OCC 99-20

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Certification Authority Systems Description: Guidance for Bankers and Examiners

TO: Chief Executive Officers and Chief Information Officers of All National Banks, General Managers of Federal Branches and Agencies, Department and Division Heads, and All Examining Personnel

PURPOSE

This bulletin defines the elements of certification authority systems, describes the roles of banks in emerging systems, and identifies the risks of such systems using the OCC supervision-by-risk framework. By outlining such risks, this bulletin should enable bankers to make informed decisions about whether and how to become involved in such systems.

Although technology firms provide many products and services for electronic authentication, banking organizations may provide important services as well. A certification authority functions in effect as an on-line notary, a trusted third party that confirms the identities of parties sending and receiving electronic payments or other communications. Because banks already have a traditional role as a trusted third party in financial and commercial transactions, they are in this respect a natural fit for the certification authority business. Banks that wish to participate in certification authority systems should consult with OCC legal or licensing staff to determine whether a legal interpretation or corporate filing is necessary. OCC staff are prepared to discuss specific risk management techniques or controls that are beyond the scope of this bulletin.

CONTENTS *Page*

SCOPE AND REFERENCE

The scope of this bulletin includes bank activities related to operating a certification authority (CA) system. Although currently few banks participate actively in a certification authority system, the OCC is aware that many banks are considering operating or investing in a CA system. Bankers and examiners need to become familiar with the elements and risks of CA systems. This bulletin is intended to provide a basis for discussion between national bank examiners and management of banks with respect to the risks of operating a CA system.

Attached to the bulletin are two appendices to assist examiners with issues that may arise in discussions with bank management about CA systems. Appendix A, "Digital Signatures with Public Key Cryptography," is a brief description of the underlying encryption technology used in CA systems. Appendix B, "Ancillary Services," is an overview of additional services banks may perform that could be associated with a basic CA system.

A CA system involves the use of mainframe and personal computers, communications networks, and supporting software systems to provide electronic authentication services. The basic operational elements of a certification authority system are similar to a PC banking system, with many possible configurations of computer software, hardware, and telecommunications links with its users. Therefore, bankers and examiners should refer to OCC Bulletin 98-38, August 24, 1998, "Technology Risk Management: PC Banking -- Guidance for Bankers and Examiners," to assess the risks associated with CA systems. Further, examiners should read this guidance in conjunction with OCC Bulletin 98-3, February 4, 1998, "Technology Risk Management: Guidance for Bankers and Examiners," which describes a technology risk management process involving three essential elements: (1) planning, (2) implementation, and (3) measurement and monitoring of risk. Because most CA systems are in the pilot stages or operating on a limited scale, this bulletin places particular emphasis on the risks associated with planning and early implementation of such systems. OCC will address the risks related to measuring and monitoring fully implemented systems when warranted by industry developments.

BACKGROUND

A variety of CA systems are in the pilot or early implementation stages. Banks are operating CA systems for internal use only, or to secure communications between bank departments, offices, or employees. Other banks, working with bank card associations, are conducting pilots of CA systems using the secure electronic transaction protocol (SET) that provides greater security for credit card payments on the Internet. Although there are small-scale operations today, the exact form that CA systems will take in the future is uncertain. Therefore, this bulletin describes only the risks associated with the basic elements of a CA system, and does not suggest specific risk management techniques.

Although the OCC has recognized CA activities as a functional equivalent of recognized banking activities, the legal infrastructure for CA activities is evolving.[Note: Conditional Approval No. 26, dated January 12, 1998, granted approval to a national bank to establish an operating subsidiary to act as a certification authority to enable subscribers to generate digital signatures that verify the identity of a sender of an electronic message.] For example, some states have passed laws recognizing digital signatures. Although no federal law to date recognizes digital signatures as the equivalent of handwritten signatures for binding parties contractually in a commercial transaction, [Note:There is no national consensus on whether existing state and federal laws concerning handwritten signatures can be interpreted to cover digital signatures. Some states have adopted statutes that specifically license and regulate the activities of a CA.] on October 21, 1998, Congress enacted the "Government Paperwork Elimination Act" that includes provisions concerning electronic authentication. [Note:The Government Paperwork Elimination Act is part of P.L. 105-277, included in H.R. 4328, the Omnibus Consolidated and Emergency Supplemental Appropriations Act for FY 1999.] While this law applies only to the federal government and its agencies, its enactment means that the federal government will be participating actively in developing standard practices for this technology. Standardization efforts abroad may have an impact on domestic banks with international operations. In April 1997, the European Commission issued a communication entitled "Towards a European Framework for Digital Signatures and Encryption," COM (97) 503. This communication declared the urgent need for common legal requirements for CA systems to promote interoperability of systems across member states of the European Union. It has fostered subsequent activity on the part of the European Commission and its member states.

