original certificate of national PKI to grid credential on separate Grid Security Infrastructure (GSI). Then, such translated credential is delegated to grid service by an extended (OAuth protocol). However, they did not explain how the citizens use such a protocol [4].

In this paper, we make a forward step to improve security in E-government models by introducing Fingerprints as an additional biometrics means to enhance both authentication and non-repudiation security services. This paper is divided into sections; section 2 will introduce an Importance about the E-government. Public Key Infrastructure will be presented in section 3. And section 4 presented the proposed model. And finally; section 5 presents the model analysis. Section 6 concludes the paper.

2- E-Government

E-government is the use of information and communication technology to enhance the delivery of information and services to others and to improve internal government procedures [5]. In the environment of E-government, citizens want to accept digitally signed tax returns. Execute electronic transactions securely. They also want to do all of this while maintaining strong security, streamlining administration, and containing operational costs [6].

2-1 Importance

E-government refers to the use of Information and Communication Technology (ICT), particularly the internet, as a tool to achieve better government [7]. E-government projects focus on automating the government activities and providing efficient and effective services to the citizens [8]. There are two areas of E-government implementation: front-office and back- office [9]. The front-office refers to the government as its constituents see it, meaning the information and service providers, as well as, the interaction between government and both citizens and businesses. The front-office involves two issues, online services and citizen engagement. The back-office refers to the internal operations of an organization that support core processes and are not accessible or visible to the public. Back-office involves the issues, such as organizational change, leadership, coordination, interagency collaboration, E-government skills, public-private partnership, managing risks and costs, monitoring and evaluation.

2-2 Stages and structure

E-government initiatives have a large potential in developing and delivering better services for citizens and to provide possibilities to interact more openly with agency constituents that lead to potential transformation in government structures and processes. The challenges in developing E-government can also be related to factors covering: information and data, the information technology (IT) as an artifact, organizational and managerial issues, legal and regulatory preconditions, and overall institutional and environmental aspects. Figure 1 shows the phase of E-government.

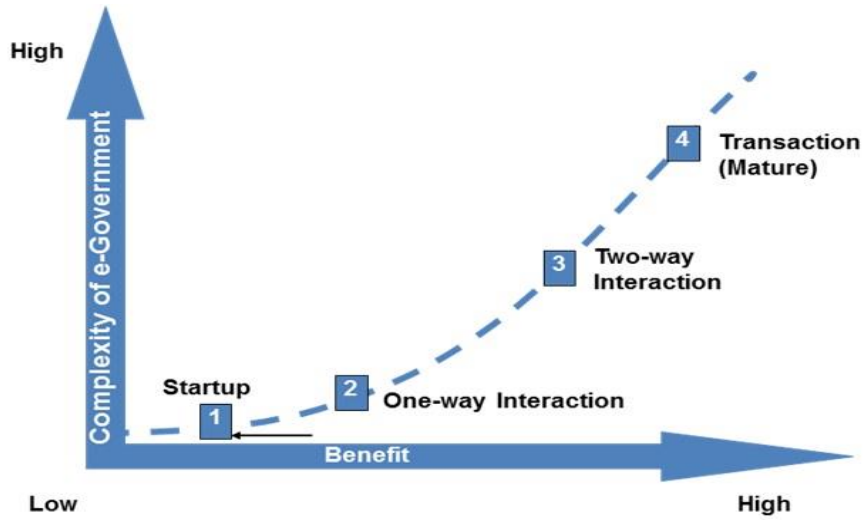

Figure1: Phases of E-government Development [10]

Phase of E-government are explained as follows [10]

Phase 1 – Startup

- Static government information published on the web: such as laws and rules, guidelines, handbooks, organizations, directories, and so on.
- An early stage in E-government development.
- Passive/Passive Relationship: government and its clients do not communicate on the web.

Phase 2 – One-Way Interaction

- Active/Passive relationship: government active – user's passive.
- To some extent, government services are available, such as download government forms (for example, income tax).
- Users can send e-mail to government, but government may not necessarily response in e-way.

Phase 3 – Two-Way Interaction

- Active/Active relationship: interactions between government and users complete on the web.
- For example, users obtain tax form on the web, fill it in on the web, and send it back to Revenue Authority through the web.
- Government and users can communicate with each other through the web.

Phase 4 - Transactions on the Web

- E-government matures at this phase:
- Complete a business transaction (for example, tax) on the web.
- Restructuring government becomes imperative; the ways that government operates are also changed.
- E-government is not merely computerizing existing government. Instead, it is to transform the existing government.

2-3 Services in E-government

E-government concerns the use of innovative systems, information and communication technologies to provide advanced and efficient services to users (Public,

Businesses, Employees and Government). The acceptance of these powerful tools in this domain has led to a variety of benefits including reduction of costs, revenue growth, transparency and accountability to governments, greater convenience, and increased productivity. Moreover, E-government services have a great potential for delivering better governmental services to users, improving the quality of the provided services and the accessibility to information/services [11].

