

Digital Signatures – The Silver Bullet for E-Signature Laws

Date: May, 2001
Version: 1.0



Digital Signatures: The Silver Bullet for E-Signature Laws

During the past few years, U.S. Federal and State governments have introduced many new pieces of legislation meant to accelerate the transition to e-business. Many of these bills focus on electronic signatures, electronic record-keeping and online privacy. What is their message? You can, you should and, in some cases, you must use e-signatures to achieve the promise of e-commerce and e-government. Because these new laws are different, ambiguous and sometimes inconsistent, they have added to the very uncertainty and risk they were meant to reduce. In their wake, organizations that want to implement electronic signatures are left to wonder, "Which law should I comply with? What if State and Federal laws are inconsistent? Will I get sued? How can I be sure a signature is secure? Whose signature is it anyway?" This paper will briefly review U.S. e-signature laws and explain why *digital signatures are the best practice for e-business transactions*.

Electronic signature is a generic term that refers to any representation in electronic form that can be used to express *intent*, including a printed name at the bottom of an e-mail, a digitized copy of a hand-written signature, a biometric mark, a sound, or a digital signature. **Digital signature** is a specific type of electronic signature based on public-key cryptography, used within a framework known as public-key infrastructure (PKI).

Recent e-signature legislation comes in many flavors, and the definition of electronic signature is not applied consistently. Some e-signature laws are technology-neutral with no caveats; others have certain restrictions. Some are technology-specific with limited requirements; others are very prescriptive. PKI-powered digital signatures by contrast, offer a clear way through this morass. Unlike many other forms of electronic signatures, digital signatures comply with even the most stringent of the new U.S. e-signature laws because they are almost impossible to forge if properly implemented. With PKI, a digital object that has been signed and sealed will stay protected wherever it is, whether stored or

in transit. Along with this end-to-end protection, comes the ability to prove how a digital transaction unfolded. Specifically, digital signatures allow you to verify:

- Who you are dealing with (identification)
- Who is authorized to access what information (entitlements)
- How individuals will be held accountable for their online commitments (accountability)
- That the information has not changed since it was signed (integrity)

Early Efforts

The American Bar Association pioneered early electronic signature guidelines, and in 1995, Utah became the first state to introduce related legislation. Today, almost all states have adopted some form of e-signature legislation. Some states, such as Minnesota, Missouri, Utah and Washington, treat digital signatures as the technology of choice; others treat electronic signatures generically. Since these statutes can be general or restricted to a specific use (like medical records or brokerage agreements), many states have more than one e-signature law. The lack of conformity and consistency among these laws and across different jurisdictions creates confusion and uncertainty.

Taming the Dragon: The Uniform Electronic Transactions Act (UETA)

In 1999, The National Conference of Commissioners on Uniform State Law (NCCUSL) approved UETA as an overlay statute to help reconcile conflicting state laws. UETA says that signatures and contracts in commercial transactions cannot be denied legal effect just because they are in electronic form, as long as the relevant parties affirmatively opt-in. It defines an electronic signature as "an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the

intent to sign the record.” Many states have already adopted UETA, or different variations of it. According to UETA, an electronic signature can be attributed to an individual only if it was the act of that person, or someone that person authorized to act on his behalf. Because digital signatures can be used to verify authenticity with a far higher certainty than any other form of electronic signature, they are ideally suited to the task of attribution, while most other electronic signatures are not.

The Feds Get Into the Act: The Electronic Signatures in Global and National Commerce Act (E-Sign Bill)

The Federal government's response to the proliferation of different state e-signature laws was to pass E-Sign, which took effect on October 1, 2000. Like UETA, E-Sign is an overlay statute that says a signature cannot be denied legal effect just because it is electronic. It allows for the use of electronic records and signatures in virtually any commercial transaction unless specifically excluded by law. E-Sign adopts most key UETA provisions and creates a baseline for all 50 states. States can comply with E-Sign by adopting the official text of UETA or adopting rules that are *consistent* with E-Sign. But since it is unclear how the courts will define consistency, parties implementing electronic signatures should carefully compare the available alternatives. The safest and surest approach? Rely on best practice, namely digital signatures, since they can satisfy even the most demanding requirements among these different bills.

The Big Three: Gramm-Leach-Bliley, HIPAA and GPEA

Other Federal statutes that deal with privacy and electronic records are driving the evolution of e-business. Among the most important are the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley), regulations associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Government Paperwork Elimination Act of 1998 (GPEA).

Gramm-Leach-Bliley contains security and privacy compliance guidelines for organizations engaged in financial activities. It requires financial institutions to safeguard customer information, protect the security and integrity of records, and protect against unauthorized access. It also requires them to provide notice and opt-out to their customers and to limit the reuse and marketing of personal information. Digital signatures offer the best means of satisfying these requirements. By allowing for authentication, authorization and accountability, digital signatures will play a crucial role in helping organizations comply with Gramm-Leach-Bliley.

Recent HIPAA regulations outline health information privacy requirements and set a deadline of 2003 for compliance. HIPAA requires authentication, authorization, secure audit trails and accountability for those dealing with health information. It includes provisions for electronic authentication of individuals who access or alter information in electronic records, patient consent for the release of information to other healthcare organizations, and the right of patients to know what information has been disclosed. Because of the criminal penalties and stiff fines for non-compliance, healthcare organizations are taking HIPAA very seriously. Digital signatures can provide the authentication, authorization, audit and accountability mandated by HIPAA.

The Government Paperwork Elimination Act set a deadline of October 2003 for U.S. agencies to develop, where feasible, the electronic maintenance, submission, and disclosure of information. This includes the use of electronic signatures, especially if they allow paper processes to be put online, and maintenance of overall system security and integrity. Digital signatures are ideally suited to this task.

Conclusion

Numerous e-signature laws that have been passed in recent years are different and sometimes inconsistent. This ambiguity has added to market uncertainty, especially when electronically signed transactions cross multiple jurisdictions. But the demand for e-business and the deadlines included in some recent privacy and electronic record laws are making it imperative for organizations to find a way to comply with them. Digital signatures are the form of electronic signatures best suited to meeting the criteria spelled out in these laws. By providing the most robust means of determining who you are dealing with (identification), who is authorized to access what information (entitlements), and providing a verifiable record of the transaction (verification), digital signatures provide the cornerstone for trust on the Internet.

For more information on digital signatures, visit the Entrust Resource Center at <http://www.entrust.com/digitalsig/index.htm>

Entrust® Inc. (Nasdaq: ENTU) is the leading global provider of enhanced Internet security solutions and services that make it safe to do business and complete transactions over the Internet. Entrust has the industry's broadest set of identification, entitlements, verification, privacy and security management capabilities. More than 1,200 major corporations, service providers, financial institutions and government agencies in more than 40 countries rely on the privacy, security and trust provided through Entrust's portfolio of award-winning technologies. For more information, please visit www.entrust.com.