

Electronic Signatures: They're Legal, Now What?

Appears in *Internet Research: Networking Applications and Policy*, 2001, 11(5), 423-434.
Copyright held by MCB University Press.

Martha A. Broderick, J.D.

University of Maine Business School
5723 Corbett Business Building
Orono, Maine 04469-5723
marthab@maine.edu

Virginia R. Gibson, Ph.D.

University of Maine Business School
5723 Corbett Business Building
Orono, Maine 04469-5723
gibson@maine.edu

Peter Tarasewich, Ph.D.

MSIS Department
College of Management
University of Massachusetts Boston
100 Morrissey Boulevard
Boston, Massachusetts 02125
tarase@umb.edu

Abstract

In the United States, electronic signatures recently became as legally binding as printed signatures. But the legislation that made electronic signatures legal did nothing to specify how they should be implemented, or what precautions must be taken to ensure the security and validity of the signature process.

This paper first reviews the status of electronic signatures in the United States, and compares it to work done by the United Nations. Next, the technology that can be used to implement electronic signatures is summarized. The paper concludes with a discussion of problems and open issues surrounding the use of electronic signatures.

Keywords

Electronic signatures, e-commerce, legal, digital signatures

Introduction

On June 30, 2000 the United States adopted S.761 The Electronic Signature In Global and National Commerce Act (e-sign), effective October 1, 2000. This landmark legislation will transform business as it legalizes a process making online electronic signatures legally binding and acceptable. This will happen despite ongoing state concerns for fraud or technical sabotage.

Under the Electronic Signature Act, the United States joins the rest of the world in moving contract creation, modification and storage into a non-paper environment. Prior to adoption of the U.S. Law, more than 40 states including Illinois, Florida, New York, Washington, and Texas had been developing individual state models to recognize contracts authorized by digital and/or electronic signatures. But a few states have been slow to act, out of

concern for such things as fraud, and the need for better document back-up systems to facilitate records inspections.

In one stroke, the federal legislation moved all fifty states into the “electronic transaction age”. The Act itself is deceptively simple. In a short 6 sections, it transforms the traditional State Contract Law requiring “written” signatures binding parties to certain contracts, to a new federal mandate. That mandate stipulates that “electronic signatures,” as yet undefined, must be recognized as legally adequate if they meet very basic criteria. Specifically, electronic signatures must be accepted as valid under this federal mandate:

SEC. 101. GENERAL RULE OF VALIDITY.

(a) IN GENERAL- Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce--

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

While the act exempts certain types of contracts and legally-required notices (see Appendix B, section 103: Specific Exceptions), it clearly is intended to be far reaching as it includes such common contracts as insurance binders, and purchase and sale contracts. Both business-to-business and business-to-consumer transactions are covered. However, when a consumer is a party to the transaction, certain minimal consumer protection is included which requires the business to make specific disclosures (see Appendix B, Section 103 (c) Consumer Disclosures).

Advocates for the disabled have already leveled criticism at this section of the act due to the need for sophisticated electronic communication. Consumer advocates are also taking issue with the provision that validates contracts even when there is no specific consumer disclosure as required by the act.

States are permitted to modify the Electronic Signature Act (see Appendix B, section 102: Exemption to Preemption), but only if they go even further by adopting the more comprehensive “U.S. Uniform Transactions Act” which codifies what constitutes a transferable record, and lays out specific operating rules for creating contracts and modifications. The Uniform Transactions Act also specifies more protection for consumers and different safety procedures for the storage and authentication of original documents. Clearly the Electronic Signatures in Global and National Commerce Act is designed to promote e-commerce in line with developments in the global economy.

Background

The U.S. lags behind many nations in adopting an Electronic Signatures Act. In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce. One article of that law addresses electronic signatures. The UNCITRAL Model Law was developed to establish a set of internationally accepted rules for electronic commerce and to help ensure a secure legal environment for e-commerce activities. UNCITRAL believed that existing national legislation created obstacles to international trade, which increasingly relies on electronic communications. The objectives of the Model Law were “enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information [to foster] economy and efficiency in international trade.” (UNCITRAL 1996, p. 13).

