

Electronic Data Transfer: Electronic Signatures

Contributed by Victor O. Schinnerer & Company Inc.

Revised February 2007

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

CONSULT YOUR ATTORNEY

The information herein should not be regarded as a substitute for legal advice. Readers are strongly advised to consult an attorney for advice regarding any matter related to the electronic transfer of documents and electronic identity authentication technology.

SUMMARY

The Electronic Signatures Act, more commonly known as “E-Sign,” has made electronic documents and signatures legally binding. Provisions of the law and practical ways to apply it are discussed. This article is part of a series on electronic data transfer. See Resources/More Best Practices for related Best Practices articles.

THE ELECTRONIC SIGNATURES ACT

In October 2001 the Electronic Signatures in Global and National Commerce Act (known as ESA or the more euphonious “E-Sign” bill) became law. E-Sign is the federal government’s effort to ensure that consistent and predictable legal rules will govern electronic transactions. Although more than 40 states had previously enacted electronic authentication laws, Congress recognized that inconsistencies in law from state to state deter businesses from using electronic signature technologies to authorize contracts or other legal transactions. E-Sign establishes a common legal framework for interstate electronic commerce.

The federal law is based largely on the Uniform Electronic Transactions Act (UETA), a model statute promulgated by the National Conference of Commissioners of Uniform State Laws. Although UETA was designed to be adopted by state legislatures, Congress eliminated the need for state statutes by passing E-Sign, which explicitly restricts the states’ rights to modify, limit, or supersede the provisions of the federal law.

PROVISIONS OF THE STATUTE

Authenticating the identities of parties to an agreement is a necessary element of law and commerce. The proliferation of electronic commerce

creates a need for reliable methods of electronically authenticating the identities of the parties to a contract, establishing payment mechanisms between them, and settling disputes using of recognized electronic audit trails as supporting evidence. The lack of a legally recognized electronic signature has been a significant impediment to the use of electronic agreements as legally binding documents.

In general terms, E-Sign establishes that contracts may not be invalidated solely because they are in electronic form or were executed with an electronic signature. The law defines an electronic signature as 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. With E-Sign, Congress has made electronic documents and signatures legally binding.

THE LAW AND TECHNOLOGY

Technology develops faster than legislation can be enacted. Mandating a specific technology might stifle innovation and the emergence of newer, more reliable technologies. Currently available digital-signature technology is only one of many possible ways to authenticate the identities of parties to an agreement. For this reason, the federal law, unlike most state laws, is technology-neutral; it does not mandate one type of electronic authentication technology over another, nor does it set forth guidelines for the use of a particular technology.

CONTRACTS AND AGREEMENTS

Under the federal law, a reply e-mail message could satisfy the definition of a valid electronic agreement if the language clearly establishes the intent. For example, an e-mail message stating, “I am replying to your e-mail with the intent to accept your offer to provide services” probably would create a valid contract if the e-mail was in response to an e-mail that transmitted a contract proposal that included standard terms and conditions as well as scope, compensation, and schedule.

It is important to note, however, that except when a government agency is required to accept electronic signatures on certain documents, the law does not require any person to agree to use or accept electronic signatures or records.

ELECTRONIC RECORDS

E-Sign further establishes that electronic records may be legally valid, provided that an electronic version of a document accurately reflects the contents of its printed equivalent and remains accessible to those persons entitled to access it in a form that can be accurately reproduced for the period required by law.

DIGITAL SIGNATURES

Most state laws focus on digital signatures, a specific type of electronic identity-authentication technology thought to be most secure.

State laws also provide for the quality and trustworthiness of digital certificate authorities. A digital certificate authority is a third party entrusted with proving the identity of the sender of an electronic document. Digital certificate authorities maintain a “private key” infrastructure that ensures the identity of the holder of a private key, making digital signatures as usable in commerce and in legal proceedings as a written signature on paper. Appropriate responsibility therefore may be ascribed should one of the parties in an electronic transaction deny liability under the transaction. Those engaging in electronic commerce are assured that the message and the electronic signature attached to the message can both be verified and can be used in court to bind the signer to the contract or agreement.

Digital signatures provide assurance not only that a message or contract was encrypted but also that the sender is who he or she claims to be and that the message has not been altered in transit. They are simple, available, and inexpensive. VeriSign (www.verisign.com), a leading provider, sells individual certificates; the registration process takes about five minutes. Once a digital signature is obtained, it can be used for signing documents and for encrypting documents sent to another person.

There are a number of questions to answer before you buy a digital signature, including what the legal requirements are for retaining the documents and what level of technology is needed.

E-SIGN IN PRACTICE

E-Sign will make contracts and records subject to federal jurisdiction acceptable in electronic form. Digital signatures will speed up electronic procurement. In the design and construction industries, bids will be received, verified, and accepted electronically; project Web sites will be used to negotiate, document, and execute change orders; and pay requests will be reviewed and signed by appropriate parties without any need for paper copies.

Although a digital marketplace may improve transaction speed and efficiency, the full legal ramifications and the effect upon professional service relationships have not yet been tested.

ADDITIONAL RESOURCES

The full text of Public Law 106-229, the Electronic Signatures in Global and National Commerce Act, can be downloaded as an Adobe Acrobat (PDF) file by visiting www.access.gpo.gov/nara/nara005.html.

RESOURCES

More Best Practices

The following AIA Best Practices provide additional information related to this topic:

- 10.02.02 Electronic Data Transfer: A Guide To Managing Opportunities and Risks
- 10.02.03 Electronic Data Transfer: Receiving Information from Others
- 10.02.04 Electronic Data Transfer: Project-Specific Web Sites

For More Information on This Topic

See also “Technology and Information Systems” by Michael Tardif, Assoc. AIA, *The Architect’s Handbook of Professional Practice*, 13th edition, Chapter 13, page 373.

See also the 14th edition of the *Handbook*, which can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by email at bookstore@aia.org



Key Terms

- Practice
- Information management
- Office information resources