DEFINITIONS

A **certification authority (CA)** is similar to a notary. The CA, in confirming the identities of parties sending and receiving electronic payments or other communications, engages in **electronic authentication**. Authentication is a necessary element of many formal communications between parties, including payment transactions. In most check-cashing transactions, a driver's license with a picture is sufficient authentication. A personal identification number (PIN) provides electronic authentication for transactions at a bank automated teller machine (ATM).

A **digital signature** is a unique code, created by a software application, that confers a certain security on a communication. In a CA system, a recipient of a message with a digital signature can verify the identity of the sender. Most CA systems enable the recipient to be confident that the message was not modified or tampered with in any way after the message was signed.

The CA issues a **digital certificate** for each identity, confirming that the identity has the appropriate credentials. A digital certificate typically includes information about the identity of the signing party, the operational period for the certificate, and the CA's own digital signature. In addition, the certificate may contain other information about the signing party or information about the recommended uses for the signature. A **subscriber** is an individual or business entity that has contracted with a CA to receive a digital certificate verifying an identity for digitally signing electronic messages.

A **repository** is a database of active digital certificates for a CA system. The main business of the repository is to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages. These message recipients are called **relying parties.**

The **Certification Practice Statement (CPS)** is a method the industry uses to inform subscribers and other parties of the division of rights and responsibilities among participants in a CA system.

Participants in a CA system may include the CA that issues digital certificates, the repository, subscribers, and relying parties. Although there are no standard practices for the specific information necessary in the CPS, a CA likely would include a discussion of the security and privacy precautions used in issuing and maintaining the certificates and related information for its subscribers.[Note: Although similar to a contract, the legal enforceability of a CPS is not yet settled. However, a CA that includes the CPS explicitly in a subscriber contract would increase the legal enforceability of the CPS with respect to the subscriber.]

CA systems may be characterized as primarily **open** or **closed**. A fully closed system has contracts defining the rights and obligations of all participants for authenticating messages or transactions. This type of system offers the CA operators less risk exposure because there is little uncertainty regarding obligations. Conversely, a fully open system would not have formal contracts defining the rights and obligations of relying parties in the system. In such a system, the firms that perform the CA activities could be exposed to an uncertain level of risk for each authenticated message or transaction. It is likely during early stages of development that most CA systems will be neither fully open nor fully closed, with contracts defining the rights and responsibilities of at least some, but not all, of the system participants.

RISKS OF CERTIFICATION AUTHORITY SYSTEMS

A CA system must deliver, arrange for delivery, or verify subscribers' acquisition of the cryptographic elements necessary to create digital signatures and create digital certificates for subscribers. As with other bank products and services based on emerging information technologies, a CA system exposes the bank to transaction, strategic, and reputation risks. The system also must have the capability to maintain a large database of active certificates and rapidly process large volumes of requests from relying parties concerning its database of digital certificates. In addition, the system must be designed to be available continuously.

A bank may choose to perform all the functions necessary for a CA system to operate, contract for some of these functions, or perform some of these functions for another business firm acting as a CA. The need for trust in a CA system offers an opportunity for banks to expand their relationships with businesses and consumers, using their experience as facilitators for payments and related transactions. A bank might choose to employ a CA system for its own internal use in order to certify employees for remote access to bank information systems. Alternatively, the bank might decide to provide CA services to certify its customers for access to bank services. Lastly, the bank might elect to participate in a CA system that is designed to certify the general public for using digital signatures with their messages and transactions.

This bulletin discusses CA system risks in two broad areas -- risks encountered when issuing certificates and those encountered when managing certificates.

Issuing Digital Certificates

To issue digital certificates, a CA must:

- Verify subscribers' identities for digital certificates;
- Determine the appropriate content of digital certificates;
- Create, distribute, and ensure acceptance of digital certificates; and
- Ensure internal security.

