Development of Certificate Authority Services for Web Applications

Sufyan Faraj Al-Janabi
College of Computer
University of Anbar
Ramadi, Iraq
sufyantaih@ieee.org

Amer Kais Obaid
Dept. of Control and Computer Eng.
University of Technology
Baghdad, Iraq
eng.amerkais@gmail.com

Abstract—**The most important security services are confidentiality, integrity, authentication, and non-repudiation. When designing a communication system, the security services of this system must be defined. The Public-Key Infrastructure (PKI) is a technology that can meet these security services with its techniques and standards. A PKI system works by having a Certificate Authority (CA) for issuing public-key certificates. The aim of this work is to design and implement a CA system that can create and assign public key certificates. Hence, the system enables secure communication and proper authentication. Besides the basic security requirements, the developed system uses an approach that can contribute in facilitating the revocation of the certificates. It also gives these certificates additional security/performance advantage by using the Elliptic Curve Cryptography (ECC) instead of the RSA cryptography. The design and implementation of the proposed system have been achieved using PHP and HTML programming languages besides MySQL database server and Apache web server.**

Keywords- authentication; certificate authority; elliptic curve cryptography; public key infrastructure; web applications

I. INTRODUCTION

The Internet provides an excellent vehicle for extending the scope of communication and business. As all information sent to the Internet is basically public, the need for security becomes critical. The most critical element of security might be the ability to provide trust and confidence to transactions over the Internet. To accommodate the scale of transactions across the Internet, some of the few technologies that can accomplish this include Public Key Infrastructure (PKI). PKI can be viewed as critical not only to the commercial sector but also to the government sector. As a result, many aspects required for successful PKI, such as insurance and legal aspects, have been greatly improved. The Public-key system makes it possible for two parties to communicate securely without either having to know or trust the other party. However, this is only possible because a third party that both the other parties trust identifies them, and certifies that their keys are genuine [1].

This third party is called the Certificate Authority (CA). CA guarantees that they are who they claim to be. The CA does this by registering each user's identification information, and issuing them with a set of Private keys and a set of Public Key Certificates. Various institutions and corporations can utilize this security technology to satisfy current business needs. Many institutions are choosing to manage their own Certificate Authority (CA) instead of outsourcing this function to a third party (like Verisign, Thawte, GTE CyberTrust, and GlobalSign) [2].

The authentication system is the first line to prevent unauthorized users from gaining access to the system [3]. Authentication is mechanism by which a process verifies the communication partner is who it is supposed to be and not an imposter. Authentication can be accomplished in many ways. The importance of selecting an environment appropriate authentication method can be one of the most crucial decisions in designing secure systems. Authentication protocols are capable of simply authenticating the connecting party or authenticating the connecting party as well as authenticating itself to the connecting party [4]. Authentication can be based on different types of authentication tokens. Authentication tokens are normally categorized in two categories: something known and something possessed [5].

The advantage of public-key cryptography is that the public key is readily available to the public. Usually, public-keys are published to public directories on the Internet so that they can be easily retrieved. This significantly simplifies key-management efforts. The integrity of the public key is of the utmost importance. It can be assured by completion of a certification process carried out by a CA. Once the CA has certified that the credentials provided by the entity securing the public key are valid, the CA will digitally sign the key. Hence, the users accessing the material that the key is protecting will know that the entity has been certified [4].

In the literature, there are already some good representatives of developed web applications which contribute to PKI and CA development (See for example [6] - [10]). These works differ in their scope and implementation techniques. It is of crucial importance to consider the common practices around the world. However, we have to adopted the best one for our situation. Thus, this work reports on the development of secure and efficient PKI-based CA services for the Web environment. The developed Certification Authority system is based on three-tier hierarchical Client/Server model.

978-1-4673-0260-9/12/$31.00 ©2012 IEEE

The functional part of the system is written by using PHP (Hypertext Preprocessor) server language, MySQL database management system engine is used to handle the related task, and Apache server is used as a web server.

