Security Model in E-government with Biometric based on PKI

Jaafar.TH. Jaafar
Institute of Statistical Studies and Research Department of Computer and Information Sciences
Cairo, Egypt

Nermin Hamza
Institute of Statistical Studies and Research Department of Computer and Information Sciences
Cairo, Egypt

Bahaa Eldin M. Hassan
Chairman at Arab Security Consultants

ABSTRACT
With the growth of Information Technology and the Internet, governments apply the same principles and technologies that are supporting E-business revolution, to achieve similar transformation. Security becomes necessary to protect the citizens and government information.

In this paper a model has been proposed to obtain security services in the E-government based on Public Key Infrastructure (PKI). To achieve more security levels, Biometrics and Hardware token are used.

Keywords
Security, Token, Biometric, Cryptography

1. INTRODUCTION
The using of e-government services increases the needs of the user information and privacy. To accomplish E-government security there are three security issues must be considered which are: authentication, authorization and non-repudiation. The main methodology to get it is to apply Public key infrastructure (PKI).

Through this research, it has discovered that there are many people who deal with PKI and E-Government such as, **Ali Shayan…etc. at 2008,[9]**, explain the importance of information security requirements during each stage of the e-government. In the results, the importance of twenty selected items was illustrated, and the most and least important practices in each stage based on the expert's opinions and the statistical data analysis were explained, but it comprehensive and the model will not generally applicable to all organizations.

At 2012 ,Phi1D'Angio….etc. [10], began in the analysis of the characteristics of successful projects PKI led by government organizations. examine E-Government project based on PKI suggested the approach for Government PKI programs emphasize strong collaboration use cases. It also examines the characteristics of PKI projects that were not successful in the past. But has not been implemented this application in the e-government system.

Ali M. Al-Khouri, 2012, **[11],** Discusses Multi-Factor Authentication, support varying strengths of authentication i.e., 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. The use of the smart ID card for physical authentication and data capture has shortened for example the process cycle of service delivery at one public sector organizations (i.e., Dubai Courts) takes less than 7 seconds, in past it takes from 7 to 10 minutes. And clarify the PKI, the ID card need materials such ID reader which need money.

DaeyoungHeo,2012,[12].suggested Some protocols and challenges that came as alternative certificate validation method which translates the original certificate of national PKI to grid credential on separate GSI (Grid Security Infrastructure) and delegate the translated credential to grid service by an extended(OAuth protocol). The proposed idea is implemented in service called SecureBox (which is implemented based on the alternative certificate path validation method described in the previous section. SecureBox allows users to login to original GSI of grid by national PKI certificate). GSI can now adapt a reliable certificate issuance process including nationwide RA system from national PKI by the service, but did not explain how the citizens use it, just explain Protocol.

This paper will be divided into sections; section 2 will introduce a brief about the Public Key Infrastructure and Biometrics. Section 3 will present some related work in security of e-government. The proposed model will be presented in section 4. And finally section 5 gives the results.

2. PUBLIC KEY INFRASTRUCTURE AND BIOMETRICS
2.1 PKI
The basis on which governments can execute transactions safe and reliable whether between individuals, governments businesses, governments or inter-government relationships is PKI. It Allows public entities to securely authenticate all participants in a transaction [2]. PKI could be defined as: the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks [3]. PKI combine 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 **[4].**

Certificate holders will obtain their certificates from different CAs; Certification Authority; depending upon the organization or community in which they are member **[5].** A PKI is typically composed of many CAs linked by trust paths. A trust path links a relying party with one or more trusted third parties. Figure 1 illustrates PKI Architectures.

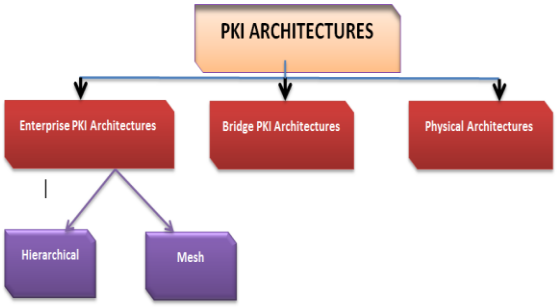

Fig 1: PKI Architectures.

Two basic data structures are used in PKIs. They are the public key certificate and the certificate revocation lists. A third data structure, the attribute certificate, may be used as an addendum [6]. Figure 2 illustrates PKI Data Structures.

