Certificate Management System, Related Technologies, and its Requirements

Kim, Chan-young * · Oh, Sang-jo **

〈Table of Contents〉

I. Electronic Commerce

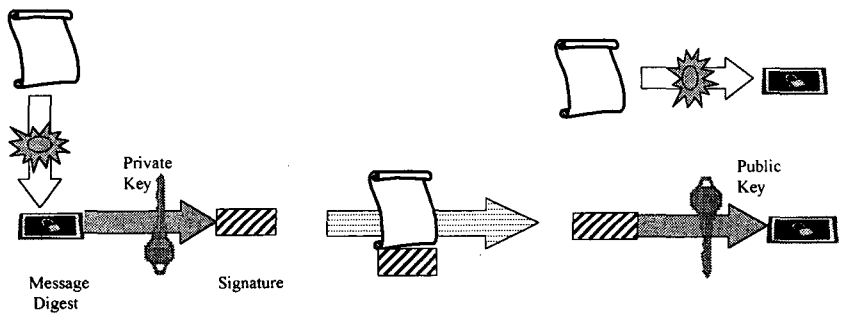
The advance of Web technology and wide spread of PCs connected to the internet created a great deal of potential to the Internet. Many corporations use the internet as a way to enhance their competitive advantage—as a sales promotion tool of their products and services, for example. Frost & Sullivan summarized the growth of internet commerce by stating that the total electronic commerce revenue increased from $6.7 million in 1994 to $103.0 million in 1996. CommerceNet/Nielsens internet demographic study (Spring '97) on 220 million people over the age of 16 in US & Canada indicates that 23% are using the Internet, 17% are on the WWW, 73% of WWW users search for information about products and services and 15% of them or 5.6 million people have purchased online. Also the Killen & Associates study predicts that within 6 years,

*동양공업전문대학 전산경영기술공학부 경영정보시스템 전공 조교수
**동양공업전문대학 전산경영기술공학부 경영정보시스템 전공 전임강사

shoppers will shop $600 billion worth of products or services, which is about 8% of worldwide purchases via Internet. The study also mentioned that the number of internet transactions will reach $17 billion in 2005 which will include about 50% of credit card transactions. This tremendous growth we have experienced or we are expecting offers a great opportunity to many involved parties.

Ⅱ. Business Transaction and Security

Most of electronic commerce transaction involves the transfer of financial value from one party to another. The transfer is initiated and executed based on the request from one party to move monetary value from his or her financial account to others. The requested entity needs to process the transaction in a secure manner by ensuring many security requirements to avoid every possible fraud. Three types of frauds frequent in electronic commerce transactions. They are 1) Merchant Fraud, where the merchant initiates transactions that purchaser did not authorize, 2) Third Party Fraud, where the transfer was requested by a unauthorized, and 3) Purchaser Fraud, where purchaser re-



Alice passes her document through a hashing algorithm to produce the message digest, then encrypts the digest with her private key.

Alice sends the signed message to Bob.

Bob uses the same hashing algorithm to create a message digest, decrypts Alice's signature using Alice's public key, and then compares the two.

Figure 1

pudiates the authorization. The chances of these three types of frauds can be minimized by using digital signature technology which ensures the identity of the requester, and the integrity of the message requesting the transfer. Some of various components of cryptography technologies involved in this process are Symmetric(or Secret) Key Cryptography(SKC) such as DES, Public Key Cryptography(PKC), and hashing algorithm. The Figure 1 shows how Digital Signature works.

When Alice wants to send a document to Bob, Alice first selects a hashing algorithm and uses it to create a message digest(also called as a footprint of the document because it is almost impossible for two different documents to result in identical message digests). This message digest is then encrypted using Alices private key. The document and the encrypted message digest are then encrypted using the receivers(Bobs) public key and sent to Bob. The transmitted message is readable only by using Bobs private key. So, the privacy can be ensured. On Bobs side, the received message is decrypted using Bobs private key. After decryption, Bob gets the content of the document and the footprint of the message encrypted by Alices private key-this is called a digital signature. Bob applies the same hashing algorithm on the document and creates a new message digest for a comparison purpose and compares the footprint of the received message(decrypted one from the transmitted message) with the newly generated message digest. The comparison provides a way to check whether integrity of the document was maintained during transmission.