The Model Law does not define electronic commerce, and is intended to include both advanced and less advanced communications techniques, including voice. The law was written to accommodate future technological developments. The law takes a “functional equivalent”

approach, looking at traditional paper-based requirements and determining how those requirements can be satisfied in an electronic context. Requirements focus on ensuring that documents are reliable, traceable and unalterable. The functional equivalent approach does not attempt to define a computer-based equivalent of paper documents, but rather, addresses the purpose of the requirements to help determine how those functions can be met. Table 1 presents functional equivalence concepts.

[take in Table I]

Each of these concepts is addressed in the UNCITRAL Model Law for Electronic Commerce. These functions reflect a hierarchy of requirements. “In writing” is the lowest level in the hierarchy. A document “in writing” is not necessarily attributable to an originator, may be alterable, or may even be fraudulent. Other levels in the hierarchy are more rigorous in ensuring integrity of transactions.

Article 7 of the 1996 UNCITRAL Model Law for Electronic Commerce specifically addresses electronic signatures. The law assumes that the two basic functions of a signature are to: (1) identify the author and (2) confirm that the author approved the contents of a document. There are various levels of signatures accepted on paper, including such things as stamping, perforation, typed signatures and letterhead. At the other end of the spectrum are requirements for handwritten signatures and signatures that are witnessed. In an electronic context the same spectrum exists. Signatures can range from a simple e-mail address or a name typed at the bottom of a message, to systems using encryption, smart cards or biometric devices.

When the Model Law on Electronic Commerce was approved in 1996, UNCITRAL created a working group to study the feasibility of establishing a more detailed set of rules for electronic signatures to facilitate their use in international business transactions. These rules were

to stand as a legal document separate from the Model Law on Electronic Commerce and would outline standards for recognizing digital and electronic signatures (UNCITRAL, 2001). The working group quickly determined that such rules were feasible, but it took five years to develop the Model Law on Electronic Signatures for approval in July 2001 at the UNICTRAL meeting in Vienna.

In the meantime, the rest of the world moved ahead. States, nations and organizations developed text and landmark legislation related to electronic signatures, including:

- American Bar Association – Digital Signatures Guidelines, 1996
- Germany – Digital Signature Law, 1997
- International Chamber of Commerce – General Usage for International Digitally Ensured Commerce (GUIDEC), 1997
- Illinois – Electronic Commerce Security Act, 1998
- Singapore – Electronic Transactions Act, 1998
- Directive of the European Parliament and of the Council on a Community Framework for electronic signatures, adopted November 1999

Today many countries, states, industries and organizations have in place policies and procedures for electronic signatures and are using those procedures in electronic transactions. Because ecommerce is global in nature, transactions will likely span different jurisdictions. It is interesting therefore, to compare the UN Model Law to the US Esignatures Act to identify areas where potential problems may arise.

The UN Model Law Versus the U.S. Electronic Signatures Act

According to Smedinghof and Bro (1999) esignature legislation should (1) remove barriers, and (2) facilitate ecommerce by helping establish trust and predictability. They suggest that esignature legislation be evaluated against three fundamental legal questions: (1) what is legal? (2) can the message be trusted? and (3) what are the rules of conduct for involved parties?

The UN Model Law and the US Esignatures Act differ in terms of how they address each of these legal questions.

The first question, "what is legal?", refers to how or whether the legislation removes barriers as to what constitutes a signature and to what types of transactions are covered. While both the UN and US laws take a "media neutral approach," the UN Model law is more specific in terms of requirements for electronic signatures. The US Act simply states that signatures and transactions will not be denied legal effect solely because they are in electronic form [sec 101 a and b]. The Act does not define or limit electronic signatures. The UN Model Law, on the other hand, addresses "reliability" of electronic signatures. Signatures are reliable if they are unique and linked to the signer, are under the control of the signer and no one else, alterations to the signature are detectable, and the integrity of the document signed is preserved. The UN Model law does not impose constraints on the types of transactions covered.. The U.S. law is intended to be far-reaching, but it does exempt certain kinds of contracts and legally-required notices (see Appendix B, section 103, Specific Exceptions).

The second question, "can the message be trusted?" refers to whether the parties can rely on the authenticity of the message (prevention of forgery), the integrity of the document (alterations are visible) and whether the sender can be held to the communication in the event of a dispute (nonrepudiation). Few electronic signature laws address issues of trust (Smedinghof and Bro 1999). Although the US Act, like most esignature laws, is based on presumptions of the signer's identity and the integrity of the message, it includes a section on notarization. The UN Model Law, however, goes further and specifically addresses the issue of trust in two ways. First, the model law recommends specific requirements to ensure reliability of signatures, as described in the previous paragraph. Second, it recommends rules of conduct for signatories,

those relying on the signatures and third-party certification service providers (CSPs). It also contains a separate section on procedures and systems for ensuring trustworthiness of the CSPs themselves.

