Secure Framework for e-Government Application using Short-Lived Certificate and Hybrid Encryption

Aye Aye Thinn
Joint Secretary
Myanmar Computer Federation
ayeayethinn@gmail.com

Mie Mie Su Thwin
Associate Professor
mmCERT, Ministry of Science & Technology
miemiesuthwinster@gmail.com

Abstract

Although electronic documents have been greatly widely used in different applications including the e-government and e-business, it would also result that electronic documents information is disclosed, counterfeited, tampered, repudiated and so on. Some of the e-Government applications may require providing user access in short limited time. Besides that sending and receiving back information must be secured and confidentiality and integrity must be guaranteed for the users. In order to solve the problems and greatly improve the security of electronic documents, a hybrid encryption technology, that is, encryption technology, digital digest, digital authentication and digital signature will be used. This paper proposes an applicable solution for e-Government Applications (where users only need limited short time access and ensure the security, confidentiality and integrity of information being sent) by using the hybrid encryption technology together with a short-lived certificate framework.

Keywords- electronic documents, e-Government security, encryption technology, digital signature, digital certificate, short-lived certificate framework.

1. Introduction

The term e-Government is defined by the Organization for Economic Cooperation and Development (OECD) as the use of new Information and Communication Technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies have the potential to transform the structures and operation of government [3].

E-Government has received more and more importance and it can provide a non-stop government information service to citizens, enterprises, public officers, government administrations and agencies over the network. There are many issues in e-government which need a careful examinations such as security issues, service requirements of e-Government, e-Government model, strategy and policy for e-Government, and domain of e-government[4].

Public-key cryptography is based on the asymmetric key model, whereby a pair of complementary keys is used for encryption and decryption. It allows the communicating parties to authenticate each other without sharing secret information in advance. With public-key cryptography, each person gets a pair of keys, a public key and a private key. Each person's public key is published, while the private key is kept secret[5]. Public-key systems are considered more secure and scalable than secret-key solutions. As the support for X.509 digital certificate standardized in most web browsers and servers, public-key cryptography is emerging as the security solution for both the Internet and intranet applications [2].

The electronic of government documents transmission and processing has greatly improved working efficiency. However, because the network has openness, connectivity and other features, resulting the network vulnerable to be attacked by hacker and viruses, and also resulting in information of electronic documents disclosure, counterfeiting, tampering, repudiation and many other issues[1].

In realization of e-Government projects, security and integrity of data being send and reply back is vital requirement and there is a need to solve this requirement in any e-Government applications.

In order to improve the security and to guarantee the integrity of electronic documents, this paper tries to research a solution, that is, integrate encryption technology, digital digest, digital authentication and digital signature four kinds of technology during the transmission of data in intranet e-Government applications together with the use of short-lived digital certificates framework to control the validity of the user access.

First of all, we present about Requirements for the Proposed Solution. Short-lived Certificate and design of the proposed system are presented in Section 3 and Section 4. Advantages of the proposed solution are presented in Section 5 and finally, the last section is conclusion and further research directions.

2. Requirements for the Proposed Solution

There are e-government applications where the user requires a short time (may be one time) access to the system to get the information he/she wants from a Government Organization. Other requirements of the system are as follows.

Sender side

Authenticity of the Sender must be ensured to request the data from receiver.

Data sent by the Sender must be securely transmitted to the Receiver. There must be no alternation and data integrity must be maintained throughout the transmission.

The data he/she received must be guaranteed for no alternation and it must be ensure that it is really sent by the intended counterpart (Receiver).

Receiver side

Authenticity of the Receiver must be ensured to get access to the system.

The data he received from Sender must be guaranteed for no alternation and it is really sent by the Sender.

Data he/she sent must be securely transmitted to the Sender and no alternation during the transmission.

Nature of the application

The users of the system needs only a limited or short time (or one time) access to the system to get the information they want.