One key factor that can help to increase the success of E-government is represented by the possibility to provide personalized services that are able to meet the actual needs and demands of users. Hence, in E-government domain, a crucial activity consists in acquiring extensive knowledge about target users of public services. Research interest is focusing on the development of strategies aimed at endowing governments with personalization mechanisms that enable to conduct their communications and services in a more user-centric way [12]. Figure 2 illustrates the main E-government Services**.**

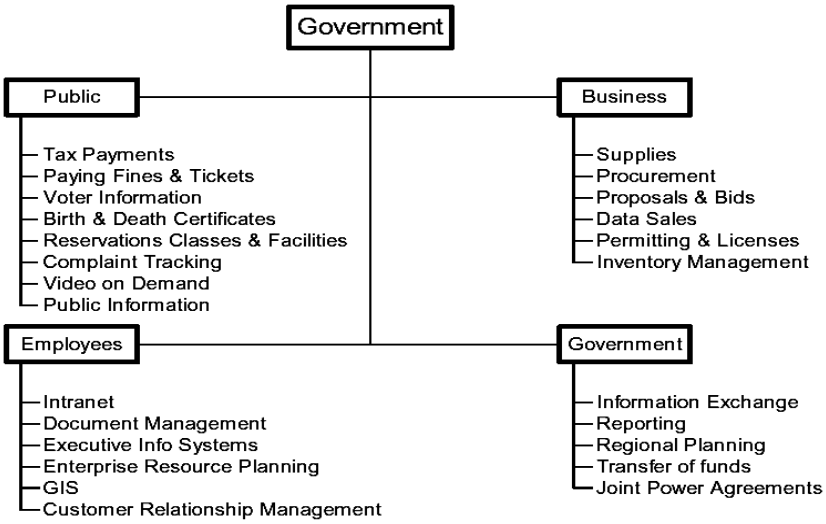

Figure 2: E-government Services [13]

2-4 Features and challenges

Janowski T. (2006) demonstrates the main features of E-government a follows [9]:

- Providing better business environment.
- Facilitating services for customers.
- Building trust between citizens and government.
- Contributing to achieve economic objectives.
- Strengthening good government and broaden public participation.
- Helping in achieving policy outcomes.
- Improving the productivity and efficiency of government agencies.
- Improving the services quality.

Implementation of E-government projects can also face a number of challenges including:

- Legislative barriers: which mean that E-government processes must have the same standing as paper-based processes.

- Financial barriers: which include financial arrangements that should be taken into account for the agencies working together on E-government projects.
- Technology change: this means adoption of the whole of E-government standards and software integration. Figure 3 shows full model of E-government systems and middleware technologies [7].
- Digital divide Digital: which means that large differences in the level of access to the internet and therefore the ability to benefit from e-government.

E-Governance is represented in government web sites, e-mail and service delivery over the Internet, digital access to government information, or electronic payments.

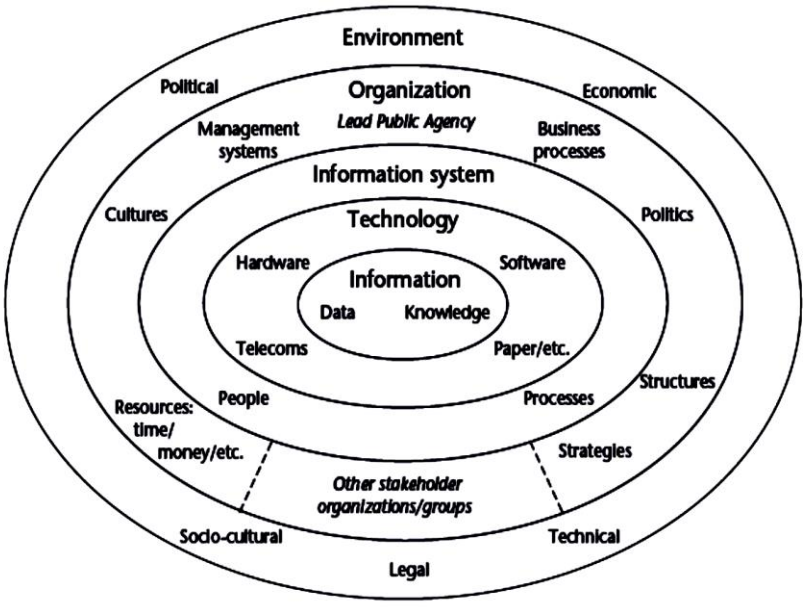

Figure 3: Full models of E-government systems [7]

3- PKI-based Security Model

Security models based on PKI are usually designed to ensure the security and trustworthiness of transactions and identities in three ways: through authentication, encryption, and digital signatures. The basis on which governments can execute safe and reliable transactions whether between individuals, governments businesses, governments or inter-government relationships is PKI. PKI allows public entities to securely authenticate all participants in a transaction [14].

3-1 Basic concepts of PKI

PKI could be defined as [4]: the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks. PKI combines digital certificates, public key cryptography, and certification authorities into a complete enterprise-wide network security architecture. The basic components of public key infrastructure are certification authority, Registration Authority, PKI Users, repositories and archives [15].

Certificate holders will obtain their certificates from different Certification Authorities (CAs); depending upon the organization or community in which they are

members [16]. A PKI is typically composed of many CAs linked by trust paths. A trust path links two relying parties with one or more trusted third parties. . Figure 4 illustrates PKI Architectures.