Both the US and UN laws address the third question on conduct of involved parties, but they take very different approaches to this issue. The U.S. Act focuses on steps to ensure consumer protection. In fact, the bulk of the text in section 101 of the US law addresses required consumer disclosures and consumer protection. The UN Model law does not address consumer protection at all, but lays out specific rules of conduct for signatories, reliers and certificate service providers. According to the UN Law, signatories must exercise reasonable care to avoid unauthorized use of signatures, notify those relying on signatures if the signature data may have been compromised, and exercise reasonable care in ensuring accuracy and completeness of information. The relying party must take reasonable steps to verify reliability of signatures and check validity of certificates. Two additional articles in the UN Model Law address rules of conduct for certificate providers, as well as procedures and systems for ensuring trustworthiness of CSPs.

Beyond the items described above there are additional similarities and differences between the UN Model Law and the US Esignature Act. For example, both laws recognize foreign electronic signatures and certificates (UN Article 12, US Section 101 h). The US Act addresses several issues not mentioned in the UN Model Law, including retention of contracts and records and accuracy and ability to retain contracts and records. It should be noted that the UN Model Law on Electronic Signatures is designed to add to and refine the earlier UN Model Law on Electronic Commerce, and some of these issues were addressed in the earlier model law.

What will happen when countries that base their laws on the UN Model Law transact business with US Firms? Based on the analysis above one can anticipate that conflicts are likely to arise over issues such as what constitutes a reliable signature or whether adequate disclosures were provided to consumers. UNCITRAL, anticipating some of these issues, plans to begin studying three topics as soon as they gain approval of the Model Law on Electronic Signatures with its Guide to Enactment at the July 2001 Commission meeting in Vienna. Those topics include electronic contracting, dispute settlement, and dematerialization of documents of title, particularly in the transport industry.

Additional complications may arise when the European Union adopts their common framework for electronic signatures. On January 13, 1999 the European Parliament approved (subject to amendments) a legislative resolution proposing a directive on electronic signatures. The directive attempts to harmonize the different member states' legal standards for such signatures, much as the U.S. Esignatures Act preempted state law in this area. Unlike the U.S. law, the EU directive does not relate the esignature issue to the validity of the contracts or non-contract formalities. Of 32 amendments adopted by the Parliament at the First Reading, 22 were accepted in some form and a modified proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures has been developed for further consideration (European, 2001). The timetable for approval and implementation of the EU framework is not yet clear and depends, in large part, on whether member states, some of whom have had electronic signature legislation in place for several years, can agree on common ground.

The United States Electronic Signature Act, the UNCITRAL Model Law on Electronic Signatures and the European Union framework are all technology-neutral. There are advantages and disadvantages of a technology-neutral approach. Among the advantages are that users are not

tied to specific current technologies, and the possibility exists to accommodate future technologies that are yet to be developed. One of the disadvantages of this approach is that the law gives legal validity to substandard methods of authentication.

Implementing Electronic Signatures

Electronic signatures, which uniquely link a person to an electronic document, can be implemented in a number of different ways. The most common method to date has been the *digital signature*. Figures 1 and 2 show how digital signatures can be used to bind an insurance policy (in electronic format) to its holder. Technical terms used in this example are further defined in Appendix A. The term digital signature is often used interchangeably with electronic signature, but is actually a distinct technological implementation of an electronic signature. Other technologies that can be used for the broader category of electronic signatures include personal identification numbers, passwords, smart cards, and biometrics (e.g., fingerprints, retinal scans, and voice recognition).

[take in Figures 1 and 2]

A digital signature uses cryptography for its creation and verification. For this process, two keys are created – a private key known only to the user, and a public key available to anyone. Any document encrypted with the private key can only be read with the public key, and vice-versa. The set of keys can be created by an independent and trusted third party, who becomes a certificate authority and confirms the identity of the person holding the private key.