An example of the application may be 'Online Matriculation Exam Mark Certificate Application' where the Student(Sender) requests for the Mark Certificate of the exam and the Government Organization(Receiver) checks and send back his/her 'Mark Certificate' to the

Student. The student needs to apply for Mark Certificate only one time and it is usually requested after the result of the exam is announced (within short limited time). As the Mark Certificate will be one of the main documents when he applies for a University and the University considers the exam result as one of screening criteria to accept the student, the non-forgeability and integrity of data is main importance among other features.

To secure delivery of electronic data need to satisfy the following basic requirements: from the transfer object's view, we need to ensure the integrity and confidentiality of information; from the transfer subject's view, we need to protect the identity of nature to be certified, non-repudiation, unforgeability [6].

As there has no security solution proposed before for this kind of application, we would like to propose a solution that guarantee the security, integrity, non-forgeability and non-repudiation and also satisfy the short time access to the system.

3. Short-lived certificate

A PKI is a framework for the management of public keys and certificates that is responsible for issuing, maintaining, and revoking of the public key certificates over insecure networks, in particular the Internet. A PKI permits users of such networks to exchange data through the use of a public and private key pair that is obtained and shared through a trusted authority [6].

Generic structure of an X.509 Version 3 public key certificate(digital certificate) is shown in Table 1.

Version	Identifies the version of the Certificate (eg. V3)
Serial Number	Unique Integer Identifier for the Certificate
Signature	Algorithm ID used to sign the Certificate
Issuer	Unique Name of the Certificate Issuer
Validity	Not before and Not after validity times
Subject	Unique Name of the owner
Subject Public key Info	Public key(and algorithm ID) of the owner
Issuer Unique ID	Optional Unique ID of the Issuing Certification Authority
Subject Unique ID	Optional Unique ID of the Subject
Extensions	Optional Extensions
Digital Signature	Algorithm ID and digital signature

Table-1 : Structure of a digital Certificate

Under short-lived certificate framework, the validity of the certificates does not need to be many months. Since there is no long-term association between a client(user) and a certificate or public-key pair, the demand for key management is greatly reduced. There is no need for certificate revocation in this framework and minimal responsibility is placed on the client. As a result, user mobility can be securely implemented [2].

Depending on the nature of the e-Government application or Intranet applications, we can design to implement the PKI system based on the short-lived certificate framework rather than full PKI system.

4. Design of the Proposed System

Our Proposed Solution for authentication technique is both Sender and Receiver will require digital certificates to successfully login and securely send and receive data between Sender and Receiver.

In addition to secure login, digital certificates are used to digitally sign the data/document and to encrypt the data. On receiving side, digital certificate is used to decrypt the data and to verify the integrity of data being sent. Our solution also integrates the symmetric key encryption with PKI to improve the processing time and for efficiency of encryption/decryption process.

The Architecture design of the Proposed System is illustrated in Figure 1. Two main components are involved in this system, Application Server and Certificate Server. Application data will be stored in Application Database. Students' data that will be used to verify the student when he requests to issue a certificate will be stored in User Register Database. Certificate Server is used to issue the certificate and issued certificates will be stored in the Certificate Database.

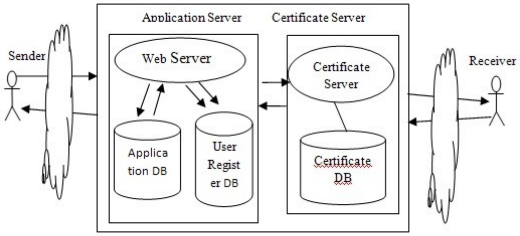

Figure-1 Over All Design of the Proposed System

The use case diagram of detailed design of the application for Sending Data and Verification is shown in figure 2.

