Digital Signatures: Are They Legal for Electronic Commerce?

Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process.

Patrick W. Brown

Digital Signature technology may be employed to produce legally enforceable signatures in electronic-based commerce among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process. Business policies for organizational use of this technology are being created as the use of digital signature technology is adopted. Standard industry practice serves to create and substantiate a legal precedent. Digital signatures are especially applicable to interpretations of contracts and statute of fraud law for the electronic medium. Digital signatures may be used to provide assurances in distributed and networked computer environments where electronic transactions require a high degree of trust.

Computer technology is evolving at a rate that is challenging society's ability to deal with the issues it raises. Newly networked and distributed computer systems place computer resources that were once physically remote and difficult to access at the disposal of many potential users. The advantage of computers is being able to quickly process and disseminate large amounts of electronic-based information rather than the slower processing and distribution of information in a physical form (e.g., on paper). Computers are often interconnected to share information and computer resources with users over a widespread geographic area. As a result, more information is available much more quickly.

Electronic-based messages (including fax, electronic mail, and videotex) are taking the place of paper based communications and installing a "new order" in everyday life and commerce. Electronic transactions or messages are passed from sender to receiver which can be resident on different computers. This exchange of data is known as Electronic Data Interchange (EDI). Users can be both people and the machines themselves as message senders and message recipients.

The lack of hardcopy records in EDI creates new risks that must be carefully considered. Individuals and organizations will act upon information included in electronic messages. Electronic messages will be used to perform legal transactions such as making contracts, filing tax returns, and regulatory reports, etc. The electronic media may also be used for illicit purposes. EDI increases information availability but also has associated risks. The law is "beginning to recognize that its classical concepts and rules literally cannot 'do justice' with regard to much actual and potential computer-related litigation" [1].

Digital signatures are a recent technological concept (based upon cryptography) that are on the verge of widespread usage in EDI. Electronic commerce is a specialized form of EDI involving the sale or exchange of goods and services via electronic messaging.

The legal standing of digital signatures has not been significantly tested. This article will focus on the applicability of digital signatures to electronic based commerce, specifically can digital signatures legally replace handwritten signatures on paper. Associated legal, technological, and policy issues will be explored. U.S. law and legal precedents are the main focus, but many of the concepts explored are applicable to electronic commerce in other countries.

Electronic commerce users assume the messages exchanged across the network may be trusted in that the person's name attached to the electronic transaction is the actual sender and the message received is that which was sent. Note that these are two separate assumptions. Without proper controls, electronic information may be easily altered with very little effort by sender, receiver, or someone in between. This is very pertinent to contracts and the statute of frauds, since the electronic medium is so malleable. Specific activities must be undertaken to assure that electronic commerce messages are authentic, accurately communicated, retainable, and that they cannot be repudiated.

In a paper-based society, these assurances are so commonplace they are often taken for granted; a handwritten signature is used to show accep-

PATRICK W. BROWN works with The MITRE Corporation Information Security Center.

0163-6804/94/$04.00 1994 © IEEE

tance/ownership of what is written on the piece(s) of paper to which it is attached. A physical copy of the item is retained on file. For more important transactions, more assurance is required: a notary witnesses signatures for some documents, while a member of a commercial bank or stock exchange is required to witness and authenticate a stock redemption signature, etc. The more important the transaction, the more stringent the requirements for signature authentication.

In electronic commerce, like elsewhere, certain types of messages are inherently more sensitive than others. For example, a contract acceptance is more sensitive than a notice of goods delivery. One requires more integrity and assurance. One will be retained, the other discarded. In the paper-based world, signatures provide a degree of assurance for the more important messages. How can the handwritten signature concept be translated into the new electronic medium? Cryptologic techniques (such as "digital signatures") may be employed to obtain similar assurances in an electronic form.

