



Electronic Signature Law and CIC's eSignature Products

Background

There is a great deal of misunderstanding in business today about what constitutes an electronic signature and whether or not any specific technology is compliant with various laws and industry specific regulations. This article will address several specific laws and regulations with the intent of providing an understanding as to how CIC has designed its products to comply with those laws and regulations.

It is important for the discussion to elaborate on the distinction between an electronic signature and a digital signature. An electronic signature is any symbol of intent that may be applied in an electronic form. It can be in the form of simply typing your name, clicking an "I Agree" button, signing on an electronic pad similar to what you see at most major retail chains, or entering a Personal ID number or password.

A digital signature is very clearly defined as part of the National Institute of Standards and Technology (NIST) standard for Public Key Infrastructure (PKI) and the Digital Signature Standard (DSS). Specifically, these can be found in NIST FIPS 140 and FIPS 186 located on the web at: <http://www.itl.nist.gov/fipspubs/by-num.htm>.

In a very simplistic form, PKI can be described as a pair of keys that are assigned to an individual for establishing his or her identity in the electronic world. The keys are referred to as a public key and a private key. The public key can be shared with anyone, while the private key is kept under the control of the owner and released, using a password, for digitally signing documents or data. A more in depth study of this subject matter is available on our website at <http://www.cic.com/resources/whitepapers/>.

The bottom line weakness of PKI is that in most signing applications a digital signature is released using a password. The fact that a password can be compromised, shared, stolen or hacked makes it the weakest point in the system. Arguably, a digital signature, in and of itself, may not be sufficient to meet legal requirements. CIC values the use of PKI technology and strongly recommends the use of PKI in conjunction with other technologies, such as biometrics to protect the digital signature or the corresponding document.

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*



Communication Intelligence Corporation

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 a user 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:

- **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 password-based signatures used in conjunction with PKI, signature stamps, 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, equally importantly, 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.).
- **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.



Communication Intelligence Corporation

- **The signature establishes the individual's intent to be bound to the transaction.**

A handwritten signature is analogous to a symbol of intent. As a society, we have spent our lives signing documents with a pen and an electronically captured handwritten signature is a logical extension of that practice into the digital world. While this is implicitly true of establishing intent, it is not always enough. Through its application interface, CIC presents a "Gravity Prompt" (a statement of intent) to ensure that the signatory is fully aware of the purpose for which the signature is being provided, regardless of the underlying technology.

- **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 Commercial Code (UCC)

The UCC, unlike e-Sign is not a federal law but rather an attempt to standardize certain laws of commerce among the various states. The UCC is typically adopted by individual states with some modifications from the model document. Certain types of transactions governed by the UCC are excluded under e-Sign.

A recommended article for review on this subject matter is:

<http://www.ntia.doc.gov/ntiahome/frnotices/2002/esign/ucc/comments/mccabe/pebcomments.htm>

Uniform Electronic Transaction Act (UETA)

In addition, requiring adoption at the state level, 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 exist as part of the original or authoritative copy that details who was the last person to receive the document



Communication Intelligence Corporation

A recommended article for review on this subject matter is:
State Legislatures Magazine: March 2000, New Laws for the Digital Age, Jo Anne Bourquar,
<http://www.ncsl.org/programs/lis/cip/300digital.htm#UETA>

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.

Disclaimer:

Electronic signature law is a complex, highly specialized and relatively new body of law. The application and interpretation of that body of law to specific transactions 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. This document 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.