II. PUBLIC KEY CRYPTOGRAPHY

In order to solve the key management problem of symmetric cryptography, public key cryptography was introduced in 1976. Public key (or asymmetric) cryptography uses a key pair, "private" and "public" keys. The private key is kept secret while the public one is published in a common directory so that everyone can access it. The relation between the key pair is that when a message is encrypted with one of them, it can only be decrypted with the other. It is mathematically infeasible to derive the private key from the public one. So that, the sender (Alice) encrypts her message with the recipient's (Bob's) public key and the receiver can decrypt the message with his corresponding private key. Because of the large key length and the nature of the public key algorithms, public key systems are slower than symmetric key systems. Thus, it is not recommended to encrypt long messages with public key cryptography. Instead of this, the key used in the symmetric cryptography is encrypted with public key cryptography, then the message is encrypted with a symmetric key system.

Among the widely implemented public key systems are the RSA and the El Gamal systems. In recent years, Elliptic Curve Cryptosystems (ECC) have also been emerged. The RSA system is widely adapted by both the industry and the international standards community for public key cryptography implementations. However, in this work, we will use the ECC because with a much smaller key length, it achieves the same security level as other peers. In fact, ECC presents some key attributes truly important in scenarios where some resources are limited such as: processing power, storage space, bandwidth, and power consumption [11], [12].

ECC was discovered in 1985 by V. Miller as an alternative method for public key cryptography. At that time, it was very difficult to perform the necessary calculations. Later, implementations became much more efficient. This enabled the performance of ECC to take the same amount of time as implementations of integer factoring schemes for the same number of bits, which in turn implies a reduction in cost, size, and processing time because elliptic curves require fewer bits for the same security level. As the bit length for secure RSA use has increased over recent years, this has also put a heavier processing lean on applications using RSA. This burden can be serious, especially for e-commerce sites that conduct large number of secure transmission. Hence, ECC are gaining more and more attraction [5], [13].

The ECC is unlike earlier cryptosystem, an elliptic curve works with a finite Abelian group formed by the points on an elliptic curve defined over a finite field. ECC can be used for key distribution, encryption/decryption, and digital signature algorithm (DSA). The key distribution algorithm is used to share a secret key for symmetric cryptography, the encryption/decryption algorithm enables confidential communication, and the DSA is used for authentication and validating the integrity [14].

III. PUBLIC KEY INFRASTRUCTURE

Public Key infrastructure (PKI) is "the combination of software, encryption technologies, and services that enable enterprises to protect the security of their communication and business transactions on networks." PKI enables users with no preexisting relationship to communicate securely regardless of the distance between them using a commonly shared certificate known as the chain of trust. PKI allows organizations to enjoy the basic services of confidentiality, data integrity, authenticity, and non-repudiation. PKI permits these by offering a way of identifying and trusting another Internet user, through the use digital certificate. This digital certificate is like a passport. It contains the Internet user's name and some other credentials (The content of digital certificates depends on the organizational policies and some other private issues). A digital certificate can also be used to verify a digital signature, which can be attached to e-mail messages or other types of electronic messages. This signature is created using public key cryptography [15], [16].

In general, PKI system mainly consists of a CA that accepts user requests for a certificate. The CA also acts as the authority, which issues and manages security credentials and public keys for message encryption. The organization of the components of any specific PKI system can vary depending on the application of the system. These components typically include: end-users, Registration Authorities (RA), Certification Authority (CA), Public Key Certificates (PKC), Certificate Repositories (CR), Certificate Policies (CP), and Certificate Practices Statement (CPS) [17]. Below is a summary of the functionalities of these components:

1. The End-users: The end-users are the people who are using the system. They are the key element of the system since application, policies, and practices are built up for them. In general, the end-user may request certificates from a CA, receive the certificate from the CA, and then use the certified keys and certificates in PKI enabled application services.

2. Registration Authorities: A Registration Authority (RA) is an optional but common component of a PKI. An RA is used to perform some of the administrative tasks that a CA would normally undertake. The main purpose of an RA is to verify an end user's identity and determine if an end entity is entitled to have a public key certificate issued. Many PKI implementations separate the operations performed by the CA and the RA to avoid the complexity of tasks.

