

ELECTRONIC SIGNATURES A CIC PERSPECTIVE

"It is not a Bitmap, cannot be copied and pasted, cannot be bulk added to multiple documents, requires physical signing by the author."

What is it?

What is the purpose of an Electronic signature?

The recently passed Electronic Signature in Global and National Commerce Act (E-SIGN) signed by President Bill Clinton will now enable true e-business solutions by giving electronic signatures the same legal weight as wet ink signatures on paper. Organizations that move towards a paperless workflow process will gain significant cost savings from electronic signatures, thanks to the technology, due to its efficiency. This is best exemplified by reducing the business cycle and operating costs such as printing, distribution, collection and, storage of paper documents. Additionally, a well-implemented Electronic Signature methodology will improve overall reliability and security of every transaction.

What is CIC's Electronic Signature?

CIC electronic signature is the most universally understood and accepted way to capture an individual's signature on an electronic document such as MS Word, Adobe Acrobat PDF, or any other electronic form. When deployed, our electronic signature eliminates the need for paper and ink and captures a legally binding and tamper evident handwritten biometric signature. Because the software is based on a handwritten signature it is intuitively obvious and socially recognized form of electronic signature.

What is Handwritten Biometric Electronic Signature?

CIC's electronic signature is defined literally as a biodynamic, which means it is a measurement of a behavior performed by the human body versus a measurement of the human body. While signing their name in a traditional manner, the electronic signature software measures the speeds, rhythm, patterns, habits, etc., unique to the individual. These measurements are different for each signer based on the qualities and characteristics of their handwriting.

Why are Biometrics important?

Because they are unique to each individual, the underlying biometrics of CIC's Signature can be used to verify the authenticity of the signature and therefore the identity of the individual signing their name. The biometric measurements from each signature may be compared to available samples and are a secure and reliable method to assure that the signature is not a forgery.

Is the CIC electronic signature technology legal?

CIC's technology has been accepted and deployed by federal and state agencies in the United States. Our electronic signature technology meets all the applicable requirements set forth by the E-SIGN bill signed by President Bill Clinton (refer to White Paper titled: Secure and Paperless with Electronic Signatures), as well as requirements by other federal agencies such as the FDA's 21 CFR Part 11 (refer to White Paper titled: Electronic Signatures & FDA). Additionally, CIC Signature has been deployed by various insurance companies throughout the United States and has been reviewed and accepted for use by the Insurance Commission in virtually every state.

How does this address Non-Repudiation?

Lets explain what the term "non-repudiation" really means. The terms "deny" and "repudiate" are synonymous in the dictionary. In the legal sense to repudiate a signature is to either claim a signature to be a forgery, or if not a forgery, then the signature was obtained using "fraud" or "undue influence". Therefore for a signature to be "non-repudiated" it must reduce the ability of the signatory to deny the signature as a forgery at a later date.

CIC's biometric signature addresses the non-repudiation issue of a signature by being:

- Unique to the person; the biometric measurements captured while signing, such as speed, rhythm, patterns, habits, etc are unique to the signer that can not be duplicated by anyone else.
- Capable of verification; the biometric measurements from each signature may be compared to available samples and are a secure and reliable method to assure that the signature is not a forgery.
- Under the sole control of the user; the biometrics of a signature are based on an individual's behavioral dynamics, which cannot be repeated by another person.
- Symbol of Intent; world wide, a person's handwritten signature is recognized and understood to be indication of the individual's intent and agreement

How is it used?

How can electronic signature be used?

The most obvious answer is that an electronic signature replaces a wet ink signature anywhere within an organization's workflow. For example, Policy Applications, Account Opening/Closings, Administrative changes to an in effect policy, Underwriting Approvals, Claims Processing, Internal Reporting, HR forms, etc.

The other area where a verifiable electronic signature can be utilized is to replace passwords. A handwritten electronic signature can be verified against a previously created template to allow access, therefore replacing the function of a password, but adding a level of security to the process. The security gained is due to the fact that a password/pass phrase can be given to someone else or stolen or even forgotten, where a signature belongs to the signer and cannot be forged easily since it is a biometric (refer to question/answer below). Some examples of electronic signatures replacing passwords are, Network access, Securing laptop or handheld computers, securing specific files on a network, etc.

How can this technology be used? Do I need special software?

CIC offers its software in two forms, either as an "off the shelf plug and play" application or as SDK's (software developer kits) for customized applications.

The "off the shelf" solution is called [Sign-it®](#). Sign-it family of products may be used with Adobe Acrobat or Microsoft Word. If the workflow being used within an organization is based on PDF or Word documents then the Sign-it provides a "turn key" implementation that does not require any software development effort.

If a different workflow or document management system is being used such as html or xml documents, visual basic applications, or any specialized applications then CIC's software developer kits, [InkTools®](#) or [iSign™](#), may be used to integrate a biometric electronic signature with the system.

Has this technology been tested in the Court System?

Yes, CIC Electronic Signature Software is deployed in several court systems in the United States where it is used by judges, clerks, attorneys, etc. to sign official court documents. In addition, many Forensic Document Examiners have been working with biometric signatures to prove the authenticity of a signature.

