UIC John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 3 *Journal of Computer & Information Law - Spring 1999*

Article 3

Spring 1999

Electronic Document Certification: A Primer on the Technology Behind Digital Signatures, 17 J. Marshall J. Computer & Info. L. 769 (1999)

David L. Gripman

ELECTRONIC DOCUMENT CERTIFICATION: A PRIMER ON THE TECHNOLOGY BEHIND DIGITAL SIGNATURES

by DAVID L. GRIPMAN†

Human Resources Manager to job candidate: "I see you've had no computer training. Although that qualifies you for upper management, it means you're under-qualified for our entry level positions."[1]

I. INTRODUCTION

In his science fiction novel *Neuromancer*, William Gibson introduces his readers to the world of "cyberspace" and the world has never been the same.[2] Gibson's virtual reality world of cyberspace included hackers and thieves who used electronic networks to engage in battle.[3] Gibson's virtual world exists today as hackers use the Internet to disable computer systems and intercept email messages of others.[4]

The explosive growth of the Internet has left a fertile ground for hackers and outlaws to practice their craft as the global economy transforms from a paper-based one to an electronically-based one.[5] According

† J.D., January 1999, L.LM Candidate in Information Technology Law, June 1999, The John Marshall Law School. Mr. Gripman is General Counsel and Director of Internet Operations for Chicago Mortgage Corporation, www.chicagomortgage.com. Prior to law school, Mr. Gripman spent several years as a technology consultant to Fortune 1000 corporations. The author extends his appreciation to Mr. Christopher McGeehan, J.D./L.LM Candidate in Intellectual Property Law, The John Marshall Law School, for his ideas incorporated in the Introduction of this article. In addition, the author extends his appreciation to Ms. Carole L. King from Roosevelt University for her assistance in producing the diagrams to this article because without her help, the diagrams would not have been possible.

1. *Humorspace*, (visited Aug. 2, 1998) <http://www.humorspace.com/humor/quotes/qboss.htm>.

2. William Gibson, NEUROMANCER 4 (1984).

3. *Id.*

4. *See* David L. Gripman, *The Doors Are Locked but the Thieves and Vandals Are Still Getting in: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167 (1997).

5. The impact of the Internet upon society has been nothing less than stunning. To communicate internationally via traditional means, it would take weeks by mail or be quite costly using the telephone. Now using the Internet, one can communicate with anyone

to Forrester Research of Cambridge, Massachusetts, electronic commerce is projected to grow to $327 billion in 2002, up from $8 billion in 1997.[6] While electronic commerce still accounts for a small percentage of overall business transactions, this percentage should continue to grow dramatically if sufficient confidence exists in a system that is safe and reliable.[7] Recent technological developments from the private sector have made the Internet a more secure and attractive vehicle for commerce.[8]

Despite such developments, a primary problem with electronic commerce is that parties cannot physically verify with whom they are dealing. Thus, it is necessary for a trusted impartial third party called a "[c]ertification [a]uthority" ("CA") to perform this function of identification.[9]

A CA can prevent disputes as to what actually occurred between two parties as well as prevent fraud and forgery.[10] While the functions of a

---

around the world via email in a matter of minutes. Using Internet "chat rooms," one can communicate live with anyone around the world at basically no charge. In addition, the value Wall Street places on Internet-based companies is astonishing. For example, compare corporate giant Federal Express to 3-year-old Internet company Yahoo!.

Federal Express	*Yahoo!*
Revenues = $16 billion	Revenues = $200 million
Profits = $580 million	Profits = $25 million
Employees = 88,000	Employees = 800
Market value = $14 billion	Market value = $34 billion

Compare Microsoft Investor, (visited March 29, 1999) <http://investor.msn.com/research/profile.asp?Symbol=fdx>, *with Microsoft Investor*, (visited March 29, 1999) <http://investor.msn.com/research/profile.asp?Symbol=yhoo>. The disparity between the sizes of the companies and their respective market values is staggering, and in some ways incomprehensible. However, the income and market values demonstrate the value and importance society places on the Internet and how the Internet will continue to affect our lives.

6. Klaus Etzel, *E-commerce Heads for the 'Net, The Value of Goods & Services Traded Via Business-to-Business Electronic Commerce Will Reach $8 Billion in 1997, Up 1000% vs. 1996: Here's Why Industry Analysts Are So Optimistic About Electronic Commerce*, COMM. NEWS, Nov. 1, 1997, at 72.

7. *See* Craig W. Harding, *Doing Business on the Internet: The Law of Electronic Commerce, Selected Issues in Electronic Commerce: New Technologies and Legal Paradigms*, 9 (1997).

8. Johnny Long, *E-commerce: Doing What's Best for Business, Forget Bits and Bytes: Business Processes Drive the Most Successful Electronic-Commerce Implementations*, DATA COMM., Nov. 21, 1997, at 77. "There are plenty of security protocols to choose from, including secure sockets layer ("SSL"), secure hypertext transport protocol ("S-HTTP"), secure MIME ("S-MIME"), and secure electronic transactions ("SET")." *Id.*

9. A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 55 (1996).

10. The CA's role is an impartial third party. Michael L. Closen & Jason Richards, *Notaries Public – Lost in Cyberspace, or Key Business Professionals of the Future?*, 15 J. MARSHALL J. COMPUTER & INFO. L. 703, 737 (1997) [hereinafter *Lost in Cyberspace*].

CA are similar to a notary, a CA is different because a CA is not physically present when the transaction is consummated. In addition, a CA is providing security for a transaction performed in an inherently insecure environment.[11] In a courtroom setting, the CA is similar to a character called the Fair Witness in Robert Heinlein's science fiction novel *Stranger in a Strange Land*.[12] Heinlein's Fair Witness is professionally programmed to testify truthfully in court when he or she is a witness to an event or business transaction.[13]

This comment will discuss the technology behind electronic document certification: digital signatures which enable parties to sign their names electronically to documents over the Internet. Part II of this comment will begin by discussing the traditional role of the notary in business transactions. Part II will also introduce encryption technology, digital signature technology, and how a CA can provide extremely reliable electronic document certification using such technologies. Part III will discuss the applications where this technology is being used today, albeit sparingly. Part III further discusses an application currently in development that will use digital signature technology in the future on a mass-market basis. In Part IV, this comment concludes that once people become familiar and comfortable with the technology as the market matures, use of digital signature technology will become more common. This in turn will provide a significant opportunity for parties to enhance the security and reliability of their traditional communications and business transactions.

II. BACKGROUND

A. THE ROLE OF THE NOTARY

The origins of the notary date back to the Roman Empire where the ability to read and write was not widespread.[14] The notary was viewed as a trusted public official who for a fee, drafted and safeguarded documents (e.g., contracts) for the public record.[15] Since then, the notary has become an essential part of modern business transactions.[16] A notary's authority is derived almost exclusively by statute as all fifty states have

11. *Cryptopgraphy is the Key to Intranet Security Needs,* COMPUTER RESELLER NEWS, June 30, 1997, at 107. The open architecture and highly scalable Internet communications protocol TCP/IP (which is the backbone of most Internet communications) were not "designed to offer secure communication services." *Id.*

12. Robert Heinlein, STRANGER IN A STRANGE LAND 129-131 (1961).

13. *Id.*

14. *Id. at* 716.

15. *Id.* at 717.

16. Gerald Haberkorn & Julie Z. Wulf, *The Legal Standard of Care for Notaries and Their Employers*, 31 J. MARSHALL L. REV. 735, 736 (1998).

laws regulating notaries.[17] The authority granted to a notary varies from state to state.[18] However, all notaries have the authority to administer oaths and to attest to the authenticity of signatures on documents.[19] This latter authority is one of the primary reasons the notary is essential to many business transactions.[20] When a notary attests to the authenticity of a document by notarizing that document, the notary is verifying both the signature on the document and the signer's identity.[21] Thus, a third party can reasonably rely on the notarization as indicating that the person who signed the document is who he or she claims to be.[22]

The notary is an objective third party who does not represent any party to a transaction.[23] Instead, the notary is a fiduciary to the public, required to perform "with competence, diligence and integrity."[24] The standard of care for a notary is that of a reasonably prudent notary under similar circumstances.[25] The notary has a duty to identify the party asking for notarization.[26] In addition, according to Illinois law, the notary "must determine, either from personal knowledge or from satisfactory evidence, that the person appearing before the notary and making the acknowledgment is the person whose true signature is on the instrument."[27] It is important to note that notaries are not liable for forgeries where the notary acted in good faith and exercised reasonable care in identifying the signer.[28] However, absent good faith and reasonable care, the notary may be liable in negligence for damages proximately caused by the notary's willful neglect or carelessness.[29]

The concept of a writing to affirm a transaction can be traced back hundreds of years to the Statute of Frauds,[30] which required transac-

17. Klint L. Bruno, *To Notarize, or Not to Notorize . . . Is Not a Question of Judging Competence or Willingness of Document Signers*, 31 J. MARSHALL L. REV. 1013, 1020 (1998). *See also Lost in Cyberspace*, *supra* note 10, at 719.