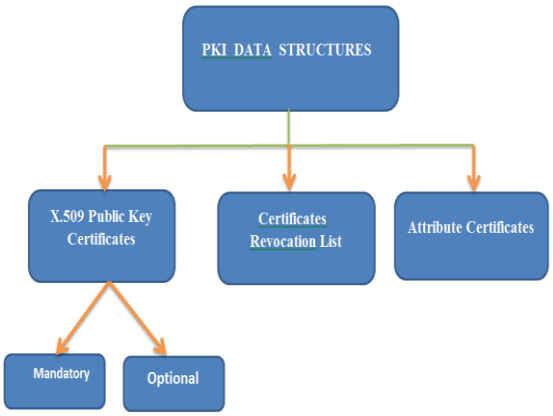

Fig 2: PKI Data Structures

2.2. Biometrics

Systems are tightly linked to a person because they can use a certain unique property of an individual for identification and/or authentication. which are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioural characteristic **[7].*The common Physical characteristics are:*** Fingerprint, Face, Retina, Iris, Vein pattern and Hand and finger geometry.

Behavioral characteristics are: Keystroke dynamics, Voice, Gait and Signature dynamics.

Biometric systems are tightly linked to a person because they can use a unique property of a certain individual for identification and/or authentication. While a person's biometric data can be deleted or altered the source from which they have been extracted can in general neither be altered nor deleted **[8].**

3. PROPOSED MODEL

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

The first one is selection of PKI cause this methodology based on the certificate and digital signature that ensure the authentication and non-repudiation security services, which we need to obtain in e-government system.

Issuing the biometrics is the second one, and differentiates between biometrics parts have been known by DaeyoungHeo and Suntae Hwang [13].

Through our study about Biometric characteristics and comparisons with Biometric parts we choose the fingerprint. Fingerprint is accomplishing some accuracy. Fingerprint is suitable for E-government applications cause it is the most economical biometric PC user Authentication technique, Easy to use, small storage space required for the biometric template, reducing the size of the database Memory required ,standardized, and one of the most Developed biometrics

And the third issue is using hardware security device. We choose hardware token; token is a physical device that an authorized user of computer services is given to aid in authentication. Advantage of the token: can be modified while in use, simple / Inexpensive to use, ensures all students get Fair treatment, reinforcing basic math skills, Teaches self-discipline.

Some people preferred to use the smart card but it noticed that a token has a lot features more than smart card. The smart card takes much time to read data from because it needs reader device while the token need no device except USB socket. Login the site through a token much faster than the smart card. Token is clearly and Chip in the smart card can be scratched while the token does not scratched.

The proposed model is based on two main levels they are to register and verification. The both levels will be discussed at the following:

3.1. Registration

This level is face-to-face level; it needs a meeting between user and the central government which act as 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 3 illustrate the register steps. The following steps discuss figure 3.