Signatures

Handwritten signatures are a symbol predicated upon paper-based transactions. They serve to bind the signer to what is printed/written on the paper to which it is attached. Black's law dictionary defines "sign" and "signature" as follows [2]:

Sign — To affix one's name to a writing or instrument for the purpose of authenticating or executing it, or to give it effect as one's act. To attach a name or cause it to be attached to a writing by any of the known methods of impressing a name on paper. To affix a signature to: ratify by hand or seal; to subscribe in one's own handwriting. To make any mark, as upon a document, in token of knowledge, approval, acceptance, or obligation.

Signature — The act of putting one's name at the end of an instrument to attest its validity; the name thus written. A signature may be written by hand, printed, stamped, typewritten, engraved, photographed, or cut from one instrument and attached to another...; it being immaterial with what kind of instrument a signature is made.

The signer is basically authenticating and showing agreement with the document (the legal message) as a whole. As noted in the definition, a signature does not need to be a handwritten signature at all, it can be any symbol adopted by the signer. The individual (an agent) may choose any mark or symbol to employ as a representative of himself (see *Ames v. Schurmeire*, 9 Minn. 221 [Gil. 206] (1864)). This is why illiterates may use an "X" as their signature and have it accepted legally. An autograph is just as popular, but not an exclusive, method of indicating message approval. For example, in *Hillstrom v. Gosnay*, 188 Mont. 388, 614 P.2d 466 (1980), a typewritten name on a telegram was held to be a satisfactory method of indicating approval [3].

The legal implications of a signature depend upon the kind of document one is signing and the circumstances that surround its acceptance. By itself, a signature does not really have much meaning. A signature only has meaning when it is attached to the document and its content in a context.

As an example, let us examine authentication in the case of a classic paper document, a purchase order. By convention, the initiator (an agent acting on behalf of himself or an organization) physically types information including his/her identity on a form or printed letter head, inks an autograph, staples the pages, makes a copy, and delivers the paper via an intermediary such as the postal service to the recipient. The convention makes clear the person is acting as an agent to bind. Trade contracts are covered under the Uniform Commercial Code (U.C.C., which is accepted in all states except Louisiana) and under the statute of frauds. Using these rules, the courts have recognized initials, marks, typewritten names, and stamps as proof of assent. Pen and ink are not necessary. Pencil, carbon copy, or photographic signatures are acceptable. The essence of a signature is intent to use it, (whatever "it" happens to be) to adopt or approve a writing. Under U.C.C. &1-201(39), for example, "signed," includes any symbol executed or adopted by a party with present intention to authenticate a writing. The U.C.C. & 1-201(39) Official Comment explains:

"The inclusion of authentication in the definition of 'signed' is to make clear that as the term is used in [the U.C.C.], a complete signature is not necessary. Authentication may be printed, stamped, or written; it may be by initials or a thumbprint. It may be on any part of the document ..." [3].

Also, the signer must have the authority and the capacity to sign. The intent to sign or authenticate must be clear. If one is not properly authorized to act as an agent, one cannot exercise this authority. The agent must be authorized to enter into a binding contract for himself or the organization he represents. This is especially true in contracting with the Government; all parties must be authorized agents to have a valid contract. If a signature is made "without actual, implied, or apparent authority" (according to the U.C.C.), it is unauthorized.

The statute of frauds illustrates many of the functions and justifications for writing and signing requirements. The statute of frauds generally holds that contracts must be in writing and signed. "Writing" is a ritual that makes the transaction binding and cautions the actors that they are entering into a solemn matter" [3]. Like the writing of the message itself, signing is associated with seriousness and deliberation. Conventional wisdom views a signature as proof (or forensic evidence) of a writing's authenticity and proof of the originator's assent to it, but the proof is not airtight with handwritten signatures. Authorities have tended to be very liberal in determining what constitutes a valid signature; irregularities in form are difficult to prove and tend to be disregarded. In a dispute, each side consults their own expert document examiners to support their position on a documents authenticity. The circumstances surrounding the assent (the parties' authority and capacity, etc.,) tend to be more important.