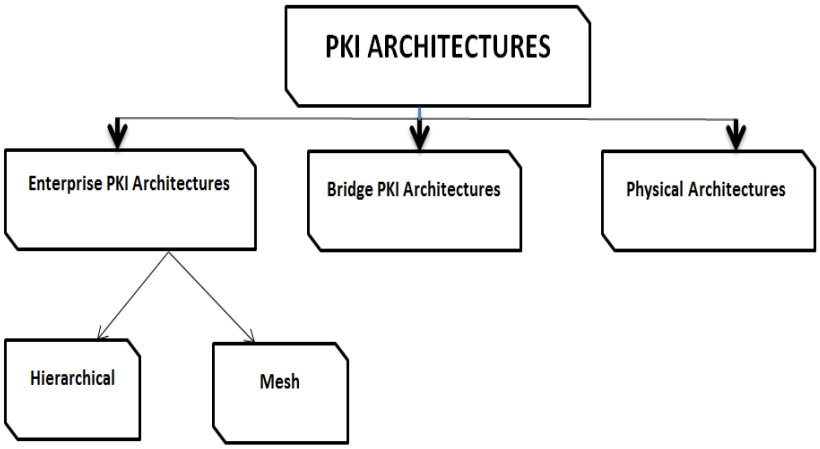

Figure 4: PKI Architectures.

3-1-1 Enterprise PKI Architectures: CAs may be linked in a number of ways. Most enterprises that deploy a PKI will choose either a "mesh" or a "hierarchical" architecture:

3.1.1.1 **Hierarchical**: Authorities are arranged hierarchically under a "root" CA that issues certificates to subordinate CAs. These CAs may issue certificates to CAs below them in the hierarchy, or to users. In a hierarchical PKI, every relying party knows the public key of the root CA. Any certificate may be verified by verifying the certification path of certificates from the root CA. Figure 5 (a) illustrates a hierarchical of authorities [17].

2.3.1.2 **Mesh**: Independent CA's cross certifies each other (that is issues certificates to each other), resulting in a general mesh of trust relationships between peer CAs. Figure 5 (b) illustrates a mesh of authorities.

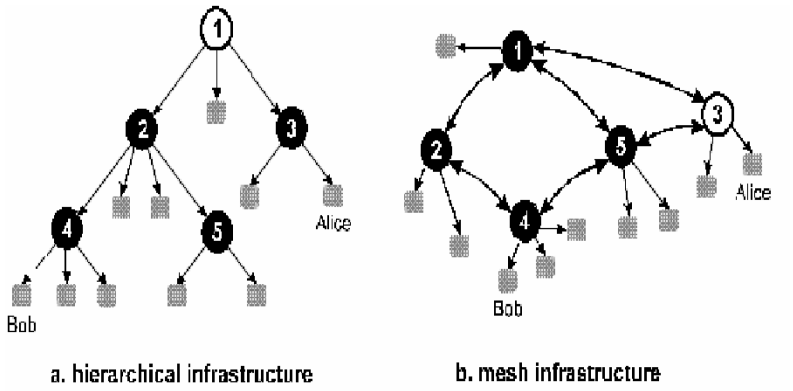

Figure 5: The two basic PKI architectures [17]

3.1.2 Bridge PKI Architecture: The Bridge CA architecture was designed to connect enterprise PKIs regardless of the architecture. This is accomplished by presenting a new CA, called a Bridge CA, whose sole purpose is to establish relationships with enterprise PKIs. Unlike a mesh CA, the Bridge CA does not issue certificates directly to users. Unlike a root CA in a hierarchy, the Bridge CA is not intended for use as a trust point. All PKI users consider the Bridge CA an intermediary. The Bridge CA establishes peer-to-peer relationships with different enterprise PKIs. These relationships can be combined to form a bridge of trust connecting the users from the different PKIs. Figure 6 indicates that the Bridge CA has established relationships with three enterprise PKIs [18].

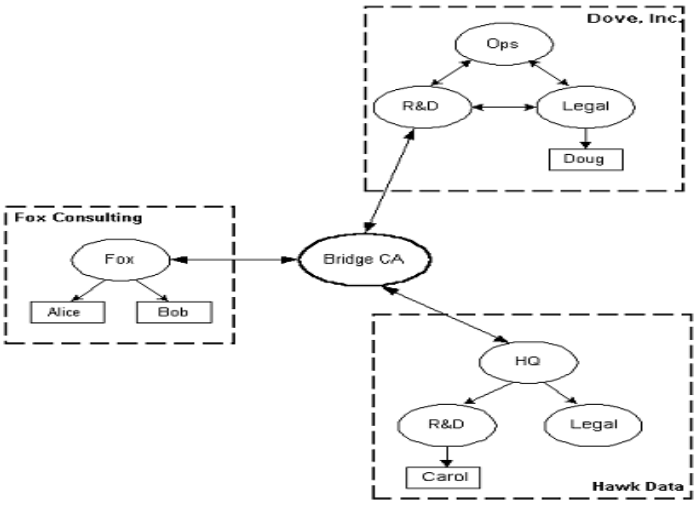

Figure 6: Bridge CA and Enterprise PKIs, [13]

3.1.3 Physical Architectures:

It is highly recommended that the major PKI components be implemented on separate systems, that is, the CA is one system and the RA is a different system and directory servers on other systems because the systems contain sensitive data, they should be located behind an organization's Internet firewall. Moreover placing the CA system behind an additional organizational firewall is recommended, so that it is protected both from the Internet and from systems in the organization itself. Of course, the organizational firewall would permit communications between the CA and the RA as well as other appropriate systems. **[19].** Figure 7 presents PKI Physical Topology.