18. *See Lost in Cyberspace*, *supra* note 10, at 723.

19. *Id.*

20. Bruno, *supra* note 17, at 1021.

21. *Id.*

22. *Id.*

23. *Id.* at 1022.

24. Richard Humphrey, AM. NOTARY MANUAL 9 (4th ed. 1948). *See also* Bruno, *supra* note 17, at 1022. "The notary is an agent or trustee of the public and is considered a public officer whose sole purpose is serving the common good." *Id.* at 1022 n.56.

25. Haberkorn & Wulf, *supra* note 16, at 737.

26. *Id.* at 738.

27. 5 ILL. COMP. STAT. ANN. 312/6-102 (West 1998). *See also* Haberkorn & Wulf, *supra* note 16, at 738.

28. *Lost in Cyberspace*, *supra* note 10, at 727.

29. *Id.* at 727.

30. U.C.C. § 2-201 (1998).

tions to be in writing to minimize fraud.[31] A document containing the written signatures of the parties indicate that both parties acknowledge the document and its underlying agreement.[32] A notary's stamp (or notarization) on such document increases confidence in those signatures as "the usual procedure has been that the document be signed by one or more parties, that the identity of each signer be confirmed by the notary, and that the notary memorialize the notarization . . . ."[33] Thus, people use notaries to assure reasonably that the signer of a document is who he or she purports to be, thus validating the legal transaction.[34] A notary does his or her job in the presence of the relevant parties. However, the advances in technology and the Internet have produced an environment where business is being conducted online without face-to-face meetings in what is called electronic commerce ("e-commerce").[35] This prompts the question as to whether a notary can notarize an electronic document on the Internet where none of the parties are face-to-face? If so, can the notarization occur with the same guarantees of trustworthiness that traditional notarizations have enjoyed? The answers to both questions are yes,[36] and the next section will discuss the technology that makes secure electronic document certification possible.

B. The Technology of Digital Signatures

Email comprises the most common use of the Internet by individuals.[37] Literally millions of emails are transmitted on a daily basis all over the world. Unfortunately, emails are not very secure because the open system architecture of the Internet leaves the communication channels publicly accessible. This means that emails can be intercepted by third parties, or emails may appear to be from party X when they are really from Party Y (a process called "spoofing").[38] Therefore, a notary cannot perform electronic document certification via email unless there is a way to ensure email document security and integrity. Digital signatures can provide such security and integrity. However, before digital

31. Glen-Peter Ahlers Sr., *The Impact of Technology on the Notary Process*, 31 J. Marshall L. Rev. 911, 914 (1998).

32. *Id.* at 914-15.

33. Michael L. Closen, et al., Notary Law & Practice: Cases & Materials 10-11 (National Notary Ass'n. eds., 1997).

34. Ahlers, *supra* note 31, at 914.

35. *Unsnarling the I-Way Traffic Jams*, Bus. Wk., Jan. 12, 1998, at 87. E-commerce is defined as "all business that takes advantage of the Internet." *Id.*

36. A traditional notary will need more credentials than currently required to perform electronic document certifications. *See supra* text accompanying notes 69-74 (discussing certfication authorities and their credentials).

37. Scott A. Sundstrom, *You've Got Mail! (and the Government Knows It): Applying the Fourth Amendment to Workplace Email Monitoring*, 73 N.Y.U. L. Rev. 2064 (1998).

38. Gripman, *supra*, note 4, at 168 n.6.

signatures are discussed, a brief discussion about encryption technology is in order.

1. *What is Encryption?*

Cryptography is "the art and science of keeping messages secure . . . [and] the process of disguising a message in such a way as to hide its substance is called encryption."[39] Encryption goes back to Lysander of Sparta who was one of the first military rulers to encode messages to communicate with his soldiers.[40] For thousands of years, encryption was primarily limited to military use.[41] During World War I, a German message urging Mexico to ally with Germany against the United States was intercepted and decoded by British cryptoanalysts who used the message to convince the United States to enter the war.[42] In World War II, allied cryptoanalysts contributed significantly to the war effort against Japan and Germany.[43] However, the advent of computer technology has brought the realm of encryption to the private sector and is now widely available on the Internet.[44]

An encryption software program takes a readable message called "plaintext" and runs it through a mathematical algorithm to scramble the message into unreadable "ciphertext."[45] The ciphertext message is sent to a receiver who uses a "key" to decrypt the ciphertext back into readable plaintext.[46] Anyone who intercepts the message will see unreadable gibberish and without the key, will be unable to unscramble the ciphertext. Thus, encryption allows private and confidential communications via email between parties over the Internet. There are primarily two types of encryption systems used today: private and public key encryption.

2. *Private Key Encryption*

Private key encryption is also known as symmetric encryption,

39. Karn v. U.S. Dept. of State, 925 F.Supp. 1, 3 (D.C. 1996).

40. Ronald J. Stay, *Cryptic Controversey: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmerman*, 13 GA. ST. U. L. REV. 581, 582 (1997).

41. David T. Movius, *Bernstein v. United States Department of State: Encryption, Justiciability, and the First Amendment*, 49 ADMIN. L. REV. 1051, 1054 (1997).

42. Stay, *supra* note 40, at 582.

43. *Id.*

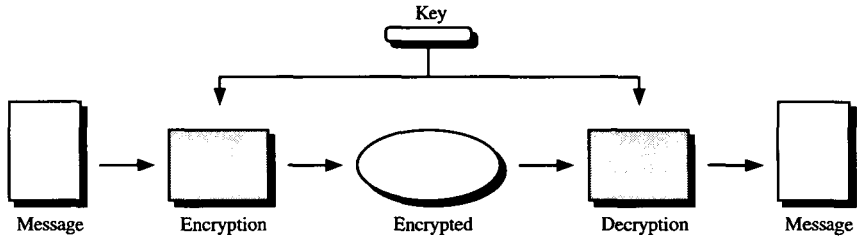
44. *See, e.g., The International PGP Home Page* (visited Aug. 2, 1998) <http://www.pgpi.com>.

45. Bernstein v. U.S. Dept. of State, 922 F.Supp. 1426, 1429 (N.D.Cal. 1996). A "key" is a stream of bits of a specified length randomly created by a computer to encrypt or decrypt a message. *Id.* The longer the key, the more difficult it is to unscramble the message, i.e., a 64-bit key is more secure than a 40-bit key. *Id.*

46. *Id.*

conventional encryption, and single key encryption.[47] Private key encryption relies on the *same* key (a stream of bits of a specified key length randomly created by a computer) to encrypt a message from plaintext into ciphertext, and to decrypt the ciphertext back into plaintext again. An example of private key encryption is a password on a computer system or a personal identification number ("PIN") on an automated teller machine ("ATM"). Hence, if John wants to send Mary an encrypted email, he uses a "key" to encrypt the message and sends the email to Mary. Mary then uses the same key to decrypt the message and only that key will decrypt the message. The following diagram (figure 1) is illustrative:

FIGURE 1



The most popular and widely used private key system is the Data Encryption Standard ("DES"), which is the federal encryption standard enunciated in 1977.[48] However, private key encryption systems have two inherent security weaknesses. First, using the example above, John (the sender) and Mary (the receiver) need to share information about the same secret key and have to trust the other not to compromise that exclusive information.[49] If someone were to steal the secret key information, the security would be effectively breached. Second, John and Mary have a secret key distribution problem.[50] It is not possible to transmit the secret key information securely across the Internet without going offline (e.g., using mail, face-to-face meetings, etc.). In situations between business partners who regularly meet or have opportunities to exchange secret key information, this may not present a problem. However, to

47. *See* Phillip E. Reiman, *Cryptography and the First Amendment: The Right to Be Unheard*, 14 J. MARSHALL J. COMPUTER & INFO. L. 325, 328 (1996). *See also* Philip Zimmerman, *Pretty Good Privacy, Public Key Encryption for the Masses, PGP User's Guide Volume I: Essential Topics*, 1, 4 (1993).

48. *See* Marie A. Wright, *Protecting Information from Internet Threats*, COMPUTER FRAUD & SECURITY BULL., Mar. 1, 1995. "The federal government has used Data Encryption Standard ("DES"), a 56-bit, single key encryption technology, since the mid-1970s for its sensitive, but not classified, information." Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 227 (1995).

49. Charles R. Merrill, *What Lawyers Need to Know About the Internet: A Cryptography Primer*, 443 PLI/PAT 187, 192 (1996).