Some statutes (e.g., statute of frauds) speak of the message being "subscribed." Courts have sometimes interpreted this to mean the signature must appear at the foot of the writing for all of it to be binding [3]. (See *R. C. Durr Co., Inc., v. Bennett Indus., Inc.*, 590 S.W.2d 338 (Ky. App 1979) vs. the signature appearing anywhere on the item as described in Black's definition. This narrow interpretation by the court seems to be following the letter rather than the spirit of the law.

Specific activities must be undertaken to assure that electronic commerce messages are authentic, accurately communicated, retainable and cannot be repudiated.

One may view digital signatures as a highly secure and specialized authentication code based upon an asymmetric cryptosystem.

Digital Signatures

Digital signatures are a specialized application of cryptographic technology utilized to assure the origin of the message and the identity of the sender (originator authentication, the person who "signed" the message sent the message). A number of cryptographic schemes have been developed to provide originator authentication often in combination with other assurances. Individuals and organizations may adopt the use of digital signature technology to assure message integrity, (guaranteeing this is the message which was sent). A digital signature is a string of bits. It is appended to the end of the message. Depending upon the importance of the message, the message itself may be encrypted (message confidentiality, to ensure the message is only available to the sender and receiver).

Digital signatures are based upon the Public Key Encryption (PKE) system first proposed by Diffe and Hellman in 1976. It involves two asymmetric cryptographic keys: one public key associated with the sender which is maintained in the public repository and open to all who ask for it; and one private key the sender uses with the encryption algorithm to "sign" the message. A digital signature binds electronic information to the message using the senders private key (which only the sender holds or knows). The public key is used by message reciepients to decode the signature. Private keys are only used to sign. Public keys are only used to authenticate signatures.

The digital signature is by definition unforgeable since the sender maintains and protects his private key, both keys work only one way and a secure and reliable public key storage and maintaince infrastructure is in place.

Digital signatures differ from handwritten signatures in two important ways:

- No matter how complicated a written signature is, a forger intent on committing fraud will eventually be able to duplicate it, while "a digital signature..., should by definition be inimitable" with a secure implementation scheme.
- A person's handwritten signature should be a constant in the sense that it is "the same" for all documents signed by that person, but digital signatures are by design different for every message

These are fundamental differences. Handwritten signatures are by assumption always "the same" but physically different while digital signatures are different yet can always be "reduced" to a mathematical certainty to be the same. Digital signatures can be measured, while handwritten signatures are more amorphous.

Legal Signatures and Their Electronic Form

There is difficulty in applying writing and signing requirements to electronic transactions since the transactions are not paper-based. It is impossible to draft practical legal rules that are absolutely unambiguous for all occasions. Rigid legal rules do not take technological change, elastic meanings, or specific situations into account [3]. New technology and specific situations are continually altering the interpretation of the statutes, so we must interpret what has come before in applying this new technology concept.

As stated earlier, any symbol may be adopted to indicate the acceptance/approval embodied in a signature.

"A signature's traceability to the signatory [is] very important. Paper-based signatures inherently include forensic traits such as unique pen stroke, ink, or paper, which help identify the signatory. In the absence of paper documents, methods to authenticate EDI transactions (for example, introducing forensic traits to help identify the parties and message content) must be used to ensure trustworthiness and degree of legally probative evidence comparable to that provided by conventional signature" [4].

In generic EDI, a Message Authentication Code (MAC) may be used for this purpose. A MAC embodies all of the attributes of a valid acceptable signature; they are unique, verifiable and "under the [certifiers] sole control such that one may presume from its use that the certifying official, just as if he had written his name in his own hand intended to be bound" [5]. One may view digital signatures as a highly secure and specialized authentication code based upon an asymmetric cryptosystem, which identifies the individual and acts as a symbol of their approval. The courts have previously recognized an array of symbols for this purpose; this is simply one more symbol an individual may adopt that is now available with new technology. This conclusion is not based on the degree of security or forensic reliability provided by the symbol. The main concern is for prevention of deceit. Absent controls, the EDI message receiver can easily alter the text attached to a signature or the signature itself. EDI is a more fluid medium than the previous, more rigid technologies employed.