The content of the document to be signed (the insurance policy in the Figure 1 example) is turned into a digest using a mathematical hashing algorithm. The digest is then encrypted with the user's private key, and is now known as a digital signature. The document, along with its

signature, can then be sent to someone (perhaps the policy issuer in our example). The person who receives the document then decrypts the signature with the sender's public key (Figure 2). They then recreate the digest from the received document using the same hashing algorithm, and compare it to the original digest (the now unencrypted signature). If the two digest versions are not identical, then the document was modified when traveling from the sender to the receiver. This entire process serves the purpose of authentication, message integrity, and nonrepudiation. It should be noted that although a digital signature uses encryption techniques, the document itself is not necessarily encrypted during transmittal. However, the document can also be encrypted if that level of privacy is desired.

Emerging Electronic Signature Technologies

Dozens of companies have been developing technologies that can be used by organizations to implement and support electronic signatures. These can be divided into three categories. First are those companies that provide digital certificates for use with digital signatures. Next are companies that sell software that supports the infrastructure necessary for electronic signatures to operate. The third category includes companies that produce biometric devices and other hardware that can be used to implement electronic signatures. Some of these companies and their technologies are described below.

Digital certificates

There are several companies, including Verisign, Entrust Technologies, and Litronic, which are licensed to issue digital certificates for use with digital signatures. Of these, VeriSign is probably the largest and most well known. The company provides a third-party verification

service to thousands of e-commerce sites using digital certificates. In 1999, they were authorized to supply certificates to the state of California, its citizens, and businesses (Hall and Thibodeau, 1999). VeriSign also offers a service that allows users to reconstruct their private key through any Internet connection, which is a step toward portable digital signatures.

Software

Some companies are focusing on the software, services, and infrastructure necessary to support the use of electronic signatures. One such company is iLumin, which offers a “digital handshake” technology that runs on a business’ Web site and allows customers to enter secured signing rooms to sign electronic documents (Yakal, 2000). Interactions are conducted through any Internet browser, and documents use extended markup language (XML) tags to support multiple signatures and prevent unauthorized changes. The company says its technology creates a “legally binding business closure process” that provides tools to securely review, edit, sign, and store electronic documents.

Many other companies are developing environments for electronic document processing. SignOnline offers a service that issues a digital certificate to an individual after verifying their identity. The individual can then affix their digital signature to any electronic document maintained by SignOnline. The company maintains secure storage and backup of all signed electronic originals, but allows document management functions such as viewing, printing, and searching. Eoriginal has developed a similar environment for electronic documents, but also allows for the transfer of documents to other parties. PureEdge Solutions, Inc. also has a product called InternetForms, which creates legally binding XML documents.

Biometrics and other hardware

Quite a few companies are developing biometric technologies and other hardware that can be used to implement or support electronic signatures. DataKey, Inc. provides smart cards that can store and protect digital credentials. Synaptics, Inc., which makes touchpads for many laptop computers, will bundle digital signature software from Silanis Technology, Inc. with its newer products. Microsoft will begin incorporating biometric authentication technology into its Windows operating systems.

Litronic is developing iris-scanning technology for identification purposes. Sony has a product that digitally records a user's fingerprints, and allows access to a digital signature only after verification of their real print with the digital copy. SecuGen offers a mouse with a built-in fingerprint scanner, or an "EyeD Hamster" scanner than plugs into a USB port. BioNetrix has developed a face-scanning capability to verify user identifications.

Potential Problems, Open Issues, and Challenges

With the new electronic signature legislation, many challenges arise for businesses and states regulating businesses. In the United States, traditionally contracts were the domain of state legislatures. The new federal act has created a host of potential problems and concerns.

Broad definition of electronic signatures

Under the new U.S. act, an electronic signature is broadly defined as:

SEC. 106. DEFINITIONS: (5) ELECTRONIC SIGNATURE- The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

Individuals entering a contract are left to their own devices to prove that the individual being held responsible truly issued the electronic signature. There is no standardization at the present time for what constitutes an electronic signature. The Act has left open the possibility that many different standards for electronic signatures will eventually be used and will need to interoperate.

Incompatibility of product lines

Organizations can create their own electronic signature service, or work with companies that provide a service or the technology to implement electronic signatures. As discussed above, many companies have begun to offer software or hardware that allows organizations to create digital signatures or other forms of electronic signatures, while some are providing software and services that assume the burden of electronic signature implementation. These technologies are not necessarily designed to be compatible with one another, which may cause problems with multi-party transactions.