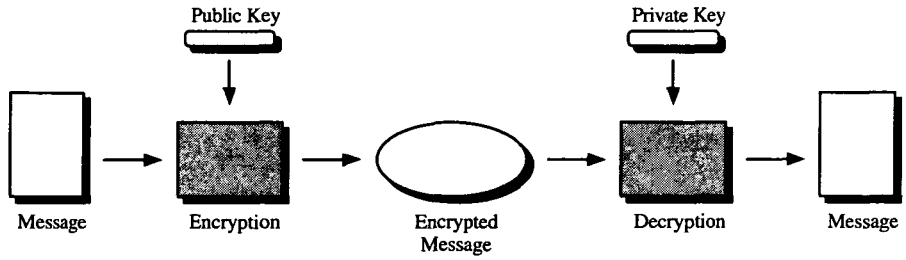
50. *Id.*

those parties who are doing business for the first time over the Internet, this situation is untenable. The solution to these security problems is public key encryption.

3. *Public Key Encryption*

Public key encryption systems use two different keys, one private and one public, to encrypt and decrypt messages.[51] The private and public key are mathematically linked to each other so that if one key is used for encrypting, then the other key is used for decrypting.[52] Unlike private key encryption, the sender and receiver do not need to share a secret key.[53] Instead, Mary (the receiver) generates a public key and a private key pair.[54] The public key is available in a publicly available database called a repository. The private key stays in Mary's possession and is only known to her. Then John downloads Mary's public key and uses it to encrypt a message that he subsequently sends to Mary. The message cannot be read without the corresponding private key.[55] However, using her private key, Mary can decrypt the message that John sent her. The most powerful and widely used public key system is the RSA algorithm.[56] Pretty Good Privacy ("PGP") is a popular public key encryption system based on the RSA algorithm that is freely available on the Internet.[57] The following diagram (figure 2) is illustrative:

FIGURE 2



51. Wright, *supra* note 48.

52. Merrill, *supra* note 49, at 192.

53. Dave James, *Barbarians at the Gate: Internet Security in the Law Firm/Corporate Environment*, 425 PLI/PAT 277, 302 (1995).

54. *Id.* The receiver can send the public key over the Internet, thus the name "public key." *Id.*

55. *Id.* "Messages encrypted with the receiver's public key can be decrypted only with the corresponding private key." *Id.* It is not mathematically feasible to determine the private key code from the public key and vice versa. Wright, *supra* note 48.

56. Rustad & Eisenschmidt, *supra* note 48, at 231. "RSA is marketed by RSA Data Security of Redwood City, California, and it has become the de facto encryption industry standard." *Id.* "RSA" represents the names of its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. *Id.* at 301 n.87.

57. *See The International PGP Home Page* (visited Aug. 2, 1998) <http://www.pgpi.com>.

Now that a basic understanding of encryption technology is established, the next step is a description of digital signature technology.

4. *What is a Digital Signature?*

"A digital signature functions for electronic documents like a handwritten signature does for printed documents."[58] However, a digital signature is not a digitized image of a handwritten signature like the type obtained from a United Parcel Service driver[59] or a Best Buy cashier.[60] Instead, a digital signature is created by reversing the role of the previously explained public key encryption scenario. For example, when John wanted to send an encrypted message to Mary, he created a message, accessed Mary's public key, encrypted the message with her key, and then sent her the message. Mary received the message and used her private key to decrypt the message. For John to create a digital signature, the use of public and private key is reversed.

For the sake of simplicity, let's assume John is not going to encrypt the message itself (which of course he could) because he is more interested in sending a valid digital signature. First, John creates a message: "I agree to pay $500 for one Compaq computer to be delivered to my residence on September 9, 1999 – Please bill my account." Second, he takes the message and runs it through a one-way hash function.[61] A "one-way hash function" is a mathematical algorithm that takes the message data and runs the data through the algorithm to create a unique "message digest."[62] Every time the same message is run through the one-way hash function, the same message digest is produced.[63] However, if a dif-

58. *See Verisign Digital ID Introduction* (visited Aug. 13, 1998) <http://digitalid.verisign.com/client/help/id_intro.htm>.

59. It is now common for a United Parcel Service driver to request a digitized signature from a recipient before the recipient receives a package. This is accomplished by having the recipient sign a hand-held device which stores a copy of the signature in its memory for proof of delivery and for possible reproduction later.

60. When a credit card purchase is made at Best Buy, the credit-card user typically signs the credit slip that lies on top of a hand-held device that digitally stores the signature.

61. C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143, 1149 (1996).

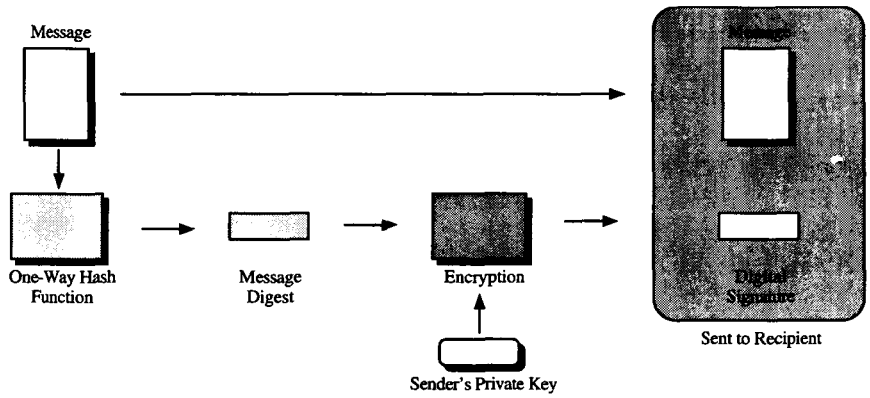
62. *Id.* As an example, a digitally signed contract looks like this:

<Signed SigID=1>
Purchase Order
I agree to pay $500 for (1) Compaq computer to be delivered
to my residence on 09/09/99 – Please bill my account.
John Doe
</Signed>
<Signature SigID=1 PsnID=Doe085>
2AB3764578cc18946A29870F40198B240CD23
02B2349802DE002342B212990BA5330249C1D

63. *Id.*

ferent message is run through the one-way hash function, then a different message digest value is produced. Thus, two different messages will never produce the same message digest.[64] The hash function is considered one-way because it is almost impossible to reconstruct the original message from a message digest.[65] Third, John encrypts the message digest with his private key and attaches the original unencrypted message. John has now "digitally signed" the message. He now sends both to Mary. It is important to note that every digital signature is unique to the document for which it was created. Thus, a forger could not take John's digital signature from one document and attach it to another document. The following diagram (figure 3) nicely illustrates the above process:

FIGURE 3



Mary receives John's original unencrypted message along with the encrypted message digest.[66] Note that Mary has the same one-way hash function that John used to produce the message digest. This is important for verification purposes and is explained shortly. Mary now performs three functions that will verify the validity of the message and digital signature. First, she downloads John's public key and decrypts the message digest.[67] She now has the message digest that John produced. Second, she takes the original unencrypted message attached to the message digest and runs it through a one-way hash function to produce a second message digest. Third, she compares the message digest

64. *Id.*

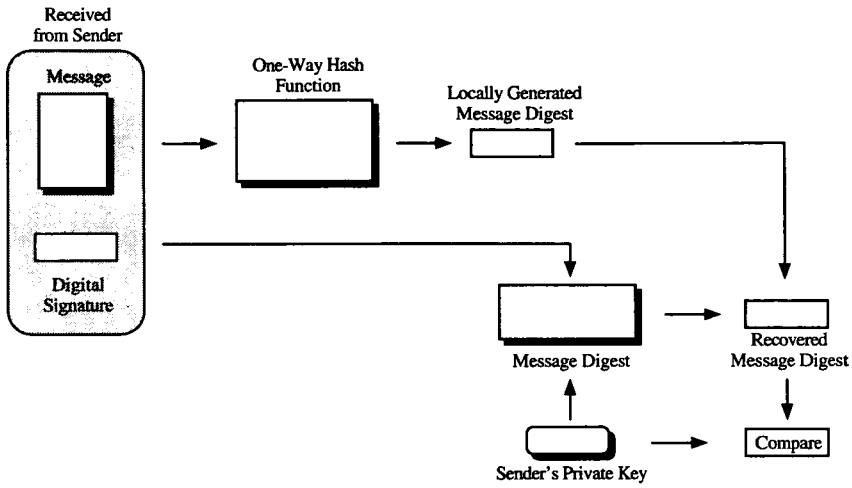
65. *Id.*

66. The message itself could be encrypted, but for the sake of explanation, and for just verifying a digital signature, encrypting the message itself is not necessary unless it requires confidentiality.

