1 Va. J.L. & Tech. 6 (Spring 1997) <http://vjolt.student.virginia.edu>
1522-1687 / © 1997 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL of LAW and TECHNOLOGY

UNIVERSITY OF VIRGINIA	SPRING 1997	1 VA. J.L. & TECH. 6

A Law Student's Guide to the Future of Transactions Over the Internet: A Review of the Digital Signature Guidelines

by Christopher P. Keefe[*]

I. The Internet as a Medium of Exchange

1. Almost from the inception of the Internet, scholars, business people and legal practitioners have predicted that the "information superhighway" will become a significant forum for commerce and transactions. The accessibility and ease of transacting on the Internet seems to guarantee that electronic transactions will play a rapidly growing role in the coming global marketplace. However, one significant problem has existed: The conduct of transactions over the Internet demands an impervious security system to protect the information being passed from buyer to seller. The credit card numbers, credit and bank information, and other sensitive data exchanged during a transaction have to be kept safe from hackers and pirates, who always seem to be one step ahead of the latest security measures. Ensuring the security of transactions has become necessary to foster popular trust in Internet as a medium of exchange.[1]

II. Digital Signatures: The Response of the Information Technology

2. Industry has been quick to realize the need for greater security on the Internet. Firms such as VeriSign, Inc. rushed to create a system that would deliver sufficient confidentiality, signer authentication (also known as authentication of origin), and document authentication (also known as authentication of document integrity). In response, Verisign has devised a system based upon dual key cryptography (also called public key cryptography or an asymmetric cryptosystem), which Stratton Sclavos, President of Verisign, has recently stated is "100 times safer than what is done off-line in the mail order and the telephone-order business."[2]

3. Briefly, the technology uses two separate but mathematically related "keys". Either key may be used to encode a given piece of information into an unintelligible form, while the other key is used to restore the data to its original form. One key is called the "private key" and is kept confidential by the holder (presumably the consumer). The other key is called the "public key" and is available to anyone who wishes to conduct a transaction with the holder of the private key. It is computationally unfeasible to derive the private key formula from the public key. Unlike conventional encryption based on a single key that is used to both encode and decode, dual key cryptography does not require knowledge of the secret key to be shared with any other person, increasing the inherent security of the system.

4. To conduct a transaction using this system, software is used to send a message using the sender's private key along with a hash function that transforms the message into a "digital signature". The party receiving the digital signature will use the recipient's software and the sender's public key to verify the signature. This process helps ensure that the message received from the sender was actually created by the sender's private key. The system also verifies whether or not the message was altered after it was digitally signed. A third-party "certification authority" then provides a digital certificate that binds the sender's identity to the sender's public key, to block an impostor from "spoofing" the sender's public key with the impostor public key.

5. The system is best explained, in less technological terms, by Jared Sandberg in a recent Wall Street Journal article.[3] Sandberg describes the following scenario:

> A customer making an on-line purchase simply transmits at the push of a button a three-tiered computer message containing a special decoder key; a message with the goods that are being purchased and their pricing; and a "digital certificate," which contains the user's identity, partial credit card number and the bank that issued the customer's credit card. The merchant uses the key to unlock the message, and uses the certificate to verify the identity of the buyer and the buyer's credit. Once the buyer is deemed legitimate, the purchase is put through and a bill is sent.[4]

Thus,

a card thief would not only have to gain access to a holder's credit-card number, but would also have to break the digital keys to make a purchase.[5]

III. The Digital Signature Guidelines: Placing Digital Signatures into a Legal Framework

6. As one could readily predict, the development of "digital signature" technology created many important legal questions. All of the questions of contract --when is a contract formed, what constitutes repudiation of the contract, who is bound by the contract, etc., --must be asked within the context of the use of the digital signature certificate.

7. Many of these questions were addressed late this summer. During the first week of August 1996, the Information Security Committee of ABA Section of Science and Technology unveiled the Digital Signature Guidelines at the ABA's national convention in Orlando, Florida.[5] A brief discussion of the Digital Signature Guidelines as introduced to the ABA follows.