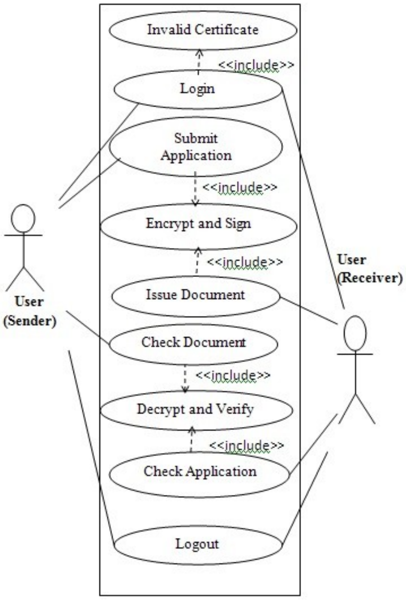

Figure 2. Use case diagram

Both Sender and Receiver require digital certificate(certificate) to login the system. So, they must apply for certificate before they use the application. First, the application will check the certificate used is valid or not and if not, it is rejected to request the data from the receiver. When the Sender requests for document(eg. Mark Certificate), his request will be signed and encrypted and then send to the Receiver. When the Receiver receives the request, he decrypts the data and check whether the digital signature is valid. If valid, he will send the document(ie. mark certificate) requested back to the Sender. The document that the Receiver sent will also be signed and encrypted. Finally, the Sender will decrypt and verify the digital signature to ensure the document integrity and confidentiality.

The proposed encryption process (from Sender to Receiver) is show in figure-3.

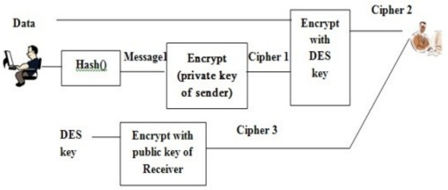

Figure 3. Encryption Process

The proposed decryption process at Receiver side to verify the data sent by Sender is show in figure-4. If the message-1 and message-2 are equal, the data integrity is maintained and there is no alternation during the transmission.

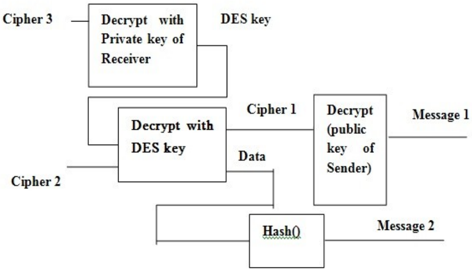

Figure 4. Decryption process

Through two steps above, the sender using the Intranet e-Government service can ensure the confidentiality of data, and the receiver of the information can verify that Sender's signature and ensure the integrity of data[1].

The same process will repeat again when the Receiver sends back the data/document(eg. Mark Certificate) to the Sender.

5. Advantages of the Proposed Solution

In order to ensure the authenticity of the identity of the subject, document integrity, confidentiality and non-repudiation, this paper combines the hybrid encryption technology with short-lived certificate for security, integrity and authentication of user for intranet e-Government applications. The advantages of the Proposed System over non-PKI e-Government application are as follows.

Data Integrity

Data integrity is the assurance of nonalteration: The data either in transit or in storage has not been undetectably altered. Clearly, such assurance is essential in any kind of business or electronic commerce or electronic government environment. A digital signature provides both data origin authentication (evidence about who originated the data) and data integrity (evidence that the data has not been altered in any way)[7]. To ensure the data integrity of electronic documents, our solution uses the digital signature to achieve the integrity of data.

Confidentiality

Confidentiality is the assurance of data privacy: No one may read the data except for the specific entity (or entities) intended. Confidentiality is a requirement when data is transmitted over unprotected networks [7]. To achieve the confidentiality of information, we use encryption technology so that even if the information is intercepted; it cannot be restored to the original.

Integrity of data

Digital digest technology is to ensure the integrity of information. Our solution uses hash functions and digital signature to guarantee the integrity of data being sent.

Identity and Authenticity

By using the digital certificate for secure login in to the system and by using the digital signature technology, we can ensure identity authentication, non-repudiation and non-counterfeit.

Both Sender and Receiver use digital certificate to prove their identity and identifying each other's identity. It follows the standard of

X.509 V3. The validation process of digital certificate will be done as shown in Figure 5.