3. Certification Authority (CA): It is a trusted authority in a network that issues and manages security credentials and public keys for message encryption. As part of a PKI, a CA checks with a registration authority to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a digital certificate. Indeed, the CA is responsible for the distribution and revocation of the certificate. Depending on the PKI implementation, the

certificate might include the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner [18].

4. Public Key Certificates (PKC): A Public Key Certificate or a "digital certificate" is an electronic set of credentials for an individual that offers proof of identity. The digital certificate contains information like the name, organization, expiration date, and the subject's public key and a digital signature of a trusted third party. Any entity that wants to use any certificate, first checks the validity of the digital signature contained in it. There are many certificate types, such as X.509 Public Key Certificates, Simple Public Key Certificates (SPKC), and Pretty Good Privacy (PGP) Certificates [19], [20]. All these certificate types have their own data structures. Due to its widespread use in most PKI systems, our work has adopted Version 3 of X.509 public key certificates. Fig. 1 illustrates the structure of an X.509 v3 certificate [21]. However, it is important to note that there is no one single definition of a public key certificate defined in the IETF standards. Vendors and integrators have their own ideas on what extensions and particular data an X.509 certificate should contain. Hence, it is preferred that each organization evaluates its business needs relative to the constructs of the public key certificates that it wishes to issue.

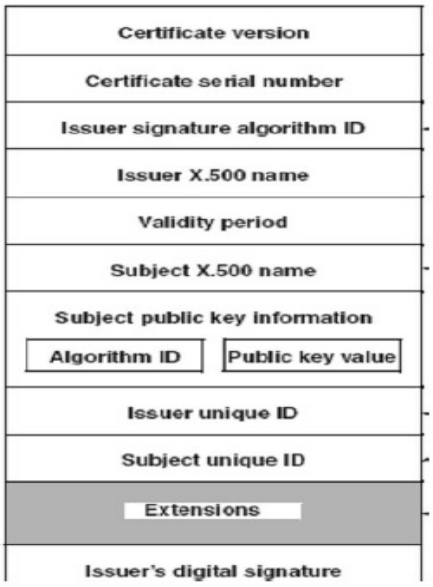

Figure 1. X.509 V3 certificate [21].

5. Certificate Repositories (CR): A certificate repository (or a certificate directory) is an optional but common component of a PKI. It can simply be posted on a public web page, and put in a database or some other form. Besides the certificates, other PKI related information such as Certificate Revocation Lists (CRL) can be stored in the repository [22].

6. Certificate Policy (CP): It is a documented set of rules and commitments made by a CA to indicate the applicability of a certificate to a particular group of users or set of applications. The main purpose of CP is to determine the security policy that is followed by a certification organization. Also, it can be used as a reference for other organizations that need to establish a domain-trust relation with this organization.

7. Certificate Practices Statement (CPS): The CPS is a statement of the practices that a CA employs in issuing public key certificates. The CPS document enumerates the procedural and operational practices of a PKI [21].

IV. THE PROPOSED SYSTEM

The proposed architecture is based on a three tier model; it is adopted instead of the two-tier (client/server) model, in response to the limitations of (client/server) architecture [23]. The proposed system has been built using the following tools:

i. PHP (Hypertext Preprocessor) which is a computer scripting language (server-side scripting), originally designed for producing dynamic web pages.

ii. HTML (Hypertext Markup Language) which is the predominant markup language for web pages. It provides a means to describe the structure of text-based information in a document and to supplement that text with interactive forms and embedded objects.

iii. MySQL which is a relational database management system (RDBMS) based on SQL (Structured Query Language).It is used in a wide range of applications.

iv. The Apache Server which is a web server notable for playing a key role in the initial growth of the WWW. It is available for a wide variety of operating systems, including Unix, Linux, and Windows. It can be used to serve both static content and dynamic Web pages on the WWW.

v. Additionally, and in order to test the operation of the proposed system on local computer before uploading it into the Internet, It has been required to configure the computer as a local server to deal with PHP language and MySQL database. The PHP Traid (v2.11) software has been used for this job.

Besides the major security requirements that should be covered by the proposed CA system, the following considerations have been also taken into account:

- Multi-level login includes the following levels: new-visit to the website, additional visits to check and update of the personnel Information, and entrance by authority staff (authorized employee).
- Secure and easy way to update some of applicant information.
- Secure and flexible way to handle the revocation of the digital certificate by the applicant.