So far, we reviewed how privacy and integrity are ensured using the digital signature technology. This assumes, of course, that the private key is only available to its owner. This process of digital signature can be illustrated as below.

Alice's Side	$C = B_{Bob}(P, V_{Alice}(H(P)))$	B : Public Key
		V : Private Key
Bob's Side	$P, V_{Alice}(H(P)) = V_{Bob}(C)$	P : Plain Text
	$H(P) = B_{Alice}(V_{Alice}(H(P)))$	H : Hashing

Ⅲ. Trusted Third Party and Its Hierarchy

Privacy and integrity requirement for secure transaction appear to be met by using digital signature. But, how can Alice be sure the public key she believes Bobs really belongs to Bob? And how can Bob be sure that the message really came from Alice? Alices transmission of the message actually claims two different things-one is that the sender is a legal person, Alice and the other is that her public key is what Bob has. But the binding between a legal person, Alice and the public key is not verified yet. What happens if Carol claims to be Alice and use her own public and private key for transmission? Is there any base for Bob to be sure that the transmission is truly from Alice that he understands who she is? Here, the need for the trusted third party (TTP) called certificate authority(CA) comes in. The certificate authority is a trusted third party who guarantees the binding of a persons identity to a public key by issuing a certificate(Figure 2) which is used an identification card like a driver license in the cyber-world.

Figure 2

As described, a certificate is to ensure the user of the certificate that a key included in the certificate belongs to the certified party. However, this assumes that the user is familiar to and trusts CA, the issuer of certificates. If the CA is not well known to the user of the certificate, he or she may require the CA to be certified by an another more trustworthy legal body. When this certification levels are escalated, relationship between higher and lower level of certificate authorities turns into the tree structure. This structure is called certificate authority hierarchy. The highest level CA is called a root CA and the leaf nodes of the tree represent certified clients.

Ⅳ. Type and Class of Certificate

Type of certificates are categorized into four groups based on its purpose and subject of its certification. The first type is identifying certificate which connects(binds, in a technical term) a name to a public key. This type of certificate just certifies that the public key included in the certificate belongs to the name of the person or the other type of legal body(i.e. certified). The second type is authorizing certificate. This type of certificate attests a certain fact regarding the subject whose name is included in the certificate. For example, the certificate may state where the subject resides, the subjects age, the subject is a member in good standing of an organization, the subject is a registered user of a product, the subject possesses a license such as bar membership, or others. This type of certificate is usually a superset of the first type. The third type of certificate is transactional certificate. This type of certificate certifies that some fact or formality was witnessed by the observer, who is usually a certificate authority. The certificate states the description of the transaction and the CA certifies the transaction actually has occurred. The last type is a Digital Time-Stamping. This type of certificate includes the contents of the documents in question or just the foot print(i.e. message digest) of the document along with the chronological time of certification. In other words, the certificate certifies that the document was in existence at a particular time. This kind of certification is called a digital time-stamping service.

As described in the above, four different groups of .certificate are serving different purposes. The certificates serving for same purposes can vary in terms of level of certification-called class of certificate. For example, different levels of certification service can be offered for identifying certificates. One may just identify the binding of public key with common name. Or the other may certify the age, sex, and other attributes of the certified. The VeriSign, Inc. , for example, currently provides three different levels of certification services. (www.verisign.com/repository/cps) Different level of certification requires not only different kinds of information, but also different information validation procedure at the time of certificate issuance.