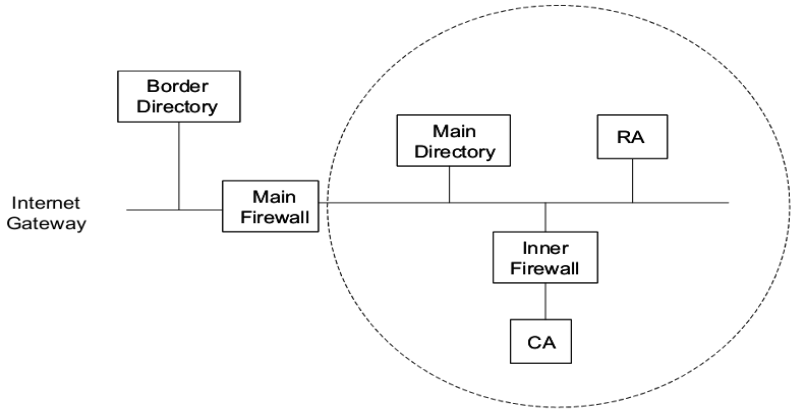

Figure 7: PKI Physical Topology

The basic data structures of PKI are: the public key certificate, the certificate revocation lists and the attribute certificate (which may be used as an addendum) [20]. Figure 8 illustrates PKI Data Structures.

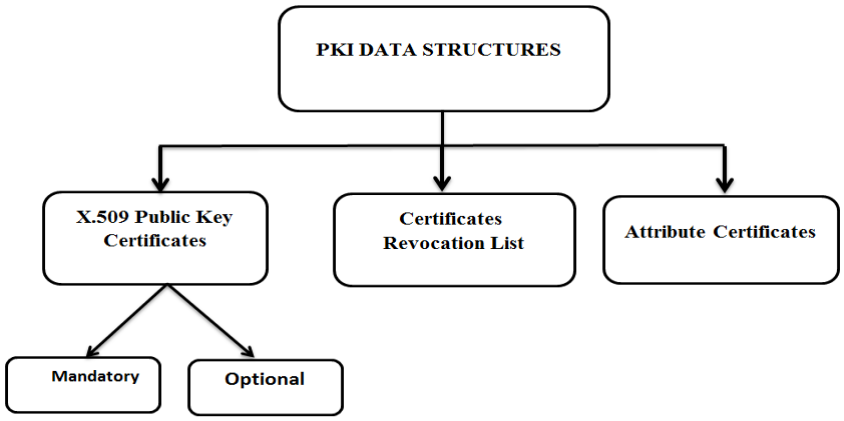

Figure 8: PKI Data Structures

- **X.509 Public Key Certificates:**

The X.509 public key certificate format, **[21],** has evolved into a flexible and powerful mechanism.

The X.509 public key certificate is protected by a digital signature of the issuer. Certificate users know the contents have not been tampered with since the signature was generated if the signature can be verified. Certificates contain a set of common fields, and also include an optional set of extensions. There are ten common fields: six mandatory and four optional. The mandatory fields are: the serial number, the certificate signature algorithm identifier, the certificate issuer name, the certificate validity period, the public key, and the subject name. The subject is the party that controls the corresponding private key. There are four optional fields: the version number, two unique identifiers, and the extensions.

- **Certificates Revocation Lists (CRLs):** Certificates contain an expiration date. Unfortunately, the data in a certificate may become unreliable before the expiration date arrives. Certificate issuers need a mechanism to provide a status update for the certificates they have issued. One mechanism is the X.509 certification revocation list (CRL).

The CRL contains the following fields:
1- Version.
2- Signature.
3- Issuer.
4- Present update.
5- Next update.
6- Revoked certificates.
7- CRL Extensions.

- **Attribute Certificates:** The public key certificates are focused on the binding between the subject and the public key. The relationship between the subject and public key is expected to be a long lived relationship. Most end entity certificates include a validity period of a year or two years **[22].**

3-2 Secured E-services based on PKI

This system is a unique solution and service platform for setting up certificate based, globally interoperable E-services on local, regional and national levels. At the core, an enterprise PKI is set up in a hierarchy comprising of a Regional Root and its local Subsidiaries. Thus small scale hierarchical trust architecture can be developed without heavy investments, and the benefits of a Chain of Trust can be fully harnessed.
The platform enables cross-government and cross-industry secured transactions and federated identity services in an interoperable way. Interoperability is achieved through standards, design and technology, and interoperability is utilized in order to integrate available third party and National identity and trust schemes into your own PKI.

