

Electronic Signature Law and CIC's eSignature Products

Background

It has been over a decade since the E-Sign Law was passed in June 2000 granting electronic signatures the same legal standing as traditional wet signatures. The legality of electronic signatures is now well established, not only through statutes such as the E-Sign Law but also in case law.

As a pioneer in electronic signatures, with close to fifteen years since our initial deployment at GINNE MAE in 1996, CIC deployments have played a key role in establishing that legality. CIC has focused on and established successful large scale deployments with leaders in the financial industry. Clearly, the legality of electronic signatures was an issue that required much discussion in past years as major insurance companies we teamed with paved the way in establishing the benefits of the unquestioned legality of electronic signatures.

As adoption of electronic signatures accelerates the issue of legality has begun to arise again, especially with small private businesses, and therefore we present in this paper an overview of the fundamental legal issues and also the several specific laws relative to electronic signatures with the intent of providing an understanding of how CIC has designed its products not only to comply with those laws but also to enhance best legal practices.

In the past there existed a great deal of confusion on the distinction between electronic signatures and digital signatures. It is important to note that much progress has been made in clarifying and communicating the distinction especially by industry analysts such as Gartner and Forester.

Concisely stated, an electronic signature combines a secure digital signature with paperless processing. More specifically, an electronic signature can functionally be defined as technology that ensures authentication (one of which is PKI authentication certificates), confidentiality, data integrity (notification and invalidation of documents if the integrity has been compromised) and non-repudiation of electronic documents and allows "straight through processing," eliminating the requirement for paper-based documents to complete contracts and agreements.

Digital signatures have become synonymous with PKI and therefore comprise a subset of electronic signatures in that it is one of the methods of authentication. Therefore a digital signature is an electronic signature that authenticates and executes a document. It ensures the identity of the sender or signatory and the integrity of the document or file.

PKI, requiring Digital Certificates is simply not efficient in high volume customer facing business processes including the need to routinely send documents to clients and customers. PKI is focused on encryption and not the signing ceremony and as such is better suited to securing servers as opposed to documents or signatures. PKI remains an integral part of nearly all major vendors' electronic signature solutions, but is not widely used on the front end for signer identification and authentication. Rather, its value is its contribution to securing a document once it has been signed to ensure that the document cannot be altered after signing, that there is a non-repudiable audit trail and the electronic document can be securely stored and viewed only by authorized parties.

"...The e-Sign Law does not specify any technology as required or acceptable for its purposes but rather establishes that a transaction or document cannot be denied enforceability because it is in electronic format..."

Electronic Signature Law and CIC's eSignature Products

“... CIC recognizes that although the process should adhere to certain standards, various organizations will adopt different technology solutions based on several factors: the cost of hardware and software, PKI management & deployment costs, environment (customer facing vs. over the web), usability and impact on legacy systems. The ultimate factor in deciding what process to use will be the acceptable risk mitigation associated with the transaction...”

US Federal Law

There are significant differences between the various laws and regulations that govern the use of electronic signature technology. However, several very important elements can be found explicitly defined or implicitly identifiable. For example, the US Electronic Signatures in National and Global Commerce Act, commonly referred to as the E-Sign Law, requires that:

1. The signature must be under the sole control of the individual
2. The signature must be verifiable
3. The signature must be unique to the individual
4. The signature must establish the individual's intent to be bound to the transaction
5. The signature must be applied in a tamper-evident manner

The E-Sign Law does not specify any technology as required or acceptable for its purposes but rather establishes that a transaction or document cannot be denied enforceability because it is in electronic format.

CIC complies with the Federal E-Sign Law through its patented Ceremony® process and associated application user interfaces. The company's Sign-it® product works from within common applications like Adobe Acrobat or Microsoft Word and provides support for several different signature technologies. The most critical issue we address is the manner in which the signature is collected, the associated Ceremony data, (Who, What, When, Where, & Why), and the protection of the data to ensure a truly non-repudiable result.

It is important to recognize that the specific implementation of an electronic signature technology will affect its legal enforceability. For example: having users click on an "I Agree" button with their mouse is acceptable technology under the law, but is it enough to cover the risks associated with a given

transaction? Today's online banking is a good example of where this concept applies. Many of us login to one of the major banks to transfer funds, send checks, or manage our investments. Virtually all of these transactions take place with the click of a button that reads "Pay Bill," "Make Transfer," etc. However, it is the fact that you entered a password that established your identity at the beginning of the process that enabled the bank to identify you; and the bank is also capturing certain activity / information about you while you are online as part of the permanent record (e.g. date/time, IP address, etc.).

CIC has approached this problem in much the same way with its Sign-it offering. The following illustrates the specific ways Sign-it meets the requirements of E-Sign Law:

- **The signature must be under the sole control of the individual**

Sign-it supports biometric signatures that can be in the form of a handwritten signature, voice, or fingerprint. For lower risk applications, CIC also supports signature stamps and electronic seals as well as simple click-wrap. Based on its modular design additional signature methods can be supported with the development of a small signature specific interface without modification to the main application.