67. As an alternative, John could have sent his public key along with the message, obviating the need for Mary to download John's public key.

that John produced (the one she decrypted with John's public key), to the message digest that she created from the original message text. If they are the same, then Mary has confidence that the message did indeed come from John and that the message has not changed since he signed it. She can now ship the computer. The following diagram (figure 4) describes the above process:

FIGURE 4



As demonstrated above, digital signatures using public key encryption technology enable parties to transact business over the Internet by verifying the identities of the parties and the integrity of the messages communicated. However, there is one inherent weakness with digital signatures: the identity of the sender.[68] John may not have sent Mary a message at all. Instead, Igor may have generated a public and private key pair and entered the public key into a public database (repository) under the name "John." Now when Mary attempts to collect the $500 for the Compaq computer, she will discover that she is a victim of a fraud. So the obvious question is how can one verify the identity of the sender? The problem is solved by the certification authority.

5. *What is a Certification Authority?*

"A [c]ertification [a]uthority is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate."[69] In the above scenario where Mary received

68. Biddle, *supra* note 61, at 1150.
69. Froomkin, *supra* note 9, at 55.

the order from John for a computer, if John did not send a CA's digital certificate[70] certifying that his public key did indeed belong to him, Mary would need to verify the validity of John's public key. Thus, she would send John's public key to a CA for verification. The CA's role is to certify that John's public key does in fact belong to John. If the CA certifies that the public key does belong to John, then the CA issues a digital certificate certifying the link between John and the public key.[71] This digital certificate is digitally signed by the CA.

Mary still must verify the authenticity of the CA's digital signature the same way she verified John's, that is, by obtaining the CA's public key, decrypting the message digest, and comparing it with the message digest she produced from the digital certificate to verify a match. If they match, Mary now has confidence that the CA's digital signature is valid, the public key does belong to John, and that his message and digital signature are valid.

There are two big assumptions being made when stating that Mary now has confidence in her transaction with John. The first assumption is that the CA has a valid method of linking public keys to people. The author proposes that a CA must have an initial face-to-face meeting with the person seeking to obtain a digital certificate for his or her public key, just as a notary would require for a traditional signature verification. This way the traditional guarantees of trustworthiness in the physical world would apply to the Internet. A "CyberNotary" might be an appropriate CA, but only if he or she had the following qualifications: "command [of] the technological knowledge and experience required to perform computerized notarizations unlike today's notaries who presumably only have to know how to operate a rubber stamp."[72] In addition, the parties to a transaction might require a CyberNotary to be an attorney, to ensure not only the authenticity of the signatures, but the validity (legality) of the transaction.[73]

---

70. Information Security Committee, Electronic Commerce Division, *Digital Signature Guidelines*, 1996 A.B.A. SEC. SCI. & TECH. [hereinafter *Digital Signature Guidelines*]. This is defined as: a message which at least (1) identifies the CA issuing it; (2) names and identifies its subscriber; (3) contains the subscriber's public key; (4) identifies its operational period; and (5) is digitally signed by the CA issuing it. *Id.*

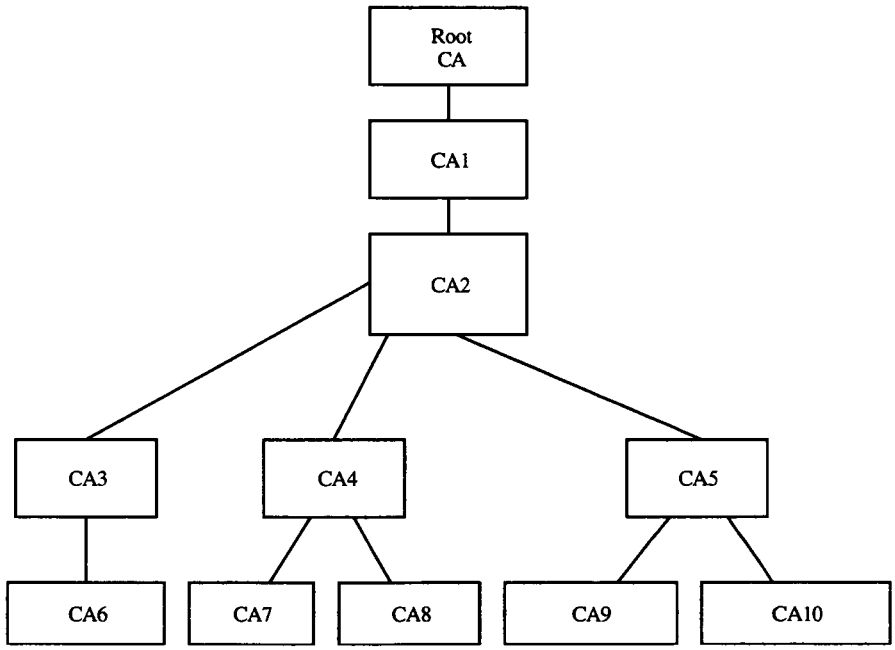
71. Biddle, *supra* note 61, at 1150.

72. Vincent Gnoffo, *Notary Law and Practice for the 21st Century: Suggested Modifications for the Model Notary Act*, 30 J. MARSHALL L. REV. 1063, 1069 (1997). "[A] CyberNotary™ would possess technical expertise to facilitate computer-based transactions requiring a high level of certification, authentication, or other information security services." *Digital Signature Guidelines*, *supra* note 70, at 31.

73. *See Lost in Cyberspace*, *supra* note 10, at 740. "It is necessary to have . . . Cybernotaries who have acquainted themselves not only with computer technologies, but also with electronic transactions and related laws." Shinichi Tsuchiya, *A Comparative Study of the System and Function of the Notary Public in Japan and the United States*,

The second assumption is that Mary is familiar with or trusts the CA and that the CA's digital certificate is in fact a certificate that it issued and digitally signed. If Mary is not familiar with the CA, she might not trust that CA's public key. So she may require another CA (CA1) that she knows and trusts to certify the public key of the original CA. As one can imagine, this can occur over and over in what is called a "certificate chain" or "hierarchy of trust," with a "root certificate" at the top of the tree. The following diagram (figure 5) illustrates the possibilities:

FIGURE 5



When Mary reaches a point in the chain where she finds a CA she can trust, her inquiry may end. One solution to reduce this chain is to make CAs subject to state regulation where they must comply with certain standards to become licensed by a state.[74] This should provide

NAT'L NOTARY ASS'N (1997). "It is proposed that a CyberNotary™ would be required to meet a level of qualification as a legal professional. . ." *Digital Signature Guidelines*, *supra* note 70, at 31.

74. Ill. Attorney General Jim Ryan's Comm. on Elec. Commerce and Crime, *90th Sess., Final Report of the Comm. on Elec. Commerce and Crime.*, (visited March 20, 1999) <http://www.mbc.-com/legis/cecc-fin.html>. Proposed Sec. 15-115 leaves the door open for the Secretary of State to adopt rules which may include "establishing or adopting standards applicable to certification authorities or certificates, compliance with which may be measured by becoming certified by the Secretary of State. . ." *Id.*

Mary with the trust and standard of care assurances she requires to conduct business over the Internet.

6. *Repositories and Certificate Revocation Lists*

After a trusted CA issues a digital certificate attesting that John's public key does in fact belong to him, the CA can publish the certificate in a repository. A repository is "an electronic database of certificates — the equivalent of a digital Yellow Pages" that is generally available to anyone.[75] A repository is generally maintained by a CA and provides users a centralized place to determine whether or not a public key is valid.[76]

However, private key validity and security remain an issue. What happens if a forger somehow discovers John's private key? Or worse, what if a forger discovers a CA's private key? The opportunity for widespread fraud is substantial as the forger can use the CA's stamp of approval for numerous deals. Thus, the ability to revoke the associated public key is necessary. In addition, there are other reasons to revoke a public key. For instance, an employee who had the authority to issue certificates and who is no longer employed should have his or her public key revoked. A certification revocation list ("CRL") provides the means to invalidate a public key.

A CRL is "a list of public keys that have been revoked prior to their expiration date [if any]."[77] A CRL is where one looks to verify whether a public key has been revoked (another function of a repository).[78] Thus, before Mary sends John a computer system, she double checks to make sure John's certificate is not on the CRL. This assures her of the current validity of John's public key and the CA's public key.

C. The Primary Advantages and Disadvantages of Electronic Document Certification Using Digital Signature Technology Over Traditional Notarization

Electronic document certification utilizing digital signature technology provides a more accurate and reliable means to certify documents

75. Thomas J. Smedinghoff, *Digital Signatures: The Key to Internet Commerce, Address Before The John Marshall Law School Conference on Internet & Web Law: Online Commerce and Law* (Feb. 13-14, 1997) (materials on file with author). A repository is "[a] trustworthy system for storing and retrieving certificates or other information relevant to certificates." *Digital Signature Guidelines*, *supra* note 70, at 48.