Any requirement for a signature or its equivalent should be critically scrutinized. Handwritten signatures protect message senders to a limited degree but do not protect message recipients much at all. With or without a signing requirement, the burden would still be upon the recipient to show the senders intent to adopt the message. Fulfillment of this burden usually must rely on the facts and circumstances surrounding the message [3].

Evidence of message origin and contents is crucial Authentication in a paper transaction rests with document examiners. In electronic commerce this may translate into providing assurance evidence of message origin (the sender) and contents (the message) [3]. Electronic messaging may interrupt the usual writing and signing concept conventions in a number of respects. Electronic signatures are not handwritten autographs. They may have a degree of assurance through cryptographic and procedural methods (key management, public key certificates, certificate authorities, etc.,) that the sender did in fact send the electronic message.

Electronic signatures on contracts are no different than the normal signature process. All of the elements to have a valid signature must be present (capacity, etc.,); only the delivery method is different. With digital signatures, even if a message is intercepted, the signature cannot be easily decrypted or altered, and re-sent with this digital signature. Like safety seals on food and medicines, these are not foolproof assurance methods, but they will require the individual to go to great lengths to try to "beat the system." Like broken physical seals, there will be tell-tale signs that indicate the message is not to be trusted.

Few courts have considered how agents act through computers [3]. Electronic messages may also be automatically generated (e.g., an electronic stock trade based upon a data trigger—a stock price change) without human intervention. No human (or no particular individual) may be in the loop. This may have a great many legal implications. In *State Farm Mutual Automobile Insurance Co. v. Brockhorst*, 453 F.2d 533 (10th Cir. 1972), an agent was acting through a computer; the insurance company computer incorrectly sent out an insurance renewal notice. The company argued an "unimaginative" computer could not bind the company. The court held the company liable, reasoning a computer does what you tell it to, so the company was responsible for the actions of its computer. Is this case, there was no signature, but one was implied by the fact the company's computer system created a legal document and sent it out using customary channels. Once again, the generic signature requirements apply (even in their absence); only the technology that provides the message is different.

Other electronic cases furnish compelling support for the proposition that a durably recorded electronic message, bearing a code or symbol intended as a signature, is written and signed. No reported lawsuit has examined whether a purely electronic message satisfies the statute of frauds. Even though there has not been a specific case on the legally of digital signatures, it fits with precedent that these signature methods would be an acceptable symbol of assent. It is simply the method/symbol selected to show acceptance.

As noted earlier, the assurances offered by digital signature technology are especially applicable to business transactions (contracts and the like between people and institutions). Many statutes, regulations, contracts, and charters require legal notices or actions to be written and signed. Government filings are required to be signed: "Every pleading, motion, and other paper of a party represented by an attorney shall be signed...." [3]. Electronic filing saves the time and resources it takes to physically print out, sign, send data, and then reverse the process to get the information back into the receivers' electronic system. The user's symbol, his or her digital signature, could travel with the data to provide authentication with a large degree of assurance. The signature could also permanently reside with the data for record keeping purposes. The government has already begun this practice (usually without digital signature technology). For example, and the IRS allows individuals and businesses to file their tax returns electronically. The government also makes payments and contracts using EDI. "In September 1987, the first payment of U.S. Government funds not requiring a written signature was disbursed" using an electronic certification system (a system developed by NIST based upon their commercial Digital Encryption System). [6].

The U.S. Comptroller General has given formal opinions (in June and December 1991) that federal agencies can use EDI technologies to create valid contractual obligations consistent with current statutory and case law. The use of an "electronic symbol" shows an intent to be bound and the message authentication code (read digital signature) can be used to perform this function [5]. This was followed by a more formal decision in response to a NIST inquiry regarding the specific use of digital signatures by the Government [7]. While these two memos do not constitute a unified legal approach to digital signatures in Government, let alone the private sector, the decisions embodied in them should contribute to the legal recognition of digital signatures [9]. Also, the law notwithstanding the two parties could agree among themselves to choose any method of assent they choose; they could agree to the meaning and use of digital signatures for contracts. As the world's largest contractor and consumer, the Government's lead will set a large degree a precedent and create *de facto* policy.