Verifying Identity

Verifying the identity of subscribers exposes a CA to transaction, strategic, and reputation risk. Transaction and reputation risk exposures result from the possibility of falsely identifying potential subscribers. The policies and procedures the CA establishes to perform this function are a source of strategic risk. To confirm the identity of a subscriber, the CA either reviews the subscriber's credentials internally or contracts with a registration authority (RA). The decision to outsource and the choice of RA exposes the CA to strategic risk. If the CA or RA confirms an identity that is false, or somehow inaccurate, the CA may suffer loss of business or even expose itself to legal actions. Moreover, the CA's outstanding certificates may become suspect if there is a pattern of insufficient due diligence in verifying identities for issuing certificates. The risk exposure from falsely identifying a subscriber may be reduced when a CA issues digital certificates for use within a closed system, because there are contracts in place between some or all of the participants in the system.

Certificate Content

Certificates' content varies by CA system. Content and a certificate's limitations are a source of strategic risk to the issuing CA. Standard certificates identify the subscriber and the issuing CA. Another important element of a standard certificate is the expiration date. [Note: The X.509 standards for certificate content, developed by American National Standards Institute (ANSI), require that digital certificates contain the distinguished name of the certificate issuer (the signer), an issuer-specific serial number, the issuer's signature algorithm identifier, and a validity period.] The more limited the life of a certificate, the lower the transaction and reputation risk exposure for the issuing CA. A certificate's security has both physical and logical vulnerabilities that are outgrowths of the software used to generate a digital signature. The longer such software is in use, the greater the likelihood that it will be corrupted or that someone will gain unauthorized access.

Certificate extensions provide information in addition to the identity of the subscriber and the ssuing CA. Additional information may include suggested limitations on uses of the certificate, such as the number of and type of transactions or messages that subscribers are authorized to sign. Any such limitation reduces the transaction and reputation risk of the issuing CA. The CA also may use extensions to establish classes of digital certificates for use with financial transactions or for transmitting highly sensitive information. Such certificates may be for a single message or transaction, used only with a specific relying party, or limited to a maximum financial amount.

Certificate Creation, Distribution, and Acceptance

The process of creating, distributing, and documenting acceptance of a subscriber's certificate exposes a CA to transaction, strategic, and reputation risk. In certificate creation, the transaction and reputation risk exposures arise from possible errors occurring in the systems that match appropriate certificate limitations to each subscriber's unique signing capabilities. Strategic risk exposures are associated with the policies and procedures that control the process.

Certificate distribution and acceptance often is not solely the responsibility of the CA. The subscriber likely will obtain the technology to create digital signatures from a software provider or other technology firm. However, the certificate is not complete until the CA acknowledges the subscriber's signing capability with its own digital signature to create the certificate of record. In a closed CA system, the CA risk exposure may be modified by the contract establishing the exact roles and responsibilities of the parties. Some of the transaction risk may be allocated to a lead organization, individual subscribers and relying parties, or another entity maintaining the database of certificates. However, the CA still may have a reputation risk exposure if problems with the technology are attributed to the CA.

Generally, a digital certificate will not be operational until the subscriber accepts the signed certificate. Certificate acceptance implies that the subscriber agrees to the terms and conditions established by the CA for the overall system as well as any specific conditions that apply to the subscriber. Errors in the communication process with subscribers regarding acceptance, from either inadequate policies and procedures or technical difficulties, expose the CA to both transaction and reputation risk.

Internal Security Concerns

Internal security breaches are a major source of transaction and reputation risk exposure. In addition to the standard risks associated with a system architecture designed for outside access, one of the primary security concerns of a CA system is protection of the elements that make up the system's own signing capability. [Note: A CA security system using public key cryptography would include protection of its own private key or keys and a key management system. See Appendix A for a more complete explanation of keys.] The transaction and reputation risk exposures of an issuing bank resulting from failure to protect its signature properly could be substantial because fraudulent certificates could be distributed in the CA's name. Thus, it would be possible for non-subscribing individuals to sign electronic messages or sign off electronically on payments for activities that could result in substantial fraud losses and affect legitimate subscribers and relying parties.

A second significant internal security exposure results from problems that could arise with respect to the records containing confidential information the CA system collects in establishing subscriber credentials. A subscriber could experience losses if any party obtains access to confidential information the subscriber never authorized for release. Such losses could expose the CA to legal or regulatory action. Even if a subscriber merely ends its relationship with the CA, the CA may lose business due to damage to its reputation.

In addition to subscriber information collected during the registration process, there are privacy issues with respect to records relating to the number and nature of relying parties' inquiries of specific subscribers. These records are necessary for effective audit of the CA repository system, but the improper disclosure of such information potentially could violate the privacy of a subscriber.