76. Smedinghoff, *supra* note 75, at 21.

77. Biddle, *supra* note 61, at 1152-1153.

78. *Id.*

over traditional notarizations.[79] However, as with any technology-based solution, it is only as good as the humans operating it.

1. *The Advantages*

a. Message Integrity

Before a traditional notarization, the notary checks the signer for identification, maybe checks for the volition and competence of the signer, and then notarizes the document after the signer signs the document. Yet unless the document is under strict lock and key, there remains a possibility for alteration of the document after signing.[80] In contrast, a digital signature is inextricably linked not only to the signer's private key, but to the document itself.[81] For John to have a digitally signed document he must have done the following:

1) run the message through a one-way hash function to produce a *unique* message digest; 2) encrypted the message digest with his private key; and 3) attached the encrypted message digest to the electronic document.

If the message was changed at any time between John digitally signing the document and Mary receiving the document, the change is detected. The change is detected because Mary will do the following:

1) decrypts John's message digest using John's public key; 2) runs the original document through her identical one-way hash function to produce another (Mary's) message digest; and 3) compares John's message digest with Mary's message digest.

Mary discovers that the message digests do not match and, therefore, concludes that the message was changed in transit and is not valid. It is important to note that while the processes described above appear cumbersome to someone outside the transaction, to John and Mary, the processes are not cumbersome. This is because the encryption software program automatically does most of the work behind the scenes. Thus, if John's message is altered in transit to Mary, her computer automatically alerts her to this fact.

b. Automatic Record Keeping (or Audit Trail)

Most states do not require notaries to keep a journal of their notari-

79. Merrill, *supra* note 49, at 2. "[T]he transition to paperless commerce actually offers an opportunity to raise our level of security expectations far beyond what we have come to expect in the paper-based world, through cryptography." *Id.*

80. Ronald S. Laurie, *Electronic Commerce & Applied Cryptography: Mapping the Patent Minefield,* 491 PLI/Pat 25, 44 (1997). The document is "sometimes easily altered after the fact." *Id.*

81. *Digital Signature Guidelines*, *supra* note 70, at 10.

zations.[82] However, with digital signature technology, a permanent record of all the transactions can be automatically logged into John's or Mary's computer systems. Thus, using a computer system creates a journal during the ordinary course of business.

c. Confidentiality

Obviously, proper care can be taken with paper-based notarizations to maintain confidentiality. However, with digital signature technology, confidentiality is preserved in the ordinary course of business. For John to use his private key to sign a message digitally (i.e., produce a message digest, encrypt it, and attach it to the original message), he must enter a password. When a message is encrypted, it is unreadable to anyone who intercepts the message. Thus, built-in confidentiality is a part of every document that John signs electronically.

2. *The Disadvantages*

a. Lack of Public Knowledge

Most people are not familiar with digital signature technology and its inherent benefits. There are significant security concerns when one considers sending email over the Internet.[83] Such concerns have prompted the Iowa Bar to require attorneys to obtain an express waiver from their clients before engaging in email communications with them.[84] If not, the lawyer has violated the ethical duty to keep his or her client's communications confidential.[85] This potential for ethical violations occurs because of a possibility that email messages can be intercepted by the Internet Service Provider employees or computer hackers. Even though Internet security is a legitimate concern, utilizing an encryption program like PGP is very secure.[86] In addition, even though the process of electronic document certification is somewhat complex, the software employed typically automates the whole process. Thus, the participants

82. *Lost in Cyberspace*, *supra* note 10, at 709.

83. *Commerce Awaits True Security: Internet Economy Will Approach $200 Billion in Year 2000 up from $15 Billion Today*, WALL ST. & TECH., Feb. 1, 1997, at 6 [hereinafter *Internet Grows*]. "Retail consumers are . . . skeptical of putting their [data on the Internet]." *Id.*

84. Iowa Comm. on Ethics and Professional Responsibility, Formal Op. 95-30, (1996). The Illinois Bar takes a different approach by reasoning that because an attorney does not violate a client confidence when a phone call is intercepted, an attorney does not violate a client confidence when an email message is intercepted because both intercepting acts are illegal. Illinois Comm. on Ethics and Professional Responsibility, Formal Op. 96-10 (1997). "[A] lawyer does not violate Rule 1.6 by communicating with a client using electronic mail services, including the Internet, without encryption." *Id.* at 3.

85. *Id.*

86. *See* Merrill, *supra* note 49, at 187-194.

literally just click a few buttons and the software takes care of all the encrypting, decrypting, message digest comparing, and other functions relating to electronic document certification.

b. Infrastructure Costs and Training

The infrastructure is not in place for digital signature technology to be commonplace. Computers and training are necessary to utilize such technology. However, infrastructure costs may not be as high as one might imagine. Many people now own computers, as is indicated by the growth of the Internet. In addition, encryption software can be obtained free of charge.[87] Thus, the infrastructure may be already in place or will be in place in the near future. Yet training will continue to be a problem because there is not an abundance of knowledgeable trainers. Moreover, computer users do not have time to download a 150 page PGP manual to teach themselves how to digitally sign documents.

As it stands today, electronic document certification using public key infrastructure ("PKI") is utilized on a minimal basis.[88] Nevertheless, it will be used on a much larger basis in the future. The next section will show how some of this technology is being used today in addition to how it will be used in the future.

III. DIGITAL SIGNATURE TECHNOLOGY IN ACTION

The growth of electronic commerce over the Internet has been staggering and is forecasted to be a $200 billion enterprise by the year 2000 according to Forrester Research.[89] The reasons are simple: the Internet is an easy and convenient method to obtain product information and to place orders.[90] Even though many people are not convinced that the Internet is a secure way to buy and sell products, electronic commerce continues to grow.[91] The incentive for companies to move their businesses to the Internet are compelling when one considers the following examples:

A face-to-face banking transaction with a teller costs 76 cents; an ATM transaction costs 43 cents; a telephone transaction costs 24 cents;

87. *See International PGP Home Page, supra* note 57.

88. *Compaq Claims Success in International PKI Tests,* ELECTRONIC COM. NEWS (visited July 14, 1998) <www.internetnews.com/ec-news/1998/07/1401-compaq.html>. "Compaq Computer Corp. announced today that the first nation-to-nation Public-Key Infrastructure ("PKI") cross-certification test, which took place on June 1 between the governments of Singapore and Canada, was successfully completed." *Id.*

89. Anita Karve, *Internet Commerce Makes the Sale,* NETWORK MAG., May 1, 1997.

90. For example, a person interested in buying a book can visit *www.Amazon.com* to obtain information on the book and to order it with a few clicks of a mouse button.

91. *See Internet Grows, supra* note 83, at 6.

and an Internet transaction costs 1 penny.[92]

As one can see, the cost comparison is compelling. Before the Internet became popular, large businesses gained the convenience and cost benefits of electronic commerce by using Electronic Data Interchange ("EDI").[93] Hence, before this comment discusses the digital signature technology behind Internet commerce, a brief discussion of EDI is offered.

A. ELECTRONIC DATA INTERCHANGE ("EDI")

Private key encryption technology has been used for decades by corporations in the form of EDI.[94] In the most basic sense, EDI is a business-to-business system used to automate corporate purchasing.[95] Through EDI a corporation can electronically transmit "purchase orders, shipping notices, bills of lading, receipts, invoices, payments, and financial reports."[96] EDI enables a corporation to place an order, to receive order confirmation, and to pay the invoice after receipt, all electronically.

General Electric ("GE") does about $1 billion of business with 1400 suppliers each year using EDI.[97] GE claims EDI has produced large cost savings including a fifty percent reduction in purchasing time.[98] However, EDI technology contains substantial disadvantages that have kept it from wider acceptance in corporate America. First, EDI requires a pre-existing relationship between the parties as they must enter into a trading agreement.[99] This agreement establishes the technical and aesthetic standard for the electronic documents, a catalog with pre-negotiated prices, and a commercial contract.[100] Second, the parties typically use a Value Added Network ("VAN"), which is a proprietary network connecting the parties. While a VAN provides high-speed and secure network communications, it is very expensive.[101] These limitations have

92. John Gunyou & Jane Leonard, *Getting Ready for E-commerce,* GOV. FIN. REV., Oct. 1, 1998.

93. Juan Carlos Cruellas et al, *Public Key Infrastructure Symposium: EDI and Digital Signatures for Business to Business Electronic Commerce,* 38 JURIMETRICS J. 497, 499-501 (1998). EDI was conceived in the 1970s and because of its high initial cost, EDI was used mostly by large companies. *Id.*

94. Ian Curry, AN INTRODUCTION TO CRYPTOGRAPHY 1 (1997).

95. Jay Palmer, *'Net Change: Though the Internet has Disappointed Many an Investor, It's About to Take Off,* BARRONS, July 7, 1997, at 25.