Many companies have written agreements in place on which their electronic commerce transactions with trading partners are based. It describes their agreement on how to utilize the electronic media. It in effect creates conventions both sides agree to follow. It becomes in effect a contract between the two parties.

As the law comes to recognize the technical changes introduced by EDI and Electronic Commerce as, legal technicalities impeding its use will diminish. Policymakers seem to be proceeding cautiously, waiting for the courts to act on a case-by-case basis to clarify how the statues apply to electronic messages. The status quo is maintained until there is a specific need for the court to address an issue when a case is brought. In the meantime, this leaves EDI and digital signature users at some risk. Adoption of this technology could be impeded where users perceive substantial risks; no one wants to be a test case. Risks for EDI users will diminish as the process develops, becomes better understood, and begins to form its own set of customs and practices.

Public Policy

For the law, the court determines what is custom. This usually follows the use of new technology systems. Historically, judicial efforts have accommodated new technology within the existing laws [3]. To proactively avoid the ambiguity and delay these causes, there are a number of options.

Industry could adopt its own standards and practices (i.e., to foster and develop trade customs that recognize electronic messages and digital signatures as legal entities [3]). The courts would strongly consider these standards in their judicial review. Also, the American Bar Association (ABA) has produced a Model EDI Trading Partner Agreement (published in *The Business Lawyer*, June 1990, known as the ABA Model) to aid in the creation of domestic EDI trading agreements and contracts [3]. The ABA MODEL &1.5 states that an electronic signature is "sufficient to verify" the origin of a proper message. Does it give more weight to an electronic signature than evidence law accords to conventional ink signatures? A signature itself is not sufficient to establish the origin of a paper document in court. Electronic evidence should be treated the same as paper messages under evidence authentication rules [3]. Considering the added assurances they provide, digital signatures may go much further in evidentiary matters. Knowledge and access to the owners private key and its' connection to the corresponding keys may be used to build toward a "preponderance" of evidence where required.

As the world's largest contractor and consumer, the Government's lead will set to a large degree a precedent and create de facto policy.

As EDI electronic commerce transactions become more accepted and widespread, a corresponding number of legal suits and a resulting body of case law will be formed.

The Government through the National Institute Of Science and Technology has developed and published a Digital Signature Standard (DSS) so uniform assurances may be created and promoted [10].

A public key infrastructure (PKI) needs to be developed and adopted to manage public keys, their associated mechanisms and repositories under the PKE. This infrastructure would allow for trusted automated key storage, dispersal and retrieval by users. The trustworthiness of this record system is paramount before the public will adopt its mechanisms. Also the courts will require that the record system be based on a trustworthy foundation before admitting evidence in court. There needs to be "sufficient fact to warrant a finding that records are trustworthy" (*United States v. Craft* 750 F.2d 1354 (C.A. Wis., 1984.)

Another option is to revise the statutes. Writing and signing requirements could be eliminated or electronic transactions could be explicitly permitted. Elimination of writing and signing requirements would require the full facts of the case to be examined in order to ascertain whether a contract truly exists versus the outdated and unworkable proposition that the court needs a specified type of physical evidence (i.e., a signed writing). These rules were developed "to motivate the parties to obtain reliable forensic evidence before acting on it" and "to shield defendants from exposure to trial over unsubstantiated claims" [3]. To throw out these prudent prescriptives seems like throwing out the baby with the bath water; these rules exist to make the process easier and more reasonable. Explicitly permitting and circumscribing EDI has risks as technology evolves further but would also be an effort to (hopefully) foster the growth of technology. Legislation may "confound an already complex picture" [8].