Conflicting government standards

Interestingly, the U.S. government is emerging as a leader in electronic signature use and could set the standards for others to follow. For two years now, federal agencies have been working under the Government Paper Elimination Act of 1998, which permits federal agencies to accept electronic signatures in place of physical signatures (Tillett and Yasin, 2000). Officials are in the process of forming a central body to set standards for verifying digital certificates issued to government employees and to the public. These certificates, which will be used to support government-related activities such as applying for student financial aid, could easily

number in the tens of millions in as little as 5 years. The U.S. Department of Defense alone has already issued over one million certificates. This means that the government must develop a model for managing a certificate volume that is one hundred times greater than anything expected in the private sector.

The most difficult challenge may be building the needed public key infrastructure to manage the certificates (Gelbord, 2000). Digital Signature Trust and Operational Research Consultants are helping to develop such a system. A virtual “bridge” will also need to be constructed to allow different government agencies to evaluate each other’s certificates. The bridge will be maintained by the Federal Bridge Certification Authority (The Evolving Federal, 2000).

Transfer of power

In the United States, the Electronic Signatures Act has preempted state law. States that had already passed e-signature laws were moving ahead of the federal government in this area. Because the federal act preempts state law, some of these early-adopter states must now readdress their own laws and decide how to supplement the federal mandates. Other states, fearing the passage of such laws, did not act and are now forced to implement a paperless state government regulation system. Areas such as banking and insurance regulations are seriously impacted by the preempting legislation.

Fraud protection

The potential for abuse in this medium exists. The widespread use of electronic signatures may also produce new and unforeseen opportunities for fraud. Protection from

contract fraud, which had been the states' prerogative, has now been drastically altered. It may be easier to pass for someone digitally than it is to forge a signature on paper. For example, forging a digital signature may occur through a breach in the security of keys. Once keys are compromised criminal acts can occur at a much faster pace on the internet than in the physical world. In a paper environment, notarized signatures reduce the potential for forgery by introducing a neutral third party into the process. How will e-signatures be notarized? The electronic signature act provides for a notary process:

Sec 101 (g) NOTARIZATION AND ACKNOWLEDGMENT- If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

In an electronic environment some sort of certification process must exist to serve the purpose currently served by Notary Publics.

Certification

An example of the need for certification is found in the traditional role of notary. Under our consumer contract example, the role of the Data Encryption Standard (DES) keys generated through a "certification service provider" (CSP) would provide verification of electronic signatures online. One could anticipate that all online contractors would find a reliable CSP. This would be an ideal place for states to become involved by licensing CSPs much as Notary Publics are now appointed. This would enable consumers and businesses to verify a CSP's reputation and integrity before relying on the CSP to verify another business or consumer's electronic signature. If fraud or other misconduct by the CSP were to develop, the State could take action ranging from reporting, through fines, to license removal.

Consumer protection

Consumer protection in cyberspace needs to be strengthened. Unsolicited offers should not be permitted to become binding under their own terms, and security of consumer's signatures must be assured. Non-computer-literate consumers will need assistance and protection from the new binding aspects of online contracts. Handicapped individuals may need additional information for contract formation purposes. There is also the potential for a new "digital divide" on the horizon, because the new law allows companies to charge more to customers who cannot or will not do business online.

Dispute resolution

Dispute resolution in contracts has traditionally been dealt with in the U.S. in state courts under state contract law. The rules of offer and acceptance, breach and termination, while uniform for businesses under the Uniform Commercial Code (UCC), vary widely from state to state for non-UCC contracts. Will the introduction of a Federal standard for e-signatures dramatically impact state court jurisdiction over contract disputes? Will a body of Federal common law develop to address these issues or will the Federal courts defer to state common law? In such cases, what would be the controlling state law? These issues of jurisdiction, precedence, conflict of laws and dispute resolution are even more difficult in international transactions. In international trade, will new treaties be necessary to accommodate the new easy to make, easy to deny contracts?

Document storage

Under the new law, businesses will no longer need to send printed copies of documents to customers. This leads to the question of where signed electronic documents should be stored so that they are accessible to all concerned parties. Storage must be secure, and documents must also be protected against destruction – in this case, deletion. Fleet Bank has begun to address this issue by offering “electronic safe deposit boxes” that organizations and individuals can use to securely store electronic documents. The bank handles all security and back-up procedures.