There are practical applications PKI on E-service. For example, in the United Arab Emirates (UAE) [3], PKI has proven to be invaluable in E-government and e-commerce environments despite the complexity and associated risks that may stem from its application. It is observable that many of the current PKI projects have limited applications in E-government domain, because they are mainly sponsored and managed by private sector organizations. Establishing and using a government based certification authority would logically acquire higher levels of trust in the certificate issuance process and in the identities of the recipients of the certificates. The integration of PKI into central government identity management systems is believed to support the diffusion and acceleration of E-government progress, that is, the provision of citizen services and outreach over digital networks.

In India, [23], PKI is a hierarchical PKI with the trust chain starting from the Root Certifying Authority of India (RCAI). RCAI is operated by the Office of Controller of Certifying Authorities of Government of India. Below RCAI there are CAs licensed by CCA to issue Digital Signature Certificates under the IT. CAs can be private sector companies, Government departments, public sector companies, or Non-Government Organizations (NGOs). The certificate policies apply to all components of the India PKI, if applicable. Examples of India PKI components include but are not limited to RCAI, CAs, Registration Authorities (RAs), and repositories.

3-3 Shortcomings of PKI-based security model

The shortcomings noticed in both UAE and India cases are as follows:

- In UAE: Establishing and using a government based certification authority, would logically acquire higher levels of trust in the certificate issuance process and in the identities of the recipients of the certificates. The integration of PKI into central government identity management systems is believed to support the diffusion and acceleration of e-government progress, that is, the provision of citizen services and outreach over digital networks. However, the process is expensive through use smart card this need reader to read smart card, and UAE is used biometrics, this needed more reader biometrics.

- In India: used hierarchical Building architecture on PKI in e-government, but this is complex and takes long time to seek the certificate. For example, when user is logged in website, the first to verification from user through certificate, the verify from certificate in sub certification authority, or verifier from different certificate authority if take long time to verifier form user.

4- The Proposed security model

4-1 model Structure

The aim of the proposed model is to achieve some additional levels of security of E-government systems. The main security services we want to achieve are: authentication and non-repudiation. The proposed model based on three security issues: PKI, biometrics, and hardware security tool.

First of all, PKI methodology will definitely be used since it is based on the certificate and digital signature that ensure the authentication and non-repudiation security services, which we need to achieve in e-government system, [24].

Issuing the biometrics comes in the second stage. Different biometric systems can be adopted [25]. However, we choose using fingerprint in our proposed model. Fingerprint is suitable for E-government applications since it is the most economical biometric personnel characteristics (PC) for user authentication technique, Easy to use, small storage space is required for the biometric template and hence relatively small sizes of databases are needed, it has been standardized, and represents one of the most Developed biometrics

The third issue is using hardware security device. We choose hardware token. Hardware token is a physical device that provides trusted user identification and authentication. Advantages of the token include, it could be modified while in use, simple and inexpensive.

Hardware tokens are so-called smartcards with a USB form factor. The smart card takes much time to read data from because it needs reader device while the token need no device except USB socket. Logging into the site through a token is much faster than smart cards. The smart card can be scratched while the token does not scratch.

4-2 Interaction with the proposed model

The proposed model is based on two main levels: registration and verification. The both levels will be discussed as follows:

4-2-1 Registration

This level is face-to-face level; it needs a meeting between the user and the central government which act as a Registration Authority (RA). At this meeting the user needs to register his information into the central government to issue a digital certificate.

In the model we choose a hardware token can take and store the user fingerprint for more security. The RA gets the personal information of the user and his/her finger-print

image. Then the user receives the hardware token carried by the user certificate and private key. Figure 9 illustrates the registration steps. They are explained as follows:

1. The user Requests Certificate from the Registration Authority (RA). RA needs to Verify the User identity, this step is by giving the identity papers for RA.
2. RA Vouch for User to the Certification Authority.
3. Certification Authority issues the Certificate and generates public and private keys.
Certification Authority Stores Certificate, both keys to Repository (for future use the user because maybe he lost).
4. RA reads the user Fingerprint.
5. RA stores Certificate, private key and Fingerprint on the hardware Token and generates PIN for the user according to his demand.
6. RA Stores PIN and Fingerprint on Repository (for future use the user because maybe he lost).

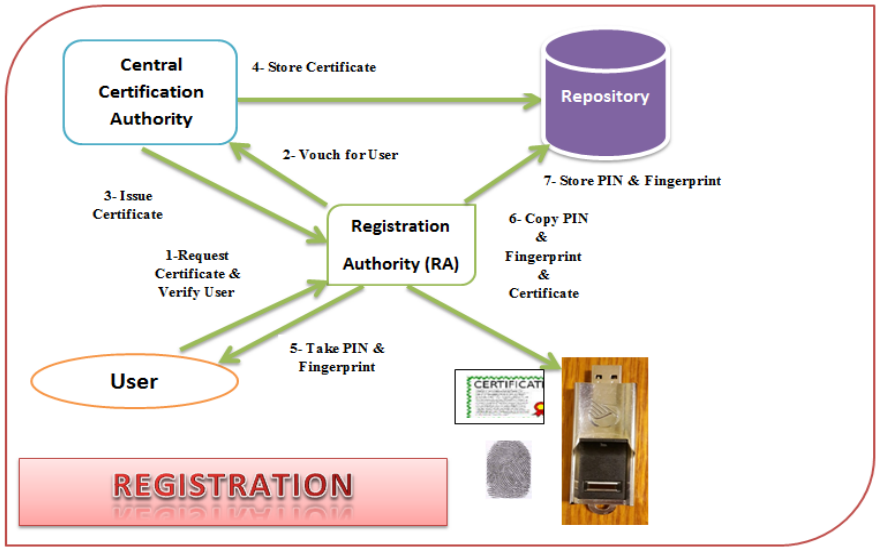

Figure 9: Registration (PIN & fingerprint & certification)