Do you have customers using this in Insurance?

Yes. Numerous insurance companies use CIC Electronic Signature technologies in a variety of applications including New Application and Administrative Policy changes. For example, American General Life Assurance has processed more than 750,000 policy applications that have been signed with our technology (refer to AGLA Case Study).

How does it fit into my environment?

I already have a document management system, how does this fit with it?

Most document management systems store native Word and/or Acrobat documents. CIC [Sign-it](#) will integrate with these authoring environments, enable an electronic signature to be applied, and the document or form can be stored in the document management systems, as usual.

Should a more sophisticated method of integration be required, our SDK, [InkTools](#) or [iSign](#), can be used to integrate an electronic signature into any system that supports ActiveX controls, 32-bit Dynamic Link Libraries (DLLs) or Java.

We already have a complete workflow process where our agents just fax a signed form directly into our document management system, why is this better?

CIC's electronic signature integrates within your existing workflow process, and eliminates the cost and effort of printing, distributing and insuring proper versioning of all forms. The documents can be generated on the agent's computer, signed electronically and automatically sent to the appropriate place in your organization. Our electronic signature is considerably more secure than a faxed signature for many reasons. More importantly, no one can alter information on an electronic document without CIC's solution detecting the change. Biometrics provide additional information beyond what a paper signature provides, to help prove its authenticity both at the time of signing or a later point in time.

How does this technology fit within our existing PKI system?

Although not dependent upon PKI, CIC's electronic signature solution can be integrated within an organization's existing PKI methodology. Typical use with PKI technologies include:

- Biometric Authentication: Using underlying biometrics, a handwritten signature is biometrically verified as an enhanced Authentication scheme to replace or in addition to password confirmation.
- New Account Opening: Collecting a "first time" customer's handwritten signature takes less time and costs less than issuing PKI credentials.

How can I use this in a web environment for Agents and/or Customers?

An electronic signature can be integrated into a web form using our software developer kit, [iSign](#). The form can be accessed through the Internet or Intranet, filled out and signed using any signing device, such as a mouse, a digitizer tablet or a PDA (Palm Pilot). The information on the form (including the signature information) will be sent to its appropriate destination using the TCP/IP protocol.

What do we need to buy, in terms of hardware and software to deploy a signature solution?

For successful installation, software is required from CIC or one of CIC's authorized resellers. CIC supports the widest possible range of hardware devices including digitizers, touch screens computers, PDAs, Palm devices, etc. Virtually any available touch sensitive screen may be used as the "sensing surface" to capture the signature.

SECURE AND PAPERLESS WITH ELECTRONIC SIGNATURES (Signature Capture & Verification)

As enterprises move to a paperless environment, the need for signatures has presented a hurdle preventing the completion of the automation loop. Since the Internet and Intranets are used to exchange information it is essential to be able to sign documents electronically in a secure fashion. In both consumer and enterprise applications, the ability to securely capture signatures, as well as to verify the identity of people, is increasingly important. The electronic signature solution used in enterprises must be simple to use, secure, and meet legal and regulatory requirements.

There is currently no universal or national standard for an electronic signature. All 50 states as well as some government agencies have enacted or currently have pending legislation governing the use and acceptance of electronic signatures. The enacted legislation from the congress are the Government Paperwork Elimination Act (1998 Senate Bill 2107), and Internal Revenue Restructuring and Reform Bill (1997 House Bill 2676). Some of the pending Bills in the congress are, Digital Signature Act of 1999 (House Bill 1572), Electronic Security Transaction Act (Senate Bill 921), Paperwork Elimination Act of 1999 (House Bill 439).

The laws and regulations differ, but there are several clear patterns. The most common definition of an electronic signature derived from many of the state laws is:

The term "Digital Signature" is defined as "a digital or electronic method executed or adopted by a party with the intent to be bound by or to authenticate a record, which is unique to the person using it, is capable of verification, is under the sole control of the person using it, and is linked to data in such a manner that if the data are changed the digital signature or electronic signature is invalidated."

CIC's technology has been accepted and deployed by federal and state agencies, as well as entire court systems. For example the Dade County Court uses CIC's signature technology to electronically file court documents, and working with Chase Manhattan Bank, Ginnie Mae uses CIC's electronic signature capture and verification for electronic submission and processing of mortgages.

CIC's technology uses the behavioral biometrics of a handwritten signature to verify the identity of the user. This is done by analyzing the shape, speed, and stroke sequence during the act of signing. It is important to note that CIC's technology does not only capture the shape of the signature, but also the biometric data, by capturing the stroke dynamics of the person signing the document. This signature and the data collected are then bound to the signed document. This meets the requirements for ensuring that the electronic signature is "unique to the person using it."

The signature once entered can not be altered or copied. The dynamic stroke data is encrypted and stored as part of the record. This satisfies the condition of "under the sole control of the person using it." CIC relies upon Industry standard encryption technology, including DES.

CIC has also developed a forensic tool, that would allow a handwriting or signature expert to extract enough information from the stroke data to enable them to compare one signature to another electronic signature captured in a similar manner. The utility was developed at the request of the U.S. Department of Justice during the implementation of this technology for Ginnie Mae