1. The user Request Certificate from the Registration Authority and Registration Authority (RA) Verify User.

2. Registration Authority Vouch for User to the Certification Authority.

3. Certification Authority Issue Certificate to user.

4. Certification Authority Stores Certificate to Repository (for future use the user because maybe he lost).

5. Registration Authority takes PIN & Fingerprint form User.

6. Registration Authority store Certificate & PIN & Fingerprint on Token.

7. Registration Authority Store PIN and Fingerprint on Repository (for future use the user because maybe he lost).

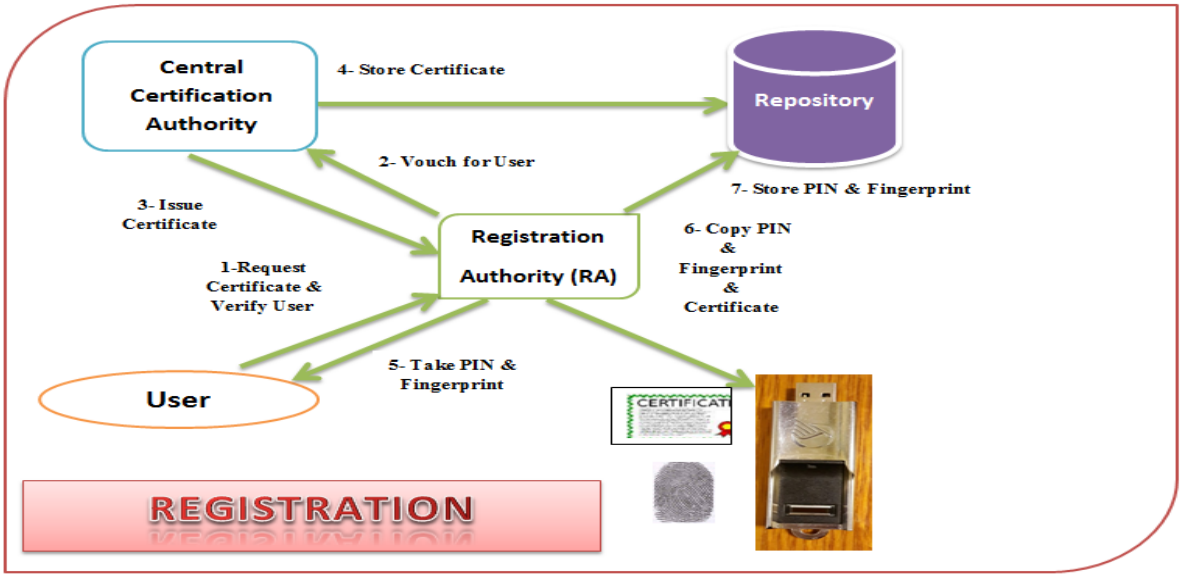

Fig 3: Registration (PIN & fingerprint & certification).

3.2 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 4 illustrate the steps of verification level. The steps will be discussed as following:

1. Verify User by PIN and then by fingerprint reader that Collect Biometric Data.

2. Verify quality fingerprint if Quality Sufficient then generates the template, if not then new biometric sample is requested.

3. Verify fingerprint by match 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. As explained in Figure 5 below.

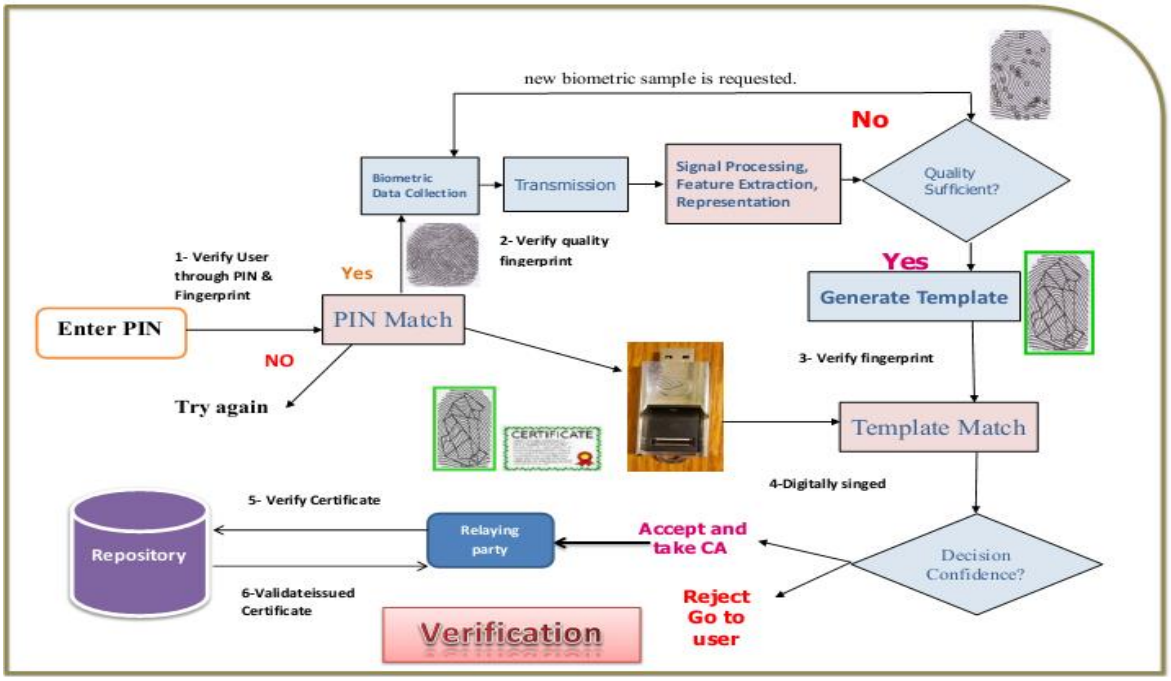

Figure 4: Verification (PIN & fingerprint & certification).