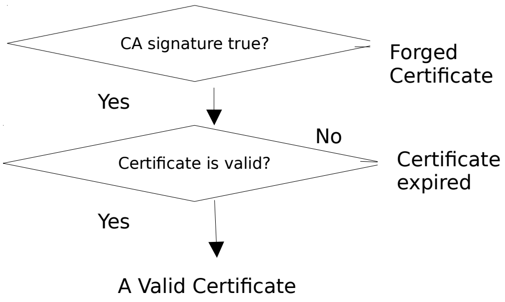

Figure 5. Digital certificate validation process

In this way, we can achieve information confidentiality, identity authentication, information integrity, non-repudiation and non-counterfeit in the process of transmission.

Less effort required in Certificate Life Cycle Management

Since the proposed solution uses the short-lived certificate and as a certificate validity period becomes a few months, we can eliminate some Certification Authority's(CA) life-cycle management functions such as certificate renewing process and Certificate Revocation List (CRL) issuing process. Publication of CRL in CA's directory and the certificate validating services (using Online Certificate Status Propocol (OCSP) or Light weight Directory Access Protocol(LDAP)) are not required to implement at the CA side. At the Application developer side, the certificate validation process is not required as well.

6. Conclusion

Myanmar is now on his way to implement e-Government to provide better service to citizens, business and also government. There are challenges and obstacles to view e-government in four perspectives: technical, political, cultural and legal aspects [4]. IT infrastructure constructions, promotion of security mechanism, integrity and secure payment mechanism have to be solved for e-government implementation [1].

The security issues of electronic documents become an important issue. Under the e-government environment, transfer of electronic data and documents is facing new vulnerabilities, and new attack techniques[1]. In this paper, we propose a solution of a PKI based application system using the short-lived certificate and hybrid encryption technology. This paper presents how an e-Government application can use symmetric and asymmetric key technology together to implement its web security, data integrity and authentication process. Using and managing of a PKI system with CRL facility is complex or complicated for small organizations[1]. This paper proposes an alternative solution for e-Government application using the short-lived certificate and automated client certification service as a means of client authentication and data security.

This paper under the guidance of the status of the electronic documents transmission and security requirements comprehensive use a variety of sophisticated security technologies, that is, symmetric encryption and asymmetric encryption, digital digest technology, digital certification and digital signatures, through these integration technologies to provide more reliable security in electronic documents transmission.

As for future work, we will implement an e-Government application according to the proposed design and analyze the impacts of using the short-live certificate as a solution. The integration of hybrid-encryption solution and authentication solution using short-live certificate can be extended to the non-Web based applications.

References

[1] Xinli Hu, Lianjie Ma, “A Study on the hybrid encryption technology in the security transmission of electronic documents”, *2010 International Conference of Information Science and Management Engineering*, IEEE Computer Society, 2010, pp. 60-63

[2] Yung-Kao Hsu, “Development of an Intranet Security Infrastructure and Its Application”, Publisher, Location, Date.

[3] Hector D. Puyosa P., “e-Government: Security Threats”, IEEE Computer Society, web page posted Nov 11, 2012, 9:46 AM by STC eGov,

[4] Min-Shiang HWANG, Chun-Ta Li, Jau-Ji SHEN, and Yen-Ping CHU, “Challenges in e-government and Security of Information”, An *International Journal*, Information & Security, Vol. 15, No. 1, 2004, pp. 9-20

[5] Elgamal, T., Treuhaft, J., and Chen, F., “Securing Communications on the Intranet and over the Internet”, http://home.netscape.com, Netscape Communications Corp., July 1996.

[6] Xiaoqi Zhang, Meina Song, Junde Song , “A Solution of Electronic Authentication Services Based on PKI for Enabling e-Business”, IEEE International Conference on e-Business Engineering, 2009, pp 431-436.

[7] Carlisle Adams and Steve Lloyd, “Understanding PKI : Concepts, Standards, and Deployment considerations”, second edition, Addison-Wesley, 2003