4-2-2 Verification

This level based on web application, this step is important for E-government. The user of E-government will be using his token to verify him. Figure 10 illustrates the steps of verification level. They are explained as follows:
1. This step is to verify User by typing PIN and then by fingerprint reader that Collect Biometric Data.
2. The token generates the template if Quality is Sufficient; else new biometric sample is requested.
3. Verify fingerprint by matching the template with the token if Decision Confidence then do the 4th step if not go back to user.
4. Digitally singed by the Relaying Party and take the Certificate.
5. Verify the certificate will be send it through to the server PKI and the certificate is verified through CRL.
6. Verify the certificate is active if generate session key and send session key to client, the client request new session and attaching the session key with his request, and the server

checks for session key if the session key correct then open session else stopping session. Else the certification is in active stopping the procedure.

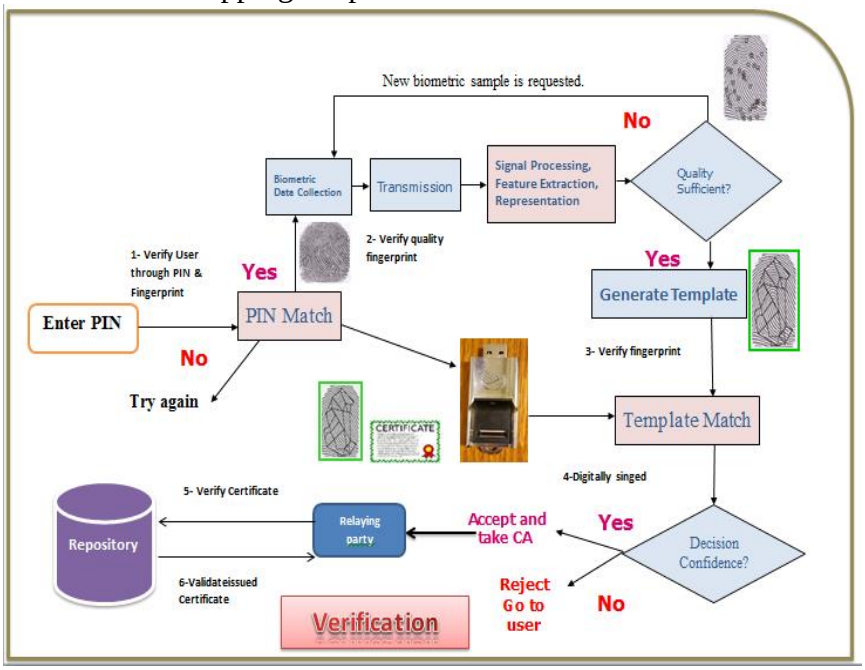

Figure 10: Verification (PIN & fingerprint & certification).

E-government must provide security during the high exchange of documents between the user and the server. To provide trusted file transfer; digital signature will be used using the stored private and public keys.

For example: if a user needs to book an electronic ticket for traveling abroad; he will open the site of traveling agency and ask to issue the ticket. Then the site asks the user to fill an application and resend it again. The server receives this document from the user. The sender could repudiate this task if any new situation happened to him.

In this case our model applies the digital signature for this document, using the stored private key on the token. The server verifies the digital signature using the database stored public key for the user. This method emphasizes that non-repudiation will be exist.

5- Analyzing the proposed model:

Through our study, it is clear that E-government is quite powerful in providing assistance to citizens. So our focus aimed to provide security to the service using the technique of user authentication and data transfer security.

The proposed model offered both two services authentication and non-repudiation. The authentication service could be implemented using two levels of security. The first one is the first level could be done on the client side and the second level on the server side. The client side authenticates the user by inserting the hardware token, writing (PIN code) and using the biometric property by using fingerprint. This step yields more user identity confirmation. It answers the question if the token is stolen what could happen? The robber may know the PIN code but cannot imitate the fingerprint for the stolen person.

On the other hand the server authenticates the user using the sent certificate. It differentiates between the sent one and the stored and also check its validity if it's expired or revoked.

The non-repudiation service could be verified by digital signature technique. The client sends the desired documents to the server. The client prepared the digital signature using the user private key which stored on the token.

Our model helps the non-experienced user to deal with E-government system. A user needs only to carry his token and insert it into the client side and only to know his PIN. We applied our model over an E-government system, which to focus authenticate the user then send a file with its digital signature. The time of using a hardware token is about 3 to 4 millisecond. On the other hand, we measure the time of sending file, calculating hash function, and the encrypting time using different file sizes. On the server side, we calculate the server decryption time, then comparing them. Then we compare between the system before and applying our security model.