The proposed system is a web application which consists of the following components: client tier, server tier, and Database tier. Fig. 2 shows a general block diagram that illustrates the structure of the proposed system. The users (applicants or authority staff) can access the data on the server through any popular web browser (like Internet Explorer or Netscape). To

build this system a number of sub-programs were built using several programming languages. In general, the presentation of services or the user interface logic is located on the client machine. The server logic is placed in the middle tier (server tier). The data services tier contains the database server. The basic concept of the three tier model is partitioning the system functionality into layers, so applications gain scalability and security. The whole system operation can also be divided into three main phases:

- Phase 1: The management of the digital certificate by the Applicant.
- Phase 2: The management of authenticating the applicant data by Registration Authority staff.
- Phase 3: The management of the information in database by the Certification Authority staff.

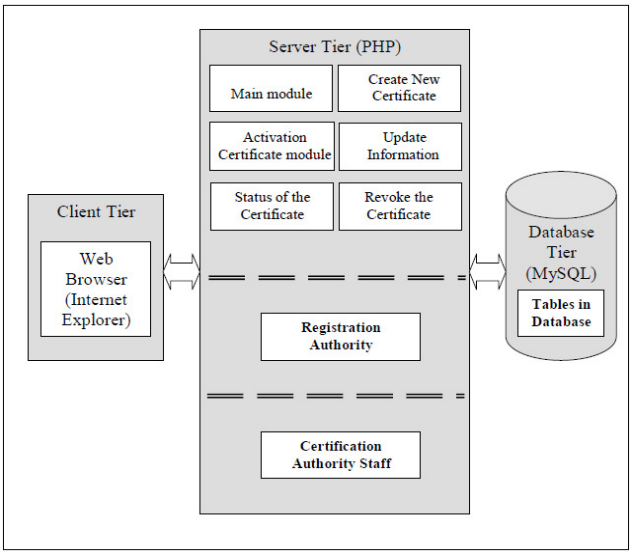

Figure 2. The general structure of the proposed 3-tier architecture model.

A. *Applicant Main Module*

The main flow steps of the applicant main page are shown in Fig. 3. The applicant can select one of the following five processes: create new certificate, activation of the certificate, update information, check status of the certificate, and revoke the certificate. Fig. 4 shows the flowchart of creating a new certificate process. As a first step the applicant requests to create new certificate, the client computer sends this request to server. After that the server will send the web-page " Authentication of the applicant identity" to the client computer. When the web browser presents the web-page contents, the applicant should fill the fields with his Authenticate information and send it to server.

After the applicant new submission is initially accepted by the CA system, the system tells him/her to visit the same site after a period of time to check if the request was accepted or rejected. Once the applicant is informed through the "Activation of the Certificate" webpage about the acceptance of the certificate request, the user can activate his/her certificate and use the assigned private key. The "Update Information" process is activated when the applicant wants to update some of his personnel information in the CA database. The server asks the user to make the allowed changes through the "update information" webpage. This webpage contains only the personnel fields which can be changed and it will appear when the server identifies the applicant identity and loads the record from the database.

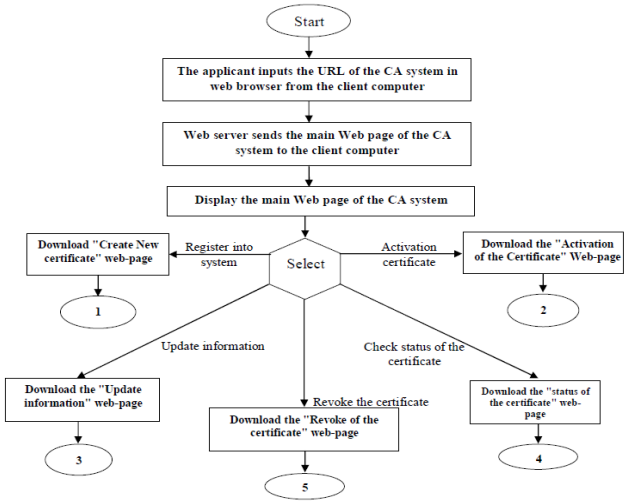

Figure 3. The flow steps of the system.