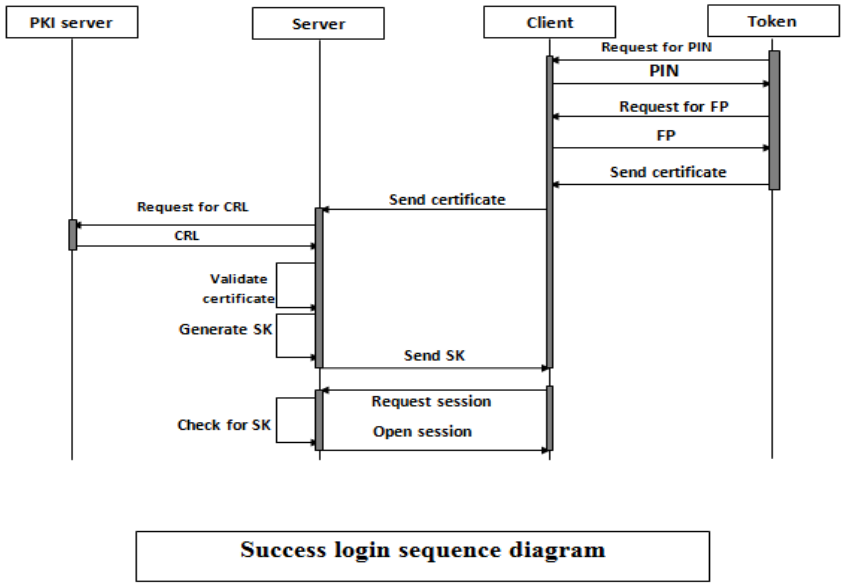

Figure 5: Explain step 5 and 6, relaying party.

- We can collect one scheme ways to illustrate the workflow, but through drawing. As explained in Figure 6 below

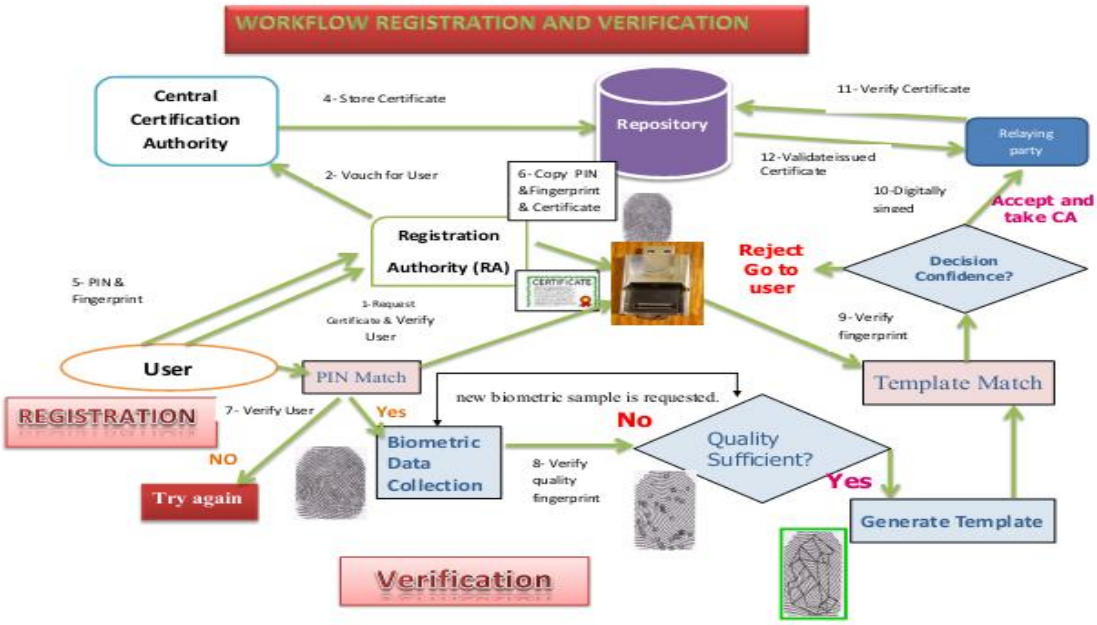

Figure 6: the workflow Registration and Verification

E-government must provide security during the high exchange of documents between the user and the server. The user login in website E-government should have a high security on Web content, including documents, as well as how to transfer these documents between the government and the user. So it must to provide trusted transfer process, according to our study and applications, which applies these days through the digital signature using the private key and public. We will explain how to be used and documentation among the governments in order to provide a safe environment for the protection of government data in the server. Initially the digital signature must be achieved from the provision of key public and private, which are stored on Token. After making sure the user opens the website of government, there are many services for e-government; we will take one of them, in the issuance of the passport. for example, if the user needs to issue a passport he will go to the site of Ministry of the Interior and then goes to the name of the application in the issue of a new passport and ask the server to open this application and the server opens application, The user fill application with his information, at the end the user puts his digital signature at the end of the application. Then encrypts this application or document with the private key that is stored in Token and sent to the server to verify the user as well as to achieve Confidentiality, Authentication, integrity and non-repudiation. The server verify the user process to decryption using the public key of the user and if the user is already active it, a server will send messages agree the process and give him a date for the receipt of the passport, as shown in Figure 7 below.