V. Certificate Management Processes

Certification processes can be described by going through whole life-cycles(Figure 3) of certificates-enrollment(i.e. application for certificate), use of certificates, certificate

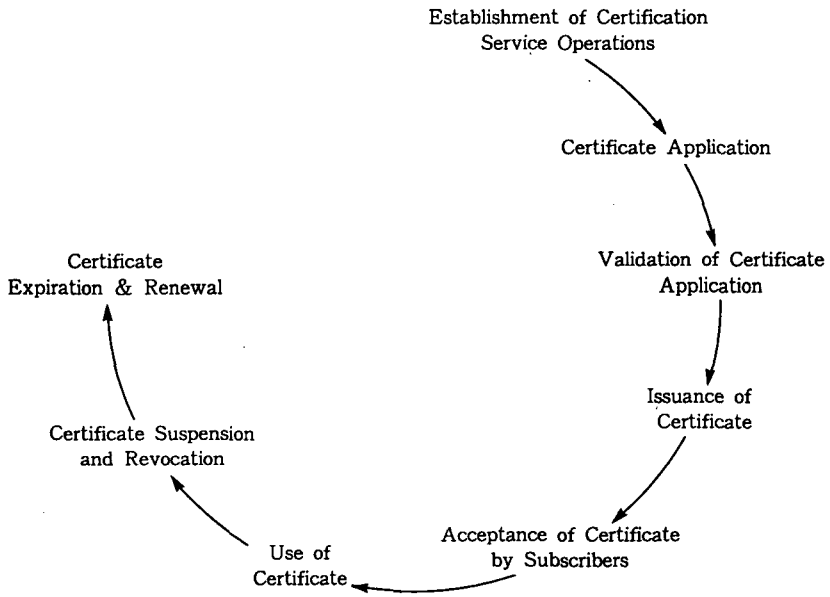


Figure 3

suspension, revocation, and expiration. The life cycle of certificates presents the events that each certificate go through chronologically from its birth to expiration. Description of each phase of life cycle follows.

Certificate Application

All persons or organizations desiring a certificate have to complete the following procedures for each certificate application: generate a key pair, protect the private key(of this key pair) from compromise, determine a proposed distinguished name, and submit a certificate application including the public key of this key pair to the certificate authority.

Validation of Certificate.

Upon receipt of a certificate application the issuer of certificate shall perform all required validations as a prerequisite to certificate issuance. The validation steps include confirming that : (a) the certificate applicant is the person identified in the request, (b) the certificate applicant rightfully holds the private key corresponding to the public key to be listed in the certificate, and (c) the information to be listed in the certificate is accurate. This validation procedures differ by certification classes.

Issuance of certificates.

Upon approving a certificate application CA issues a certificate. Although the issuance of certificate completes the process, sometimes provisional certificate is issued pending verification of the subscriber's further information. A provisional certificate becomes a "normal" certificate at the end of the provisional period provided there has been no revocation.

Acceptance of Certificates.

The subscribers assume the following representations by accepting certificates issued by certificate authorities : 1) each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational(not expired, suspended or revoked) at the time the digital signature is created, 2) no unauthorized person has

ever had access to the subscriber's private key, 3) all representations made by the subscriber to the CA regarding the information contained in the certificate are true, 4) all information contained in the certificate is true, and 5) the certificate is being used exclusively for authorized and legal purposes. The issuer of certificates(CA) may also limit its liability by requesting subscribers to sign the indemnification statement at the time of certificate issuance. Upon acceptance of certificates, a copy of certificate is published so that the information becomes available for use by public.

Use of Certificate

Verification of a digital signature, is undertaken to determine that 1) the digital signature was created by the private key corresponding to the public key listed in the signer's certificate and that 2) the associated message has not been altered since the digital signature was created. The verification process are performed in following sequence : 1) establishing a certificate chain(i.e. finding a trustworthy CA in the hierarchy for the certificate), 2) checking CRL(Certificate Revocation List) for revocation or suspension of certificates, 3) check whether the document was signed while the certificate is valid.