Managing Digital Certificates

When a CA issues certificates to support subscribers' digital signatures, the CA usually is interacting only with subscribers or a representative or agent acting on behalf of the subscribers. However, if the CA also chooses to manage outstanding certificates, i.e., act as a repository, the CA will transact with relying parties that receive messages. The following discussion outlines the risk exposures that arise with respect to repository services for both subscribers and relying parties. It is organized to address four aspects of managing digital certificates:

- Customer disclosures
- Subscriber service and support;
- Suspending and revoking certificates; and
- Processing the requests of relying parties.

Customer Disclosures

Although there is no legal disclosure requirement at present, a CA will need to provide some information concerning the basic services provided and the rights and responsibilities of subscribers and relying parties. The nature of the disclosures will have an impact both on the transaction and reputation risk exposure of a CA. For example, if disclosures clearly describe the CA error resolution procedures and privacy policy, there may be less confusion on the part of subscribers. Further, if the CA provides some technical discussion about the use of the software associated with certificates, subscribers correctly may ascribe problems to the software provider rather than the CA, shifting some of the reputation risk exposure away from the CA.

Subscriber Service and Support

Like many new information technology products and services, CA requires customer support, which is a source of reputation risk. A bank may consider establishing a help desk or some other form of direct interaction with subscribers and relying parties. The policies, procedures and operation of the help desk are a potential source of transaction and strategic risk. Resolving problems or errors subscribers and relying parties encounter from lack of familiarity with the use of the underlying technology will require substantial resources from the CA or a customer service contractor. Although the CA typically will not supply software for creating a digital signature, there may be some circumstances in which subscribers attribute all difficulties in using the technology to the CA.

Subscribers may have technical problems because of software configurations on their personal computer systems that may not become apparent until they attempt to sign a message or transaction. When difficulties arise, subscribers are more likely to seek support directly from software providers with widely recognized brands. The many smaller or less recognized companies may not have subscriber confidence. Because a bank providing CA service ultimately may wish to maintain the customer relationship, the practical decision may be to provide customer service either internally or to contract with a firm with appropriate expertise. [Note: Some technology firms now provide integrated chip cards to hold subscriber certificates. Instead of downloading the software to the PC hard drive, the subscriber would have a smart card reader attached to his PC. The smart card and reader would be pre-programmed to load the certificate information appropriately for the subscriber. Some of the transaction and reputation risk of subscriber service and support may be reduced by the simplicity of the use of hardware rather than requiring PC users to load the software from another source.]

Suspending and Revoking Certificates

Because the subscriber is responsible for maintaining the security of the signature capability, the potential exists that the system may be compromised and made available for unauthorized use. Thus, the CA may be required to suspend or revoke a certificate. If the CA (or another responsible party within the system) does not monitor and take such action in a timely manner, the CA may authenticate messages or transactions carrying expired digital signatures. Thus, CA systems that render a subscriber's digital certificate invalid are potentially exposed to substantial transaction, strategic, and reputation risks. Poorly designed policies and procedures are a source of strategic risk, and improperly implemented ones expose the CA to transaction and reputation risk. The timing of necessary repository updates may differ with the type of certificates involved; a delay in the suspension of a certificate used for sensitive messages or transactions carries relatively high risk.

A digital certificate may be rendered invalid in one of two ways. The CA may *revoke* a certificate if it is certain that a subscriber has compromised his signing capability. [Note:The most likely compromise would be if the subscriber did not keep his private key secure. If a subscriber's private key became known, unauthorized individuals could sign messages and transactions.] If there is some question as to the status of the certificate, the CA instead may *suspend* the certificate until its status is determined. Transaction and reputation risk may result from errors in processing both requests for revocation and suspension of certificates. For example, a subscriber whose certificate is erroneously invalidated and hence is unable to sign messages could potentially experience losses and may pursue legal action, damaging the CA's reputation in process. Conversely, the CA may suffer exposure if a relying party accepts a message or transaction that is signed by a subscriber whose certificate should have been revoked or suspended.

Processing Relying Party Requests

Substantial transaction, strategic, and reputation risk exposure is associated with processing requests by relying parties regarding the status of individual certificates. Although the CA-subscriber contractual relationship may define obligations to subscribers and others, such contracted protection may not exist for transactions with relying parties, particularly in open systems. For example, if the CA represents an expired certificate as operational to a relying party, the CA may be exposed to reputation damage or a lawsuit. [Note:There is an additional risk in an open system that the circumstances of an individual subscriber or class of subscribers have changed during the valid period of a circulating certificate.] Any delays in processing certificate revocation requests as a result of inadequate policies and procedures or technical processing may result in such errors. If the repository processes requests in batch mode as opposed to real time, the risk exposure is greater. As the volume of transactions processed by the repository increases and as more certificates are placed in circulation with varying limitations and expiration dates, risk exposures also may increase.