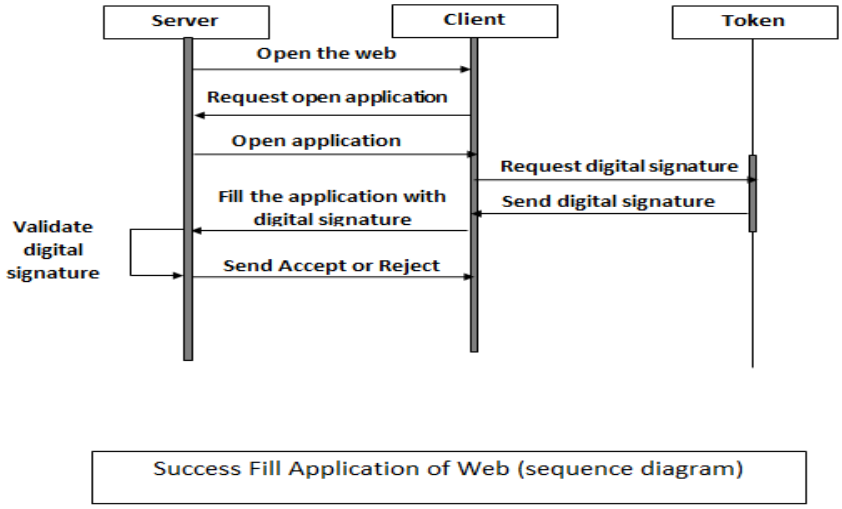

Figure 7: Success Fill Application of Website

4. EXPERIMENT

Through our study, it is clear that e-government is a great thing in providing assistance to citizens so our focus was to provide security to the service using the technique of user authentication and data transfer security. Through the application of our token using PIN code, fingerprint and the digital certificate the give us the highest security, and compared with the smart card, there is a big difference in time in terms of make sure from person takes less than 3 seconds in the token and smart card takes less than 7 seconds, and this difference in the science of accounts.

As well as the applied file transfer between the citizen and the server, which is done through the digital signature on the file and give us the results of which will be in the case of encryption and signature on file when the home is as shown in Figure 8 below.

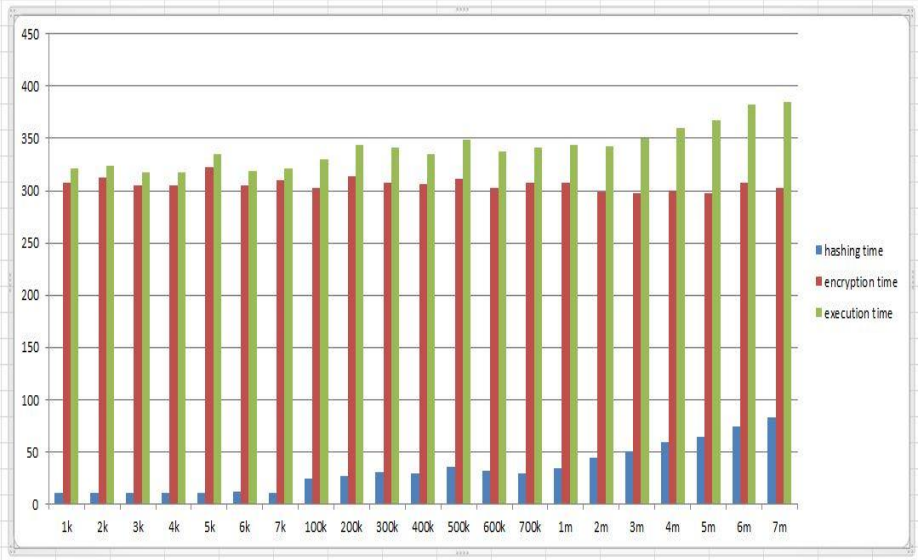

Figure 8: Comparing a hash, encryption and execution time

In the case of decryption, and the comparison that the user effective or not effective,

and the response to the user's acceptance or rejection of the results were as shown in Figure 9 below.