Suspension and Revocation of Certificate.

A certificate needs to be suspended or revoked immediately to limit the possibility of the certificate being used unlawfully in cases where 1) there has been a loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject, 2) the certificate's subject has breached an obligation, or 3) the performance of a person's obligations is delayed or prevented by an act of God, natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised. When certificates are suspended or revoked, the CRL should be immediately updated to include them.

Certificate Expiration

When a certificate is issued, the certificates expiration date and time is specified in

the certificate. This is the time when the operational period ends, without regard to any earlier suspension or revocation. Subscriber is required to submit application for renewal or a re-enrollment in order to continue to use certification service.

Ⅵ. Erroneous Certificates and CA's Business Risk

In electronic commerce, the purpose of certificate is to raise trust level between involved parties in the transaction. Low trust level frequently becomes as a major stumbling block to the initiation of business transactions. On the other hand, high trust level becomes the ground for business transaction. When the trust represented through certificates deviates, the CA must be held responsible however. Therefore the business risk that CA's take by issuing certificates is determined by how well the certificate reflects the real trust level the subject of certificate deserves. Erroneous certificates are the cases that CA is certifying subscribers for the facts that they do not represent. To minimize the likelihood of inaccurate representation thereby to minimize CA's business risk, various cryptography technologies are adopted and tight controls are enforced in internal certification processes.

No matter how hard the CA tries to be precise, its inevitable for CAs to produce some of errors in its certification process. When involved parties become victims of financial losses due to erroneous certificates, someone has to be held responsible for undesirable results. There can be many different scenarios for erroneous certificates and answers on to whom the responsibility belongs differ by scenarios. Some of them are listed below.

1. The certificate is accurate, but the transaction goes wrong for some other reason. : A CA should not be liable for the ways in which accurate certificates may be used by others.
2. The security of Alice's key is compromised and Mallet uses it, along with Alice's

publicly available certificate, to impersonate Alice. : Unless Alice and CA have made a special arrangement, a CA should have no duty to monitor the use of a certificate that they have agreed will be publicly available. Once notified of a key compromise, a CA should have a duty to publish this in the CRL quickly.

3. Alice revokes her key because she learns of Mallet's actions, but Mallet manages to transact during the period between Alice's revocation notice to Carol and Carol's posting of a certificate revocation. : Presumably the critical issue in this scenario will be whether Carol acted quickly enough. If Carol has acted reasonably quick enough, she is not responsible for the loss.
4. The security of Carol's key is compromised and Mallet begins issuing bogus certificates or bogus certificate revocations. : Liability here may in part depend on how the key was compromised. If the compromise could have been blocked by CA(and this is an expected behavior of a good CA), then the CA is responsible.
5. Carol erroneously lists Alice's key as revoked, and Bob refuses to transact with Alice. : CA is clearly responsible in this case, erroneously reporting that a credit limit has been exceeded or the card stolen.
6. The meltdown scenario : there is a major discovery in number theory or computation and the algorithms on which Alice and Carol's keys are based are no longer secure. : Nobody really could have anticipated the a major discovery. But CA is expected to react to the change of situation as fast as it can.

Ⅶ. Requirements of Certificate Management System

The business risk that certificate authorities assume is affected by 1) monetary value involved in transaction backed by certificate, and 2) frequency of erroneous certificate in use-erroneously issued, unlawful and false certificate. In order to manage this business risk at the level that CA hopes to maintain, proper preventive actions on every potential causes for wrong certification should be taken. Since the system controls most of processes related to certification, the requirements of CMS(Certificate Management