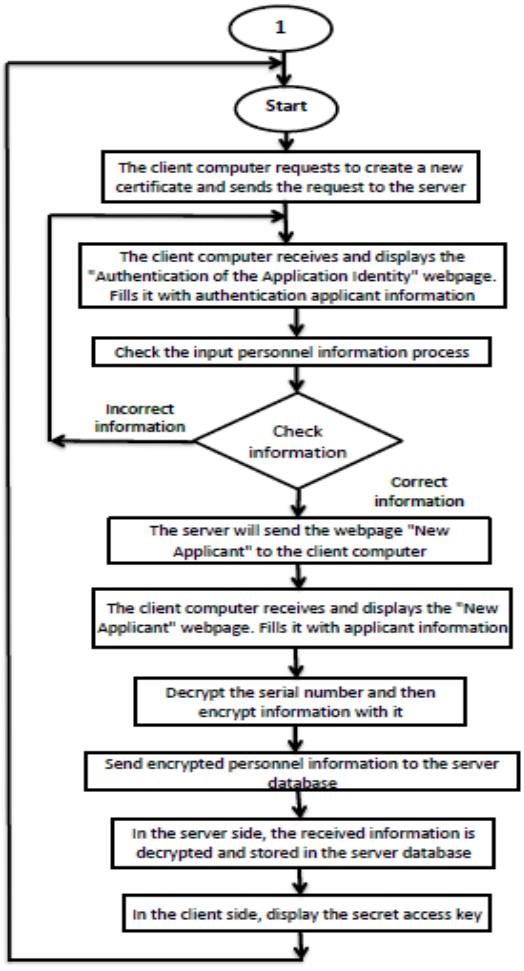

Figure 4. The system flowchart for the process of "Create New Certificate".

When the user wants to check status of the certificate of the other user if it has validity or not, he/she can visit the "Status of the Certificate " webpage and fills available fields with the information that is assigned to this certificate. After sending the correct information to server and checking it in database, the system will display the status of validity of this certificate. In addition, if the user lost his/her private key or challenge phrase, the certificate might be used by another person for malicious purposes. In this case, the user must revoke his certificate to avoid this problem. In this work, we propose a way in which the revocation of certificate process is down directly by the client. The advantages of this way are:

i. It decreases the time that required to revoke the certificate since It does not need to communicate with the CA before revoking the certificate.
ii. There is no need to publish the RCL in certificate repository, because the process is done between the client and the certificate repository.

The flowchart for "Revoke the Certificate" is shown in Fig. 5.

B. Authorized Staff Module

To operate the CA system with high efficiency and flexibility, there is a need to manage its services by the authority staff. There are two types of authority staff. The first is RA staff which is responsible for registering the authenticated applicants information in the database for authenticating the identity of the applicants. The second type is the CA staff who is responsible for CA system management. To access the CA system by the authority staff, each one of them should enter his private secret information which authorizes him the privilege to access the part of the system, and the server will check the passwords, in the authority staff database. If the server finds the staff member's password matches what is registered in the database, the server will send to client (officer) computer the authorized officer webpage. If the system considers the request invalid, then it will send an error webpage.

V. PROTOTYPE IMPLEMENTATION

A prototype implementation of the proposed system has been done for university registration example application. When someone (like a student) wants to get a digital certificate for accessing certain university resource, he/she can use this system. As a starting step the user needs to (directly) contact the RA and register by filling the authenticate applicant form with the required information. Thus, the user can get from the RA officer the secret number for connecting to the CA system online. Fig. 6 illustrates the main webpage for the applicant when accessing the CA system services. Thus, the user can decide to create new certificate, activate the certificate, update information, check the certificate validity, or revoke the certificate.

For example, when the user wants to get digital certificate through the system, he/she should click on the first button (Create New Certificate). Then, a new page (Authentication of personal identity) will appear. This page consists of four fields: full name, secret number, birth date, and nationality. The snapshot shown in Fig. 7 depicts the contents of this webpage. Once the applicant enters all the required information, this information will be sent to the server for integrity and consistency check.