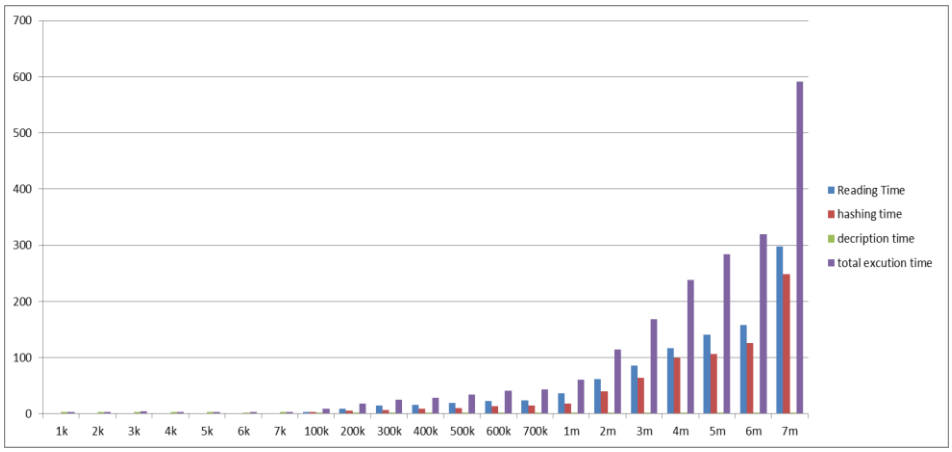

Figure 9: Comparing a reading, hash, decryption and execution time

5. CONCLUSION

In the proposed work we have created a security model to achieve higher security through authentication, non-repudiation, and encryption of information, as well as take a little time to verify user and achieves trust between the user and the party responsible. And this based on PKI Issued digital certificates and digital signature and etc. Which is the basis of our work, as well as on Biometrics a fingerprint that is easier type of Biometric, and stores all these parts in the token, which we explained its features and the difference between it and the smart card, And this made us less time with high security where it takes about 3 seconds.

The future work, we are implementing this model in the field of e-government, and there many of the areas that can be

applied for example in the field of e-health, e-learning and e-voting.

6. REFERENCES

[1] RICHARD HEEKS ,I Government, Centre for Development Informatics, Institute for Development Policy and Management, SED University of Manchester, Arthur Lewis Building, Manchester, M13 9PL, UK,2010.

[2] NATIONAL PKI: THE FOUNDATION OF TRUST IN GOVERNMENT , Symantec World Headquarters 350 Ellis St. (2011).

[3] D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang, "Introduction to Public Key Technology and the Federal PKI Infrastructure", National Institute of Standards and Technology, 26 February 2001.

[4] Matti Järvinen, PKI Requirements for IPsec, helsinki university of technology department of computer science and engineering,2003.

[5] RFC 2104 HMAC: Keyed-Hashing for MessageAuthentication.http://www.ietf.org/rfc/rfc2104.txt, visited Jun. 2014.

[6] Lee A. Guideline for implementing cryptography in the Federal Government, NIST SP 800-21. National Institute of Standards and Technology November, 1999.

[7] Anil Jain, 50 Years of Biometric Research : Almost solved, The unsolved, and the Unexplored, Michigan State University ,Jun 5,2013.

[8] **Biometric-S-2013,** [Online] Retrieved from:http://www.biometric-security-devices.com/facial-biometrics.html,Facial Biometrics An Excellent Time Attendance And Tracking Option, [Accessed: 2 NOV 2013].

[9] Jacob KOHNSTAMM, Done at Brussels, on 27 April 2012,Opinion 3/2012 on developments in biometric technologies, Website: http://ec.europa.eu/justice/data-protection/index_en.htm.

[10] Ali Shayan, BehnamAbdi, and MaliheQeisari,,identify the importance of information security requirements during each stage of the e-government maturity, 2008.

[11] Phi1D'Angio .PanosVassilliadas• Phaidon Kaklamanis, PKI - Crawling Out of the Grave &Into the Arms of Government,2010.

[12] ali m.al-khouri, pki in government identity management systems , Emirates Identity Authority, Abu Dhabi, United Arab Emirates. ali.alkhouri@emiratesid.ae,2011 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, July, 2012.

[13] Ali M.Al-Khouri, eGovernment Strategies The Case of the United Arab Emirates (UAE), European Journal of ePractice · www.epracticejournal.eu,Nº 17 · September 2012.

[14]