There are two recognized methods for responding to a request about the validity of an individual certificate. The most well-known method requires the repository to retrieve a lengthy list of invalid certificates, the Certificate Revocation List (CRL), to check the validity of a single certificate. Inaccuracies in the CRL are a source of transaction risk for the CA system. In addition, the scheduled frequency for generating the CRL will affect the risk exposure of the repository. More frequent generation of CRLs will reduce a CA's transaction and reputation risk exposure. [Note: There is also an issue as to whether certificate status is "pushed" out by the CA repository to interested relying parties, or "pulled" from the repository by the relying parties in question. There are different transactions and reputation risk exposures associated with each method. The "pull" method allows the CA repository to transfer any reputation risk exposure successfully to the relying party with respect to accepting an invalid certificate. On the other hand, the "push" method places the responsibility clearly on the CA if the CRL is not accurate or is not distributed on a timely basis.] Because of the risks and cost inefficiencies of the CRL approach, the industry is developing a second method. Several technology firms have developed software that allows a repository to search its records for the validity of a single certificate in real time.

Another source of repository transaction risk relates to the ability of a relying party to understand certificate extensions. To date, there is no widely accepted industry standard on the implementation of certificate extensions. [Note: The American National Standards Institute (ANSI) has formulated standards for secure electronic financial transaction, including X.509 which specifies certificate content. There are some applications, such as the certificates used in secure socket layer (SSL), for which participants comply with ANSI standards. For other applications of digital certificates, such as SET, the X.509 standards are not in use.] Thus, two parties seeking to authenticate a message may be delayed or ultimately unable to do so. To the extent that certificates are used within a closed system, interoperability of certificate extensions is not an issue. However, in open systems, the lack of industry-wide standards or practices, errors in reading extensions, or the inability of relying parties to read important extensions, increase the CA's transaction risk exposure. As the industry adopts common practices and achieves interoperability, certificate extensions that impose or suggest limitations on use of digital signatures would reduce the risk exposure potential of the issuing CA.

RESPONSIBLE OFFICE

Questions regarding this bulletin should be directed to:
Clifford Wilke, Director, Bank Technology, (202) 874-5920, or by e-mail:
clifford.wilke@occ.treas.gov

____
Clifford A. Wilke
Director for Bank Technology

Attachments: Appendix A — Digital Signatures with Public Key Cryptography
Appendix B — Ancillary Services

Appendix A

DIGITAL SIGNATURES WITH PUBLIC KEY CRYPTOGRAPHY

Although public key cryptography is not a new technology, it is relatively new to the financial services industry. In the past, the financial services industry has relied on symmetric cryptography to ensure confidentiality. Symmetric cryptography, often called "shared secret" or "secret key" cryptography, uses the same mathematical function or algorithm to encrypt and decrypt a message. The **key** is actually a number that is used in conjunction with a mathematical function or algorithm to encrypt a message or transaction. Both the sender and receiver of a message must have the algorithm and the key to encrypt and decrypt any encoded message. In general, the security of symmetric encryption methods is based on keeping the key and/or the algorithm secret or using very large numbers for the key in the algorithm to ensure that it is prohibitively expensive for an unauthorized individual to decrypt an encoded message. DES, a well-known symmetric algorithm used by the Federal Reserve and others for wire transfers, relies on the use of large numbers in the encryption algorithm, because the algorithm is publicly available.

Digital certificates associated with the few widely implemented electronic commerce systems employ digital signatures that are created with public key cryptography. Public key cryptography adds a layer of security beyond that of symmetric key systems by associating two keys or algorithms with the encryption/decryption process: a public and a private key. Public key cryptography also is known as asymmetric key cryptography. Although the public/private key pair is related functionally, the mathematical function associated with the public key is not identical to the function associated with the private key. The combination of the more complex mathematics and large numbers used for public key cryptographic system means a more secure system that would require great expense of time and computing power to "break."