8. The Digital Signature Guidelines comprise a 99-page book, which after an introduction and technology tutorial, is arranged into five sections, titled: 1. Definitions, 2. General Principles, 3. Certification Authorities, 4. Subscribers, 5. Relying on Certificates and Digital Signatures.

A. Definitions

9. Although the title of this section is somewhat self-explanatory, certain novel definitions incident to digital signature certificates are worth noting. For example, along with basic cryptographic terms, the meaning of acceptance and rejection of a certificate is discussed. An accurate definition of these terms is crucial to establish uniformity and certainty in any commercial system, and digital signature certificates are no exception.

B. General Principles

10. This section enumerates the principles of interpretation intended under the Digital Signature Guidelines. Consideration is also given to possible contractual variation of the provisions of Guidelines by parties and the fiduciary relationship of the certification authority to the parties.

C. Certification Authorities

11. Certainly, this section is one of the most significant sections of the Digital Signature Guidelines. As noted above, the viability of the digital signature certificate system depends on the effective functioning of certification authorities, independent parties who are able to bind the identity of the public key to its owner, to prevent the spoofing of public keys by impostors.

D. Subscribers

12. This section describes the rights and duties of subscribers to the certification authorities, including the method by which a party generates a key pair, and the responsibility to safeguard the private key from compromise.

E. Relying on Certificates and Digital Signatures

13. Finally, the nature, reasonableness, and implications of reliance on a digital signature certificate are discussed. Among other things, this section enumerates the rights and duties of parties who issue and rely upon a digital signature, and apportions responsibility among the signer, the relying party and the certification authority in the event of damage to an innocent party.

IV. The Future of Transactions on the Internet and the Digital Signature Guidelines

14. The Digital Signature Guidelines, while not the final word, provide guiding principles for the resolution of the most pressing questions facing those seeking greater security in on-line transactions.

15. The stakes of this movement are not small. Industry analysts estimate that the type of fraudulent transactions that a dual key system can help prevent (those involving unauthorized transactions) cost credit card companies and banks approximately four hundred million dollars annually. In the coming years, any client who operates either on-line or through a credit-based payment system will expect their counsel to be reasonably fluent in the terms of the Digital Signature Guidelines. This article is intended as a starting point for further consideration of the import of this on-line payment security governance system for those currently at law school.

Footnotes

[*]Mr. Christopher P. Keefe (cpk4s@virginia.edu) is a third-year student at the University of Virginia School of Law. Mr. Keefe is President of the Virginia Society of Law and Technology (VSLaT) and Executive Editor of the Virginia Journal of Law and Technology (VJoLT). The author expresses his appreciation for the contribution of Charles R. Merrill (merrill@mccarter.com), partner of McCarter & English in Newark, New Jersey, and Co-Reporter of the ABA Digital Signature Guidelines, for his suggestions and review of this note.

[1]Specific challenges to security arise from the relative ease with which both identity and address may be "spoofed" by third parties to a transaction. This weakness is compounded by the vulnerability of Internet message packets to undetectable interception, reading and modification by hackers. This vulnerability is primarily due to the TCP/IP Protocol (transfer control protocol/Internet protocol) used by the Internet for transmission of data. In simplified terms, the Internet uses a dynamic, virtual circuit to "ooze" a message packet to its intended destination. This method of transmission can be contrasted with land-based telephone communications, which use switched circuit technology. Although traditional telephone service is certainly vulnerable to intrusion, it is more difficult to do so in an undetected fashion.

[2]Jared Sandberg, *Visa to Introduce Codes to Protect On-Line Purchases*, Wall Street Journal, Sept. 22, 1996, at B2.

[3]Id.

[4]Id.

[5]Id.

[6] ISBN 1-57073-250-7. Available through Service Center, American Bar Association, 750 North Lake Shore Drive, Chicago, IL 60611-4497, Fax: 312-988-5568 (US$34.95 for Section of Science and Technology Members, US$39.95 for non-Members, plus applicable sales tax and handling charges. $20.00 per copy for more than 5 copies, $15.00 per copy for more than 25 copies. VISA, MasterCard, and AmEx accepted.)