96. Long, *supra* note 8, at 77.

97. Palmer, *supra* note 95, at 25.

98. *Id.*

99. *Ireland: An Overview of the Legal Implications of Internet Trading - A & L Goodbody,* MONDAQ BUS. BRIEFING, Jan. 28, 1998.

100. Greg Rice, *Host-to-Web Creates Bridge for VWR,* ENTERPRISE SYS. J., Oct. 1, 1998, at 54.

101. Etzel, *supra* note 6, at 72.

kept EDI a "big companies' game" reaching "no more than 2% of America's six million companies."[102] However, recent developments, such as "Web EDI," have dramatically reduced EDI's costs and may increase EDI's acceptance by the rest of corporate America.[103]

B. SECURE SOCKETS LAYER ("SSL")

SSL is the most popular form of securing retail Internet commerce.[104] If one logs into such sites as *www.Amazon.com* or *www.1800flowers.com*, one can order books or flowers by clicking a few mouse buttons and entering a credit card number. SSL is the security protocol that encrypts the order and credit card information to provide secure electronic commerce. The following is a summary of how it works.

The Cardholder is logged into a Merchant web site that can process an order using SSL. After the products are selected and an order is ready to be placed, the Cardholder clicks the "order" button. This initiates a process known as an "SSL Handshake:"[105]

1. A "ClientHello" message is sent along with a list of encryption algorithms and the version of SSL the Cardholder supports.[106] 2. The Merchant server ("server") responds with a "ServerHello" message along with the server's choice of encryption that it will use to secure the communications.[107] The server generally chooses the highest encryption algorithm available that the Cardholder will support.[108] 3. The server sends its digital certificate which includes the server's public key. 4. The Cardholder authenticates the site by comparing the information in the certificate with the information the Cardholder has received from the site: the domain name and public key.[109] 5. The Cardholder generates a session key utilizing the agreed upon algorithm.[110] 6. The Cardholder encrypts the session key with the server's public key and sends the encrypted session key to the server.[111] 7. The server decrypts the session

---

102. Palmer, *supra* note 95, at 25.

103. Rivka Tadjer, *Shopping Around for the Best Internet EDI Deal,* NETWORK COMPUTING, Aug. 1, 1997, at 26.

104. *See* LINCOLN D. STEIN, WEB SECURITY: A STEP-BY-STEP REFERENCE GUIDE 1 (1998). SSL is the security standard used most often to accept credit card payments on the Internet. *Id.*

105. *See* Robert S. MacGregor, et al., HOW TO BUILD A SECURE WORLD WIDE WEB CONNECTION, 57-59 (1996) [hereinafter SECURE WORLD WIDE WEB].

106. *Id.*

107. *Id.*

108. *Id.*

109. *The Internet Marketing Center, Learn How to Start and Promote a Business on the Internet, Enabling Technologies: SSL in Action* (visited on Jan. 3, 1999) <http://sellitontheweb.com/e-zine/tech21.shtml>.

110. SECURE WORLD WIDE WEB, *supra* note 105, at 57-59.

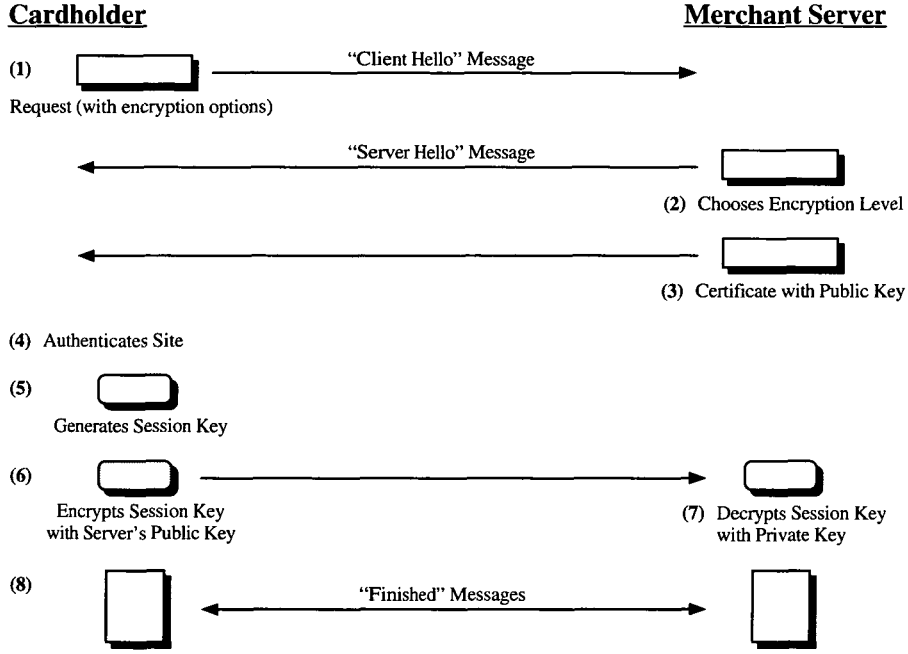
111. *Id.*

key using its private key.[112] 8. The "SSL Handshake" is concluded by the Cardholder and server exchanging "Finished" messages.[113]

This process establishes that the Cardholder and Merchant server are prepared to exchange credit card information securely as "both the [Cardholder] and [Merchant] server switch into encrypted mode, using the session key . . . to symmetrically encrypt subsequent transmissions in both directions."[114]

The following diagram (figure 6) explains the above process:[115]

FIGURE 6



SSL uses the public key encryption system previously explained in the Background section of this comment.[116] The Cardholder's web

112. *Id.*

113. *Id. See also* Stein, *supra* note 104, at 42.

114. SECURE WORLD WIDE WEB, *supra* note 105, at 57-59.

115. It is important to note that with respect to all of the diagrams in this comment, some background processes and optional features are omitted. The author hopes to provide the reader a clear and logical explanation of these detailed and intricate processes without causing the reader a migraine headache. In addition, all of these processes are processed automatically in the background by the Cardholder's and Merchant's hardware and software. The diagrams are based upon information provided by SECURE WORLD WIDE WEB, *supra note* 105, at 57-59. *See also* Stein, *supra* note 104, at 40-42.

116. *See supra* Part II(b)(3).

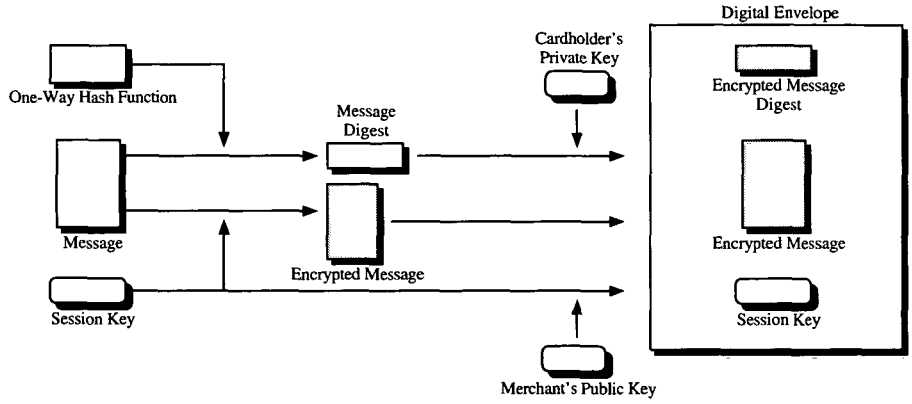
browser software in conjunction with the Merchant server's software enables all of the foregoing processes to occur.[117]

1. The Cardholder's browser software runs the order and credit card information (message) through a one-way hash function to produce a message digest.[118] 2. The message digest is encrypted using the Cardholder's private key and this produces the Cardholder's digital signature for the transaction.[119] 3. The message itself is encrypted using the session key produced during the SSL handshake.[120] 4. The session key itself is encrypted using the Merchant server's public key.[121] 5. The digital signature (encrypted message digest), the encrypted message, and encrypted session key are put together into a "digital envelope" and transmitted to the Merchant server.[122]

The following diagram (figure 7) explains the above process:

FIGURE 7

CARDHOLDER



When the Merchant server receives the digital envelope, it completes the following steps.

1. Uses the Cardholder's public key to decrypt the message digest (MD1).[123] 2. Uses its private key to decrypt the session key.[124] 3. Uses

117. These processes may not occur exactly in the order specified, but do occur contemporaneously within seconds of each other.