At client side; before applying the security model the E-government web application didn't have any overhead of time but after applying the model it spent more time for calculating the sent file digital signature according to the file size. Figure 11 illustrates the time for different digital signature file sizes;

It is noted that the typical time taken to calculate the digital signature for different sizes of the sent files is evenly matched but it increases as the file size increases. It is also calculated in milliseconds so that it will not have a major impact on the operation of our proposed system that has such additional of security.

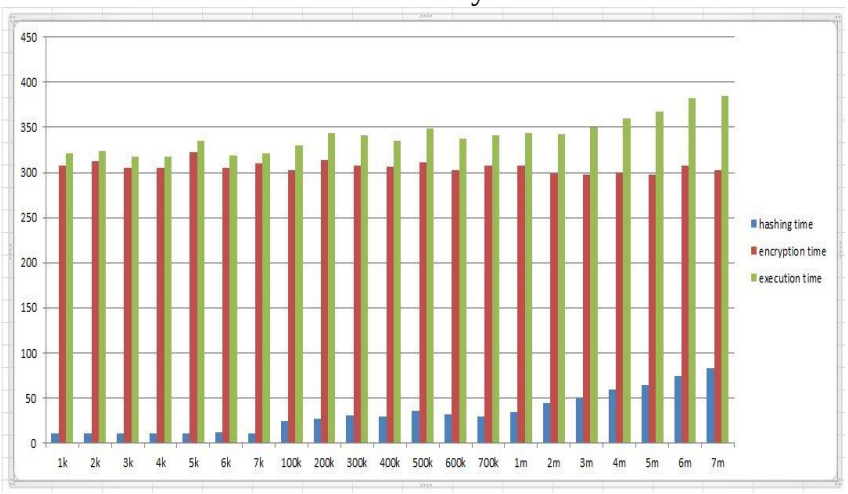

Figure 11: Comparing a hash, encryption and execution time

At the server side; we calculated the verification of the sent digital signature part for different file sizes, the communication time of the files in both cases ; after and before applying the security model;. Figure 12 illustrates the total time taken between e-government web applications before and after applying the security model. It is noted that: the time it takes to send the file after applying the proposed model is three times it takes before applying it.

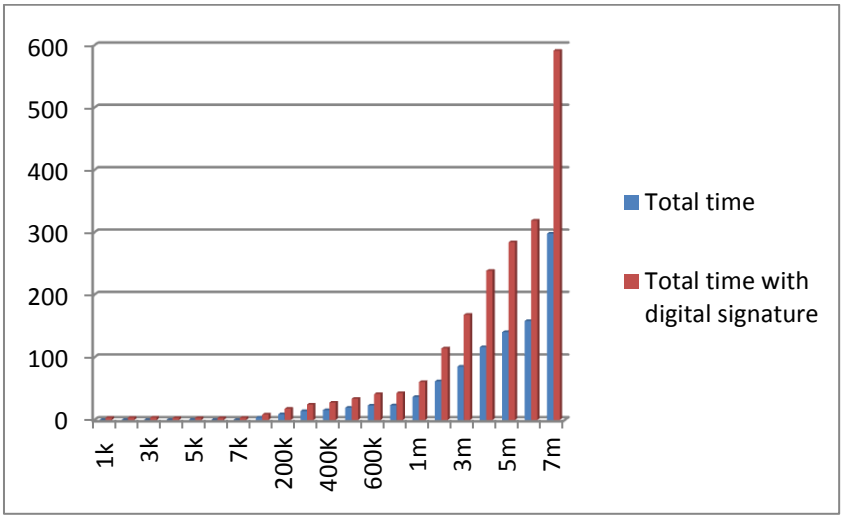

Figure 12: The total time taken between e-government web applications

Figure 13 illustrates the differentiation between the e-government web application after and before applying the proposed model on both sides; client and server.

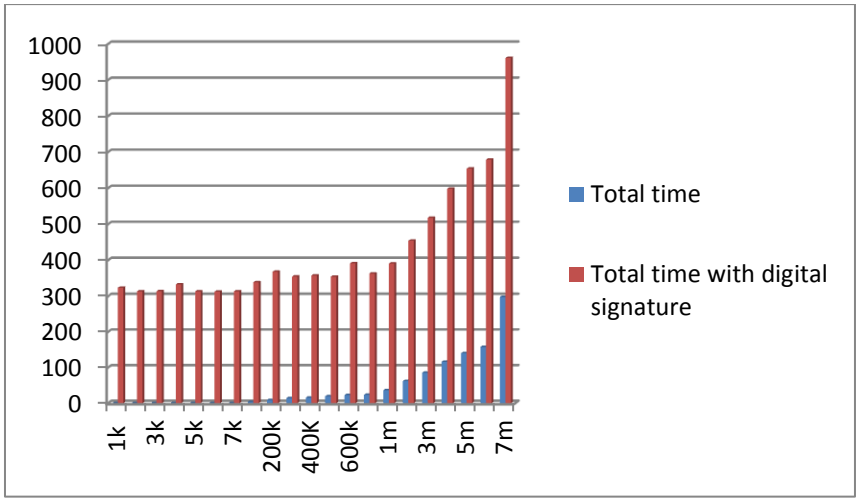

Figure 13: the differentiation between the e-government web applications

6- Conclusion

In this paper, we introduced a model to achieve security over e-government applications. Authentication and non-repudiation were the main two security services we achieved, using PKI, Biometrics and Digital signature. The Fingerprint was selected as it is easier to use.