Each user in a public key cryptographic system has a unique public/private key pair. The private key is an algorithm known only to its owner; the public key is published for general use. If public key cryptography is used for message encryption, the individual sending a message likely would use the public key of the intended message recipient to encrypt. In this way, only the intended reader, the owner of the associated private key, would have the ability to decrypt and thus gain access to the message content. Among the variety of asymmetric cryptographic algorithms, the three most common are DSA, RSA, and elliptic curve (ECC). [Note: DSA and RSA are the most common asymmetric algorithms in use at present. With DSA, signature generation is faster than signature verification. On the other hand, with RSA signature verification is faster than signature generation. The strength of the RSA algorithm used to generate key pairs is based on the difficulty of deriving the factors of a product of two very large numbers. For DSA, the strength is related to the difficulty of computing discrete logarithms for large numbers. An alternative algorithm currently being discussed is elliptic curve. The strength of this algorithm is based on generating key pairs using the algebraic relationship between two points on a curve. Like DSA and RSA, the strength of this algorithm increases as larger numbers are used for the keys. However, the strength of ECC is greater for smaller numbers than for either DSA or RSA.]

In a CA system, the public key cryptography is used primarily for message authentication. Message encryption is a separate software application. Subscribers and relying parties use the public/private key to generate and verify a digital signature. Although the subscriber may not be aware of it, digital signature creation is a two-step process. First, the message a subscriber wishes to sign is encoded with a special purpose algorithm to create a "hash." Next, the hash is encrypted with the sender's private key, producing the digital signature. Typically, this digital signature is attached to its associated message providing a unique identifier, much like a written signature. The relying party is able to authenticate the message by referring to the subscriber's digital certificate. The CA system provides the digital certificate that formally links the identity associated with any given digital signature to the signer's public key.

Digital signature verification by the relying party repeats the process of digital signature creation using the sender's public key, obtained with information from the sender's certificate. The repository for the CA system maintains the list of valid and invalid certificates which provide information about subscribers' public keys. Digital certificates formally associate the identified subscriber with a public/private key pair as well as the authority issuing the certificate. The message recipient must have the appropriate software to compute a new hash function of the original message, which is in clear or encrypted text, as determined by the sender. Using the sender's public key, the message recipient should be able to verify that the digital signature was created with the sender's private key.

Thus, digital signatures created with public key cryptography ensure that the recipient is confident of the identity of the sender. In addition, digitally signed messages assure the message recipient that the contents of the message have not been altered in transmission, because the signature includes the hash of the original message. If there is any change in the message in transmission, it will not be possible to authenticate the message, because the signature verification process will not produce a match with the hash associated with the original signature.

Appendix B

ANCILLARY SERVICES

Depending on the scope of transactions and messages for which subscribers use digital certificates, there are a number of other ancillary services that may be part of a CA system.

Private Key Escrow

Once the subscriber has requested or generated a public/private key pair for a digital certificate, each key requires different treatment. While the public key as certified by the CA will be made available for appropriate use by relying parties, the subscriber's private key necessarily is for his exclusive use. A subscriber will want easy access to additional copies of his private key, in case it is accidentally corrupted or deleted. The CA may provide escrow services as a backup for their subscribers. Such key escrow services create transaction and reputation risk exposures if the CA does not implement sufficient physical and logical security to limit unauthorized internal and external access to stored private keys.

Archival Services

In addition to the repository of valid certificates, subscribers and relying parties may have need for an archive of once-valid, but no longer active, digital certificates used for authenticating past transactions and messages. The risks involved with this function are the same as those for maintaining the integrity of any large data base, including transaction and reputation risk associated with managing access to the database.

Certificate Manufacturer

A CA issuer may outsource some technology operations to a certificate manufacturer. Banks may serve as a manufacturer for other entities that act as CA. Depending on the contract between the issuer and the manufacturer, the manufacturer is likely to generate the issuer's own public/private key pair. In addition the manufacturer may generate, sign, and publish subscriber certificates under direction of the issuer. The risks involved with this function are the strategic, reputation, and transactions risks associated with certificate issuance. The overall risk exposure would be shared between the certificate manufacturer and issuer, according to the terms of their contract.

Message Encryption

Some digital signature software includes an option to encrypt messages that are digitally signed. Although not necessary for message authentication, or for proof of data integrity, message encryption restricts access to messages and transactions to those persons who know the code. While a CA providing such software has the transaction and reputation risk exposures of any company providing a similar software product, its compliance risk exposure can be even more significant. This compliance risk arises from the uncertain legal environment and public policy position with respect to encryption. There are restrictions on encryption export and an ongoing domestic debate about law enforcement access to encrypted information.

Time Stamping

Some documents require a specific time assigned to identification or validation. If the software application allows subscribers to insert a time stamp, the CA is exposed to additional transaction risk from the possibility that an incorrect time or date is assigned to a digitally signed document.