118. *How SSL Works*, NETSCAPE NETCENTER (visited January 4, 1999) <http://home.netscape.com/products/security/ssl/howitworks.html>.

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

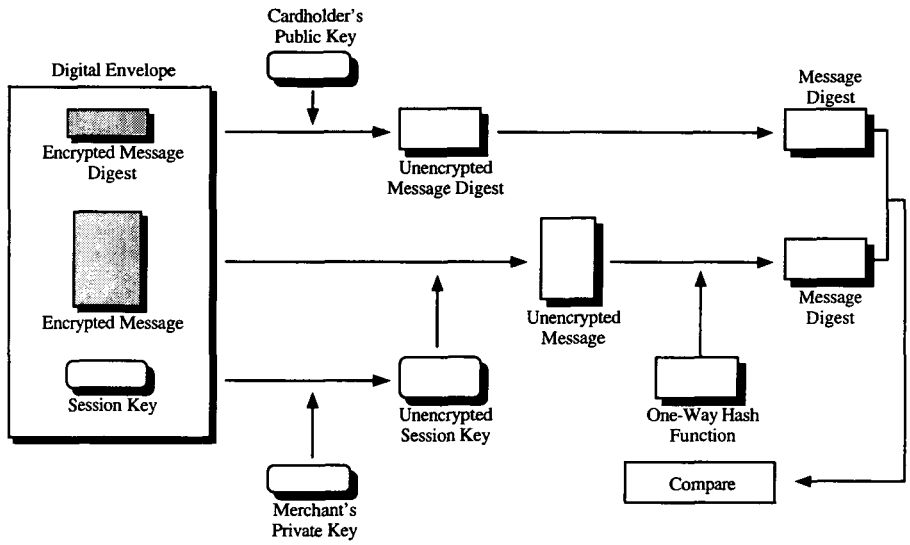
124. *How SSL Works*, NETSCAPE NETCENTER (visited Jan. 4, 1999) <http://home.netscape.com/products/security/ssl/howitworks.html>.

the decrypted session key to decrypt the message (order and credit card information).[125] 4. Runs the decrypted message through the same one-way hash function the Cardholder used to produce a message digest (MD2).[126] 5. Compares the Cardholder-created message digest (MD1) with the Merchant-server-created message digest (MD2).[127]

If the message digests are the same, then the Merchant server knows that the message has not been altered since the Cardholder digitally signed the message.[128]

The following diagram (figure 8) explains the above process:

FIGURE 8



As discussed above, SSL is the most popular way to provide secure retail commerce on the Internet. However, SSL has some significant limitations, which have prompted such corporations as MasterCard, VISA, American Express, Chase Manhattan Bank, Verisign, Microsoft, and Netscape to develop and promote a new security protocol named Secured Electronic Transactions ("SET").[129] The following section de-

125. *Id.*
126. *Id.*
127. *Id.*
128. *Id.*
129. *SET Secure Electronic Transaction Specification, Book 1: Business Description,* Ver. 1.0 (May 31, 1997) [hereinafter *SET Book*]. "Visa and MasterCard have jointly developed the SET Secure Electronic Transaction protocol as a method to secure payment card transactions over open networks." *Id.* at i.

scribes SET technology.

C. Secure Electronic Transactions ("SET")

SET is a new protocol that provides online Cardholders additional security in their online transactions. As in SSL, a session key is created, encrypted, and then decrypted for use only by the intended parties. However, among the new benefits to Cardholders, SET ensures that the merchant is not allowed to view the Cardholder's credit card information.[130] This means that SET may actually provide more security than even person-to-person transactions because one less party has access to the credit card information, thereby eliminating another possible area for fraud and abuse. In addition, all parties to the transaction (the Cardholder, Merchant, and Merchant's bank), are required to authenticate themselves through the use of certificates.[131]

SET provides some additional advantages over SSL. With SSL, the Merchant cannot confirm whether or not the person purporting to be the Cardholder is actually the Cardholder.[132] With SET, when a Cardholder first installs a software "wallet" on her computer system, the Cardholder must obtain a digital certificate from her bank or CA for each credit card.[133] In addition, whenever the Cardholder uses her computer system, she must enter in a PIN number to have access to the secure "wallet."[134] Thus, the chances are significantly better that the Cardholder using SET is who she purports to be over the Cardholder using SSL.

Another advantage is that SET Cardholders can use 128-bit or greater encryption worldwide whereas SSL is subject to United States encryption export restrictions which limits the strength of encryption al-

130. Kelly Jackson Higgins, *Secure Online Transactions: Getting SET,* InternetWeek, Oct. 20, 1997, at 83. "One of the more attractive features of a SET transaction is that the merchant doesn't always get the cardholder's credit card number, unlike SSL . . ." *Id. See also Overview of the SET Protocol* (visited Jan. 4, 1999) <http://www.seas.upenn.edu/~ross/lectures/commerce/set.htm>.

131. *Id.*

132. Jim Kerstetter, *MasterCard Takes Steps to Spur SET Adoption,* PC Week Online (visited Jan. 4, 1999) <www.zdnet.com/zdnn/stories/news/0,4586,269162,00.html>. "Currently, a consumer who makes an online purchase through standard security methods, such as SSL [Secure Sockets Layer] as used by most browsers, is not authenticated to the merchant. (That is, there is no confirmation to the merchant that the person typing in the credit card number is the valid credit card holder)." *Id.* Enhancements to SSL 3.0 include client authentication even though a typical Internet user is currently not required to produce a digital certificate to order products over the Internet. *See generally* Lynda Radosevich, *Digital Certificates Goes Well Beyond Passwords: Digital Certificates, Object Signing, and Secure Internet E-mail Surpass Password-Based Security,* Infoworld, July 28, 1997.

133. *See SET Book, supra* note 129, at 37.

134. *See* Jackson Higgins, *supra* note 130, at 84.

gorithms used outside the United States to 40-bits.[135] Despite the advantages of SET over SSL, however, SET has been accepted by the market very slowly.[136] One major drawback of SET is that it is very slow.[137] Some transactions take 15 to 20 seconds while others take up to 90 seconds.[138] However, the industry is working on improving SET's performance and it may be a viable industry standard in the future.[139] The following summarizes SET processing:

1. The first process in the transaction begins with the Cardholder completing an Order Information message ("OI message").[140] This message is essentially an order form and lists the items the Cardholder wants to purchase. 2. Along with the OI message, the Cardholder completes a Purchase Instructions message ("PI message"), which contains the Cardholder's credit card information.[141] 3. Both the OI Message and the PI message are digitally signed.[142] 4. The Cardholder then uses a session key to encrypt the OI message and then encrypts the session key with the Merchant's public key.[143] 5. The PI message is encrypted using the Merchant's Bank's public key.[144] 6. The encrypted messages are placed into a digital envelope along with the encrypted session key and the Cardholder's certificate.[145] 7. The Cardholder sends the digital envelope to the Merchant, who then uses its private key to decrypt the session key.[146] 8. The Merchant then uses the decrypted session key to decrypt the OI message (while the Cardholder's certificate and digital signature are verified).[147]

---

135. 15 C.F.R. § 730 (1999).

136. Kerstetter, *supra* note 132. "SET's market acceptance has been disappointingly slow." *Id.*

137. Bill Roberts, *On your mark, get SET, wait!* (visited Jan. 4, 1999) <http// www.datamation.-com/PlugIn/issues/1998/april/images/04ecom.html>.

138. *Id.*

139. *Id.*

140. *SET Book*, *supra* note 129, at 58.

141. *Id.*

142. *Id. See also* figure 7 *supra* Part III.B (reviewing digital signing to aid in the understanding of how the OI and PI are digitally signed by the Cardholder). In this case, separate message digests are created for the OI and PI and are concatenated to compute a message digest for both.

143. *SET Book*, *supra* note 129, at 58.

144. *Id.* A more detailed explanation is that a session key is generated which encrypts the PI message and then the session key is encrypted with the Merchant Bank's public key.