We differentiate between the e-government application before and after applying the security model. The proposed model took an overhead to implement the authentication and digital signature but this overhead is calculated by milliseconds and we could overlook this time for achieving the goals of the security goals.

Future work, applied the proposed model in E-government applications, this availability less time comparison with smart card and more security in E-government area.

References

1. Ali Shayan, BehnamAbdi, and MaliheQeisari, "identify the importance of information security requirements during each stage of the e-government maturity", Springer-Verlag Berlin Heidelberg, pp. 250–262, 2010.
2. Phi1D'Angio .PanosVassilliadas• Phaidon Kaklamanis,"PKI- Crawling Out of the Grave &Into the Arms of Government", Securing Electronic Business Processes. Vieweg (2009). 108-115.
3. Ali m.al-khouri, "pki in government identity management systems" , European Journal of ePractice · www.epracticejournal.eu, Nº 14 · January/February 2012 · ISSN: 1988-625X.
4. DaeyoungHeo and Suntae Hwang, "Proposed to Adapt Reliability of National PKI to Grid Security Infrastructure by Credential Translation and Delegation with OAuth", International Journal of Security and Its Applications, Vol. 6, No. 3,pp.65-74, July, 2012.
5. Nugi Nkwe, "E-Government: Challenges and Opportunities in Botswana", International Journal of Humanities and Social Science, Vol. 2 No. 17; pp 39-41, September 2012.
6. Valentine (dardha) ndou, "e – government for developing countries: opportunities and challenges", EJISDC (2004) 18, 1, 1-24.
7. Heeks R, 2006, Implementing and Managing e-Government, Sage Publications Ltd, London.
8. Chen, H., Schroeder, J. , Hauck, R., Ridgeway, L., At abakhsh, H. , Gupta, H. , Boarman, C., Rasmussen, K. and Clements, A.COPLINK Connect : information and knowledge management for law enforcement . Decision Support Systems (DSS), Special Issue Digital Government: technologies and practices", Volume 34, Number 3, February, pp.271- 285, 2003.
9. T. Janowski, E. Estevez, and A. Ojo, "Conceptualizing Electronic Governance Education", 45th Hawaii International Conference on System Science (HICSS-45), Grand Wailea, Maui, Hawaii, IEEE Computer Society, 01/2012.
10. R. Housley and T. Polk,Wiley & Sons, "Planning for PKI: Best practices for PKI Deployment", GAO-01-277, February, 2001.
11. Leo Iaquinta, M. Alessandra Torsello, Marco Comerio,Anna Maria Fanelli, and Giovanni Semeraro, "User Segmentation in e-Government Services", Systems and Communication Viale Sarca 336, 20126 Milano (Italy), University of Bari - Dep. of Computer Science Via Orabona 4, 70125 Bari (Italy), 2012.
12. X. Guo and J. Lu, "Intelligent e-government services with personalized recommen-dation techniques". Int.J. Intell. Syst., 22(5):401{417, 2007.
13. Hanna, Nagy, "Why ICT Matters for Growth and Poverty Reduction", EJISDC (2009) 39, 3, 1-24
14. National pki: the foundation of trust in government, Symantec World Headquarters 350 Ellis St. (2011).
15. Matti Järvinen, "PKI Requirements for IPsec", helsinki university of technology department of computer science and engineering, 2003.
16. RFC 2104 HMAC: "Keyed-Hashing for Message Authentication".

http://www.ietf.org/rfc/rfc2104.txt, visited Jun. 2014.
17. D.A, "A model of certificate revocation," Proceedings of the Fifteenth Annual Computer Security Applications conference, pp. 256-264, December 1999.
18. D.A, "A model of certificate revocation," Proceedings of the Fifteenth Annual Computer Security Applications conference, pp. 256-264, December 1999.
19. W. Diffie, M.E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, v. IT-22, n. 6, (Nov 1976), pp. 644-654.
20. Annabelle Lee. "Guideline for implementing cryptography in the Federal Government", NIST SP 800-21. Security Technology Group Computer Security Division National Institute of Standards and Technology Gaithersburg, MD 20899-8930November, 1999.
21. Lee, A. Guideline for Implementing Cryptography in the Federal Government, NIST SP 800-21. National Institute of Standards and Technology,November,1999.http://csrc.nist.gov/publications/nistpubs/800-21/800-21.pdf.
22. "Public-Key Infrastructure (X.509)" Visited at (pkix): http://www.ietf.org/html.charters/pkix-charter.html. [Dartmouth PKI, 2013]
23. X.509 Certificate Policy for India PKI, Controller of Certifying Authorities Department of Information Technology Ministry of Communications and Information Technology, December 2010.
24. C. Ryan Brewer, "CMS System Security and e-Authentication Assurance Levels by Information Type", CMS Chief Information Security Officer and, Director, Office of the Chief Information Security Officer,pp.1-6, March 30, 2011 – Version 4.0 FINAL.
25. Valentine (dardha) ndou, "e – government for developing countries: opportunities and challenges", EJISDC (2004) 18, 1, 1-24.