- **The signature must be verifiable**

CIC can verify biometric signatures in real time with complex algorithms or, of equal importance, provide subsequent verification of the data through forensic analysis of the signature dynamics or measurements, (e.g., analyzing the stroke sequences or writing speed of a handwritten signature, or the speech patterns of a voiceprint, etc.).

Contact:
1-650-802-7888

info@cic.com
www.cic.com

Electronic Signature Law and CIC's eSignature Products

“...CIC complies with the Federal E-Sign Law through its patented Ceremony® process and associated application user interfaces...”

Contact:
1-650-802-7888
info@cic.com
www.cic.com

- **The signature must be unique to the individual**

The use of biometric data ensures that it is unique to an individual regardless of whether it is a physical measurement like a fingerprint or a behavioral biometric like handwriting or speech. In the case of cryptographic signatures, CIC utilizes unique keys for each signatory.

- **The signature must be applied in a tamper-evident manner**

CIC uses industry standard encryption to protect users' signatures and the integrity of the documents to which they are affixed. Specifically CIC uses the SHA-1 message digest algorithm to create a value unique to the document and signature data, so that any tampering with either can be detected. To protect the integrity of the data itself, CIC uses three layers of NIST approved cryptography. In the event a user has his or her own PKI keys, CIC also supports those keys provided they are compliant with PKCS-7 or PKCS-11.

State Law Uniform Electronic Transaction Act (UETA)

Attempting to bring uniformity to the state law level, and having been adopted by virtually all states, the UETA puts electronic and paper-based commerce on the same legal footing. It grants electronic signatures or records the same validity and enforceability as manual signatures and paper-based transactions. It does not make electronic transactions mandatory; it simply provides a framework to ensure their legality when they are used.

In general, the UETA specifies that an electronic signature system, in order to conform to the law, must provide an environment that proves:

- The record can be controlled by an individual
- If a document is revised, the revision is identified as authorized or not authorized

- That a single original version (authoritative copy) of the document exists and it is identifiable as such and can be shown to have been transmitted to the controlling individual
- If a copy is made, that the copy is easily identified as a copy, and that copies can only be made with the permission of the controlling individual
- That an audit trail exists as part of the original or authoritative copy that details who was the last person to receive the document

Conclusion

CIC recognizes that although the process should adhere to certain standards, various organizations will adopt different technology solutions based on several factors: the cost of hardware and software, PKI management & deployment costs, environment (customer facing vs. over the web), usability and impact on legacy systems. The ultimate factor in deciding what process to use will be the acceptable risk mitigation associated with the transaction.

It is common practice for an end user license agreement to require a user to click on an "OK" button before allowing installation of a software application. For an ordinary software application where most users understand the risks associated with software applications the risk level is acceptable. However, from a pure risk standpoint, clicking a simple button likely would not be acceptable in closing on a mortgage or buying a car.

CIC is confident that it is one of the only companies in the market today that has designed a solution that enables organizations to deploy a technology that embodies their legal and compliance strategy and policies within a common enterprise component to minimize the risk associated with automating signature-centric processes.

For more information or to discuss CIC's products in detail, contact us at sales@cic.com.

Electronic Signature Law and CIC's eSignature Products

“...The e-Sign Law does not specify any technology as required or acceptable for its purposes but rather establishes that a transaction or document cannot be denied enforceability because it is in electronic format...”

Disclaimer:

The application and interpretation of the Electronic Signature body of Law to specific transactions and processes can be highly dependent upon, among other considerations, the nature of the transactions and specific circumstances surrounding the transactions as well as the industry in which the electronic signature technology is being used. The legality of the overall transaction or business process can involve both the functionality of the electronic signature product and the solution it is embed into. This document, therefore, is not intended to provide any form of legal opinion or legal advice and should not be relied upon for that purpose. It is provided solely for familiarizing the reader with certain aspects of CIC's products and to denote certain aspects of electronic signature law that CIC took into consideration in designing those products.

Any method.

Any popular format.

The key to paperless business processes.

Communication Intelligence Corporation (“CIC”) is a leading supplier of electronic signature solutions for business process automation in the Financial Industry and the recognized leader in biometric signature verification. CIC's products enable companies to achieve truly paperless work flow in their eBusiness processes by enabling them with “The Power to Sign Online”® with multiple signature technologies across virtually all applications. Industry leaders such as AGLA, Allstate, Charles Schwab, JPMorgan Chase, Prudential, Travelers, and Wells Fargo chose CIC's products to meet their needs. CIC is headquartered in Redwood Shores, California and its products are sold and supported globally. For more information, please visit our website www.cic.com.



Contact:

1-650-802-7888

info@cic.com

www.cic.com