145. *Id.*

146. *Id.*

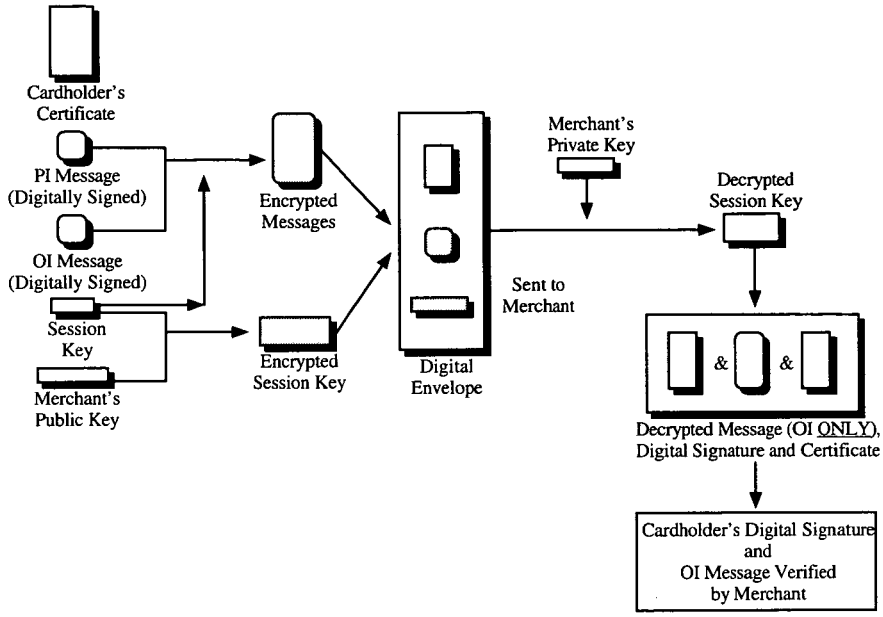
147. *Id. See also* figure 7 *supra* Part III.B (providing a review of how a digital signature is verified). Here, the Cardholder's certificate is verified using the Cardholder's Bank's (or CA's) public key. The Cardholder's digital signature is verified by using its public key as well.

Please note that the Merchant is unable to decrypt the PI message, as it is not encrypted with the Merchant's Bank's public key, of which the Merchant is not in possession.[148]

The following diagram (figure 9) explains the above process:

FIGURE 9

CARDHOLDER TO MERCHANT



When the Merchant receives the digital envelope from the Cardholder, the following protocol is employed:

1. After the Cardholder's information has been verified by the Merchant, the Merchant completes a request for authorization and digitally signs it.[149] 2. It then encrypts the request by using a session key.[150] 3. The Merchant encrypts the session key with the Merchant's Bank's public key and sends it to the Merchant's Bank, along with the authorization request, the PI message from the Cardholder and the Merchant's certificate.[151] 4. Upon receiving this digital envelope, the Merchant's Bank decrypts the session key with its private key and uses the decrypted session key to decrypt the authorization request (while the

148. *Overview of the SET Protocol* (visited Jan. 5, 1999) <http://www.seas.upenn.edu/~ross/lec-tures/commerce/set.htm>.

149. *SET Book*, *supra* note 129, at 60.

150. *Id.*

151. *Id.*

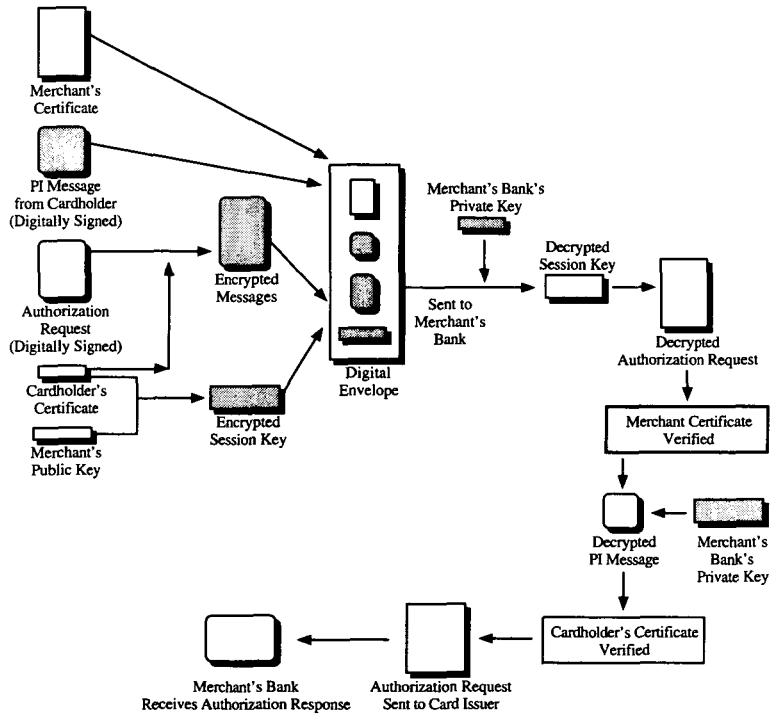
Merchant's certificate is verified).[152] 5. Then the Merchant's Bank verifies the Merchant's identity.[153] 6. If the Merchant's identity is verified to the Merchant's Bank's satisfaction, the Bank decrypts the PI message, again using its private key.[154] 7. The Merchant's Bank then verifies the Cardholder's certificate and sends the authorization request to the institution that issued the credit card.[155]

This authorization request is performed using the standard method that is currently used for any credit card transaction, electronic or otherwise.[156] The Merchant's Bank then receives a response from the credit card issuer.[157]

The following diagram (figure 10) illustrates this process:

FIGURE 10

MERCHANT TO MERCHANT'S BANK



152. *Id.* at 65. The Merchant's certificate is verified by using the CA's public key.

153. *Id.* This is accomplished by verifying the Merchant's certificate and using the Merchant's public key.

154. *Id.* The Merchant Bank actually decrypts a session key with its public key and then uses that session key to decrypt the PI message.

155. *Id.*

156. *Overview of the SET Protocol, supra* note 148.

157. *SET Book, supra* note 129, at 65.

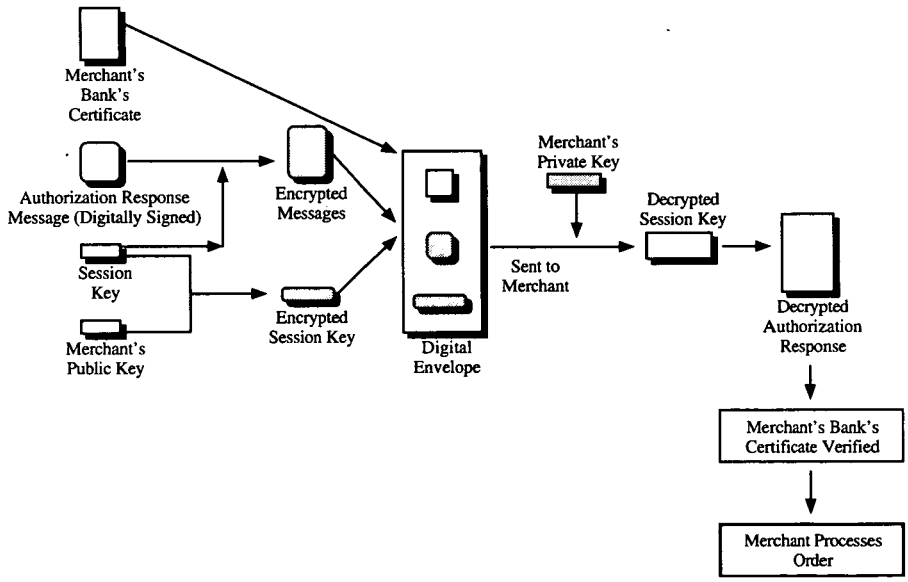
After the Merchant's Bank receives the authorization response from the card issuer, the following process occurs:

1. The Merchant Bank digitally signs the response and places it in a digital envelope along with the Merchant's Bank's certificate and session key (which it has encrypted using the Merchant's public key).[158] 2. The Merchant's Bank sends this information to the Merchant, who decrypts the session key using its private key and uses the decrypted session key to decrypt the authorization response.[159] 3. The Merchant's Bank's certificate is verified and if all has gone properly, the Merchant processes the Cardholder's order.[160]

The following diagram (figure 11) illustrates the process described above:

FIGURE 11

MERCHANT'S BANK TO MERCHANT



IV. CONCLUSION

This Comment has elucidated the somewhat abstruse nature of digital signature technology. Fortunately for a computer user, most of the technological functions of this technology operate automatically, unobservable from the computer user's perspective. While SSL is not the

158. *Id.*
159. *Id.*
160. *Id.*

most secure protocol, it has been used in hundreds of thousands (possibly millions) of transactions with very few actual thefts reported.[161] The more powerful SET protocol has demonstrated that when used properly, SET actually provides *greater* security than traditional face-to-face credit card transactions. Hence, as users become more familiar with such technology and begin to have confidence in their strong security features, electronic commerce will likely fulfill the strong growth projections touted by analysts.[162] There is no question that electronic commerce will continue its torrid growth. Instead, the question is how much will electronic commerce affect traditional commerce and the legal infrastructure behind it.

161. Roberts, *supra* note 137. "A handful of retailers have already completed hundreds of thousands, perhaps millions, of credit card transactions protected by SSL, and no major breaches have occurred." *Id.*

162. Etzel, *supra* note 6, at 72.