Conclusion

Many businesses, consumers, and lawmakers are waiting to see what happens with electronic signatures. There are predictions of disaster, and of more legislation before the dust settles. Organizations must decide for themselves whether to be an early adopter of this new technology, or to wait a little longer to see if some form of standardization emerges. Examples of U.S. organizations which have been successful early-movers in the implementation of electronic signatures include:

- DLJdirect, which uses digital certificates to verify customer identities.
- Etrade, which has allowed digital signatures to open accounts since March 2000.
- IBM Global Financing, which is using technology by eOriginal to facilitate Web-based commercial lease transactions.
- Salt Lake City, Utah courts, which have accepted digitally signed documents since March 2000 through a system from iLumin Inc.
- The Securities and Exchange Commission, which is using PureEdge software to accept 10K and other regulatory filings via the Web.

There is also a shift occurring from traditional e-commerce to wireless e-commerce, also known as mobile commerce or m-commerce (Tarasewich and Warkentin, 2000). Implementation of electronic signatures using wireless devices will create increased difficulties in terms of security, interface design, and bandwidth limitations.

While the United States has made electronic signatures as legally binding as printed signatures, there is still a long way to go in terms of realizing the benefits of such a move. Much of the uncertainty lies with the fact that the technology is still relatively new, untested, and not standardized. Other less obvious, but nonetheless important, concerns include the sudden preemption of state power in the matter, and the thought that needs to be given to issues such as consumer protection, fraud protection, dispute resolution, certification, and document storage. The authors plan to address each of these open issues further in future research.

Acknowledgements

The authors would like to thank two anonymous referees and the editor for their constructive feedback on the first version of this paper.

References

- The Electronic Signature In Global and National Commerce Act (e-sign). Available at www.senate.gov/search/index.html under S.761 in the 106th Congress
- European Parliament and Council Directive on a common Framework for Electronic Signatures, Amended Proposal (July 2001). Available at <http://europa.eu.int>
- “The Evolving Federal Public Key Infrastructure,” (June 2000). Available at http://www.gits-sec.treas.gov/documents/PKI_Brochure.pdf
- Gelbord, B. (2000), “Signing Your 011001010: The Problems of Digital Signatures,” *Communications of the ACM*, Vol 43 No 12, pp. 27-28.

- Hall, M. and Thibodeau, P. (October 18, 1999), "California Signs Up Digital Signature Provider," Computerworld. Available at <http://www.computerworld.com>
- Smedinghoff, T. J. and Bro, R.H. (1999), "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce," The John Marshall Journal of Computer & Information, Vol 17, pp. 723-768.
- Tarasewich, P. and Warkentin, M. (2000), "Issues in Wireless E-Commerce," ACM SIGecom Exchanges, Vol 1 No 1, pp. 19-23.
- Tillet, L. S. and Yasin, R. (July 14, 2000), "Feds Build ID Model for E-Biz," Internet Week Online. Available at <http://www.internetwk.com/lead/lead071400.htm>
- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996). Available at <http://www.uncitral.org>
- UNCITRAL Draft Model Law on Electronic Signatures with Guide to Enactment (2001) A/CN.9/WG.IV/WP.88. Available at <http://www.uncitral.org>
- Vijayan, J. and Ohlson, K. (July 10, 2000), "Standards Issue Mars E-Signatures," Computerworld. Available at <http://www.computerworld.com>
- Yakal, K. (September 19, 2000), "Sign on the Digital Line," PC Magazine, pp. 32-36.

Appendix A - Glossary of Terms

Authentication – Verifying the identities of individuals.
Certificate – Data message or other record issued by a certifier that ascertains the identity of someone holding a particular key (open, bounded and closed models).
Biometrics – Authentication technologies which measure and analyze human characteristics such as fingerprints, eye retinas, voice patterns, facial features, and hand geometries.
Certificate authority – An independent and trusted third party that issues and manages security credentials and public keys for message encryption.
Cryptography – The science of communicating over untrusted communications channels (see encryption below).
Data Message – Information generated, sent, received or stored electronically.
Digest – A unique, fixed-length number that can only be derived from the contents of a message or document using a hashing algorithm.
Digital Signature – A specific type of electronic signature that uses encryption and keys.
Electronic Signature – A personal identification system that may include digital signatures, personal identification numbers (PINs), passwords, smartcards, biometric or other methods.
Encryption – A method that uses mathematical algorithms and keys to scramble (or encode) a message before sending, and unscramble (or decode) the message when received.
Hashing algorithm – Mathematical procedure for deriving a fixed-length number (a digest) from a message or document.
Information certifier – Person or entity that certifies information and identifies signature holder.
Integrity – Guaranteeing that data are not altered.
Non-repudiation – The inability to disavow a transaction.
Signature holder – Person on whose behalf an electronic signature is created and affixed to a data message.

Appendix B

Excerpts from S.761 The Electronic Signature In Global and National Commerce Act

SEC. 102. EXEMPTION TO PREEMPTION.

- (a) IN GENERAL- A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 101 with respect to State law only if such statute, regulation, or rule of law—
- (1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection; or
 - (2) (A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if –
 - (i) such alternative procedures or requirements are consistent with this title and title II; and
 - (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures; and
- (B) if enacted or adopted after the date of the enactment of this Act, makes specific reference to this Act.

SEC. 103. SPECIFIC EXCEPTIONS.

- (a) EXCEPTED REQUIREMENTS- The provisions of section 101 shall not apply to a contract or other record to the extent it is governed by--
- (1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;
 - (2) a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or
 - (3) the Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A.
- (b) ADDITIONAL EXCEPTIONS- The provisions of section 101 shall not apply to--
- (1) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;
 - (2) any notice of—
 - (A) the cancellation or termination of utility services (including water, heat, and power);
 - (B) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;
 - (C) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or
 - (D) recall of a product, or material failure of a product, that risks endangering health or safety; or
 - (3) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

(c) CONSUMER DISCLOSURES-

(1) **CONSENT TO ELECTRONIC RECORDS-** Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if--

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement—

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer—

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of consent, the person providing the electronic record—

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(2) OTHER RIGHTS-

(A) **PRESERVATION OF CONSUMER PROTECTIONS-** Nothing in this title affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, regulation, or other rule of law.

(B) **VERIFICATION OR ACKNOWLEDGMENT-** If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

(3) EFFECT OF FAILURE TO OBTAIN ELECTRONIC CONSENT OR CONFIRMATION OF CONSENT- The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) PROSPECTIVE EFFECT- Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) PRIOR CONSENT- This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) ORAL COMMUNICATIONS- An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

Table I - Functional Equivalence

Traditional Paper-Based Concept	Function or Purpose of the Concept
In writing	Information in a message is accessible and usable for future reference.
Signed	Author of a message is identifiable and has indicated approval and/or receipt of information in the message.
Original	Integrity of the information is assured from the time it was first generated in its final form. The data must be complete and unaltered, apart from endorsements or normal changes arising from communication.
Retention	Message must be accessible and usable, retained in the form generated, enabling identification of date and time received and sent. Dates of modification must be identifiable.
Attribution	Addressee can assume that the message was sent by the originator, a person authorized to act on the originator's behalf, or sent by an information system authorized to operate automatically.

Figure 1 – Example of Attaching a Digital Signature to an Insurance Policy

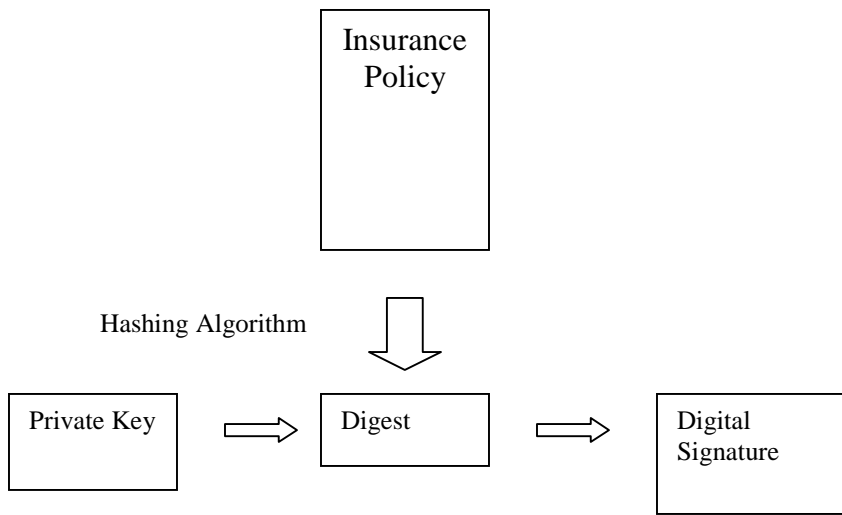


Figure 2 – Example of Reading a Digital Signature from an Insurance Policy and Verifying the Integrity of the Document

