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.