〈Table 1〉

Business Risk Factor	Causes	Prevention Methods
Monetary value involved in transaction backed by certificate	Use Certificates for financial business transaction.	• Certificate Authority can have subscribers to sign the indemnification statement when they accept the issued certificate.
Erroneous certificate issuance	Erroneous Validation and Issuance of Certificate.	• Maintain consistency in application validation-CA should publicly state its validation requirements and policies. • Maintain accuracy in certification processes.-Should implement good audit procedure. • No single person should be allowed to own 100% of controls on certificate issuance.
Unlawful certificate	Compromise of Subscribers Private Key.	• Immediate update to CRL and certificate re-issuance. • Should support regular private key change. Each certificate should carry expiration date.
Unlawful certificate	Compromise of CAs Private Key.	• Should support very long keys, preferably 1,000 bits or longer. • Should support regular private key change. • Should support automatic recall and re-issuance of large volume of certificates. • CAs private key should be kept in a high-security box, tamper resistant off-line device, known as a CSU (certificate signing unit).
False Certificate	Improper System Operation	• Maintenance and publication of CRL • Proper Back-up and Recovery. • Should support a challenge phrase at the time of revocation request. • Contingency and Disaster Plan • Round-the-clock customer service.

System) need to be formulated and looked into closely for development and implementation of a successful system.

Types of business risk factor, causes, and prevention methods are listed below.

Ⅷ. Conclusion.

Security has been the major stumbling block to wider spread of electronic commerce. Various technologies-such as cryptography, certificate, Trusted Operating System (TOS), Virtual Vault, Firewall and others-are available in the market to increase the level of security of business transaction. All these technologies make contribution in increasing involved parties confidence in privacy, integrity, authentication and non-repudiation. Certificate technology provides good solutions to authentication and non-repudiation part of puzzles. The solution is implemented in the form of Certificate Management System and supports all phases of operation related to certificates from issuance to expiration.

Business risk that CA takes is inversely proportional to accuracy of certification management processes. All certification management processes are performed through automated computer system, CMS. In other words, CA's business risk can be managed and controlled only through proper operation of CMS. Therefore, prior to design and development of a successful CMS, identification of proper system requirements is necessary. This paper offers requirements of the system in terms of a way to minimize CA's business risk. The requirements of CMS discussed in this paper provides the minimum preventive measures against erroneous certificates.

References

1. Quick Summary of Important CPS Rights and Obligations http://www.verisign.com/repository/summary.html
http://www.verisign.com/repository/CPS/
2. Taher Elgamal, Jeff Treuhaft, Frank Chen, July 1996 Securing Communications on the Intranet and Over the Internet http://home.netscape.com/newsref/ref/128bit.html
3. Microsoft Corporation, Microsoft Certificate Server, April 17, 1997 http://www.microsoft.com/intdev/security/certsrv/certsvr.htm
4. Digital IDs-Frequently Asked Questions-〈http://www.verisign.com/if-faqs.htm#multiple-use〉
5. Ravi Kalakota, Andrew Whinston Electronic Payment System, Ch 6, Electronic Commerce-A Managers Guide
6. A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, Ch 6 Readings in Electronic Commerce, Addison Wesley

초 록

인터넷은 최근 수년간 괄목할 속도로 보급이 되고 있으며, 그 높은 성장속도는 당분간 지속될 것으로 전망된다. 인터넷이 전자상거래의 가장 우세한 기반으로 등장하면서, 전자상거래의 보안의 중요성이 강화되어 다양한 보안기술이 채택되어지고 있다. 본 논문은 인증기술의 개요를 논하고 인증기관이 인증관리시스템을 이용하여 어떻게 사업상의 위험을 최소화할 수 있는가의 방법을 제시한다.

Abstract

We have experienced tremendous growth in commercial use of Internet especially in the last couple of years, and the rate of growth does not appear to be slowing down. As the Internet becomes a dominant platform for electronic commerce, all involved parties of electronic commerce are concerned about security of transactions. Various technologies are adopted to enhance the security of business transactions. This paper briefly discusses certificate technology and a way to minimize the business risk of certificate authority in a form of system requirements of CMS(Certificate Management System).