Public policy on digital signature technology and its effects are in the initial stages of being formed and refined. How will society deals with these technology-based issues in a equitable matter for the greater public good? Our society has gone through a similar policy-making process in the past with the introduction of the telegraph and telephone. These forms of communication also had implications in contracts and fraud. The telegraph produces a paper output which has a legal signature (the typed name of the sender) attached to it, when the other things needed to make a signature are present (see discussion above). Voice over a telephone is more fleeting, but may be stored/recorded if special preparations are made to record it; but it may not be sufficient legal evidence in some cases (e.g., if recorded without the participant's knowledge, etc.) EDI is yet a new form of communication; it can be signed and stored in electronic form. Digital signatures and other cryptographic methods can be used to provide assurances of the message sender and the message content. Public policy does not have a direct relationship to the law but does factor into its interpretation by the courts.

Conclusion

In conclusion, digital signatures may be used as legal signatures for electronic commerce transactions within the same general guidelines and requirements as handwritten signatures on paper. They promise more assurance than a written signature; to the technologist, the assurance is assumed with the understanding of the technical details of how digital signatures are designed and operate. From a legal standpoint, this assurance remains to be tested in the evidentiary process.

Digital signatures seem especially applicable to interpretations of contracts and statute of fraud law in electronic commerce. They may be used to provide assurances in distributed and networked environments where electronic transactions need to have a degree of trust associated with them. The federal Government has already begun the acceptance process for this emerging technology; it has begun to issue policy forming statements, is executing legal contracts utilizing EDI, and has issued a DSS. An infrastructure for public key management is being developed. As EDI electronic commerce transactions become more accepted and widespread, a corresponding number of legal suits and a resulting body of case law will be formed. Legislation may also be enacted to make the peculiarities of EDI legal authentication clearer (as they are uncovered with use). The development of the digital signature standard and adoption practices will serve the public by fostering an environment where EDI can flourish and come to its true potential as a communications medium. The main value of digital signatures comes in computer transactions, where electronic users can be sign and execute transactions on-line. And thus authenticate the originator, even when the two parties involved have never before interacted. EDI will not take the place of paper communication with written signatures; it will supplement it and perhaps even someday surpass its usage. Legally recognized digital signatures can expedite this process and may provide an extra/improved level of assurance.

References

[1] Gemignani, Michael C., 1981, Law and the Computer, CBI Publishing Company, Inc., Boston, MA.

[2] Black, H. C., Black's Law Dictionary, 5th edition, (West Publishing Company, 1979).

[3] B. Wright, The Law of Electronic Commerce. EDI, Fax and E-mail: Technology, Proof and Liability, (Little, Brown and Company, 1991).

[4] M. S. Baum, "Legal Standing of Digital Signatures," electronic mail, pp. 1-2, Jan. 1992.

[5] T.H. Armstrong, June 19, 1991, "Electronic Contracting," Memorandum, Office of the Assistant General Counsel to the Controller General, pp. 1-6.

[6] National Institute of Standards and Technology, (NIST), September 1989, Computer Systems Security, Gaithersburg, MD.

[7] Office of the Comptroller General, File 245714, 13 December 1991, "Matter of NIST-Use of EDI to Create Valid Obligations."

[8] J. Newman, "Contracts Made by Electronic Mail: Legal Issues, Technology, and Services," Ethical Issues in the Use of Computers, Wadsworth Publishing Company, Inc., 1985) pp. 237-246.

[9] Department of Justice, Systems Policy Staff, Justice Management Division, Oct. 1990 Admissibility of Electronically Filed Federal Records as Evidence: A Guideline for Federal Managers and Council.

[10] National Institute of Standards and Technology (NIST), September 1991, Proposed Digital Signature Standard (DSS), U.S. Department of Commerce, FIPS Publication.

Biography

Patrick W. Brown has a M.S. degree in technical management from Johns Hopkins University and B.S. degrees in both Computer/Information Science and Horticulture from the University of Maryland at College Park. He has taken coursework in Technology/Engineering Policy at M.I.T. and Washington University. He has 12 years of system engineering experience in governement, industry and consulting roles. He currently works with the MITRE Information Security Center supporting US TRANSCOM efforts at Scott Air Force Base, Illinois. His main interest areas are: secure systems development, electronic commerce, hypermedia, and intellectual property law.