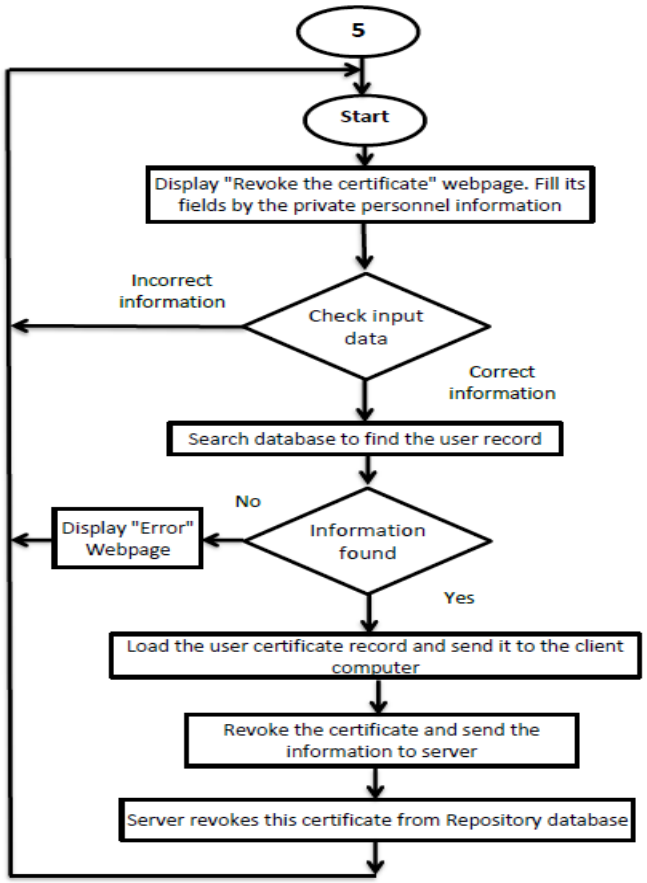

Figure 5. The flowchart for the process of "Revoke of the Certificate".

Figure 6. The prototype main webpage "University of Technology CA main page".

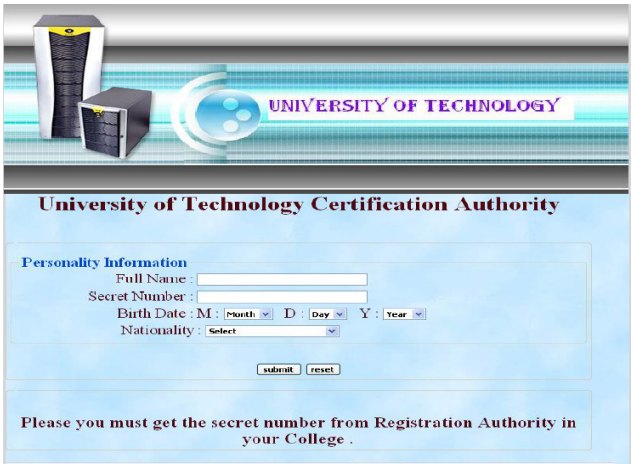

Figure 7. The "Authentication of applicant identity" webpage.

Concerning the authority staff, if for example, the CA officer wants to check some information about a new applicant who has recently registered in the database, the CA officer can according to his privileges enter the system and see the related database records, as illustrated in Fig. 8.

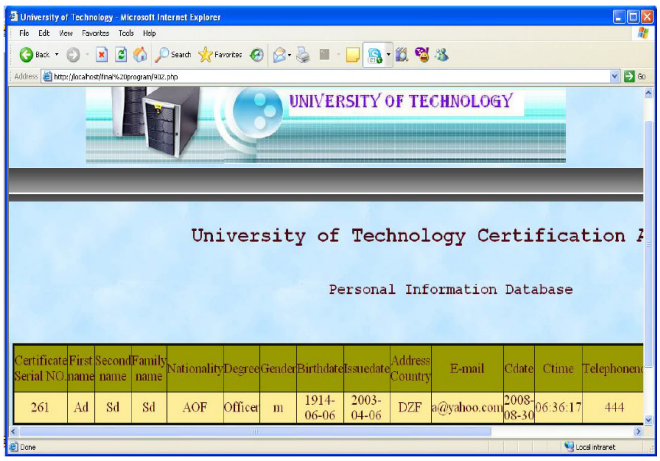

Figure 8. The records of "New Applicants" webpage.

CONCLUSION

The proposed system enables institutes or organizations to issue digital certificates for their network users. The applicant can manage his digital certificate from any computer that is connected to Internet. The system assumes a way that the revocation of the certificate is done directly by the client. The main advantage of this method is to decrease the time needed to acknowledge the CA to revoke it and publish it in certificate repository. However, the current system implementation considers only one domain of trust (i.e. all clients trust one Authentication server).It is important to extend the design to provide cross domain trust or hierarchical domain trust. For example, the system can be extended to be implemented in multi-institutes environment connected to root certification authority.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security Principles and Practices*, Prentice Hall, 2003.

[2] V. Patriciu , "Design Aspects in a Public Key Infrastructure for Network Applications Security", August 2000.

[3] H. Wang, *Security Architecture for The TEAMDEC System*, MSc. Thesis, Department of Electrical Engineering, Virginia Polytechnic Institute, July 1999.

[4] R. Duncan, "An Overview of Different Authentication Methods and Protocols", Report submitted to SANS Institute, October 2001.

[5] K. Klemetti, *Authentication in Extranets*, MSc. Thesis, Helsinki University Of Technology, July 2001.

[6] R. Hunt, "PKI and Digital Certification Infrastructure", Department of Computer Science, University of Canterbury, New Zealand, IEEE, 2001.

[7] X. Zeng , C. Yang, "Design and Implementation of CA/PKI on the Windows Environment ", SCIS 2002.

[8] W. Zhao, "Implementation of Software Tools for The Medium-Size Certification Authority-X.509 Certificate", ECE Dept., George Mason University, December 2003.

[9] A. Parvez, *Design and Implementation of Public Key Infrastructure: a Proposed Solution for Bangladesh*, MSc. Thesis, Independent University, Bangladesh, May 2006.

[10] A. Majid, *Implementation of Distributed Database for Electronic Visa System*, MSc. Thesis, Iraqi Communication for Computer and Information, September 2006.

[11] N. Potlapally, S. Ravi, A. Raghunathan, N. K. Jha, "A Study of The Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols", IEEE Transactions on Mobile Computing, Vol. 5, No. 2, 2005.

[12] W. Rao, Q. Gan, "The Performance Analysis of Two Digital Signatures Schemes Based on Secure Charging Protocol", International Conference on Wireless Communications, Networking, and Mobile Computing, Vol. 2, September 2005.

[13] A. Jurisic and A. Menezes, *Elliptic Curves and Cryptography*, 2005.

[14] Certicom Corp., "The Elliptic Curve Cryptosystem", A Certicom White Paper, 1998.

[15] H. Ray, "Technological infrastructure for PKI and digital certification". J. Computer Communications, University of Canterbury, Vol. 24, No. 14, 2001.

[16] L. M. KohnFelder, *Towards a Practical Public-key Cryptosystem*, B.S. Thesis, Massachusetts institute of technology, May 1978.

[17] S. Kiran, P. Lareau and S. Lloyd, "PKI Basics - A Technical Perspective", November 2002.

[18] B. Lee, "Certificate authorities: Who Do You Trust?", Data Communications, vol. 27, no. 4, March 1998.

[19] E. Yildiz, *A Proposal for Turkish Government Public Key Infrastructure Trust Model*, MSc Thesis, December 2001.

[20] P. Zimmermann, "The official PGP User's Guide", Cambridge, MA, MIT Press, 1995.

[21] S. Choudhury, K. Bhatnagar, and W. Haque, *Public Key Infrastructure Implementation and Design*, M&T Books , 2002.

[22] D. Kopparhed, "A Secure Model for Certificate Distribution and Management for Dynamic Access Control", August, 2007.

[23] E. Trichkova, "Application of PHP and MySQL for search and retrieval Web services in Web information systems" Proceedings of First International Conference on Information Systems, Sofia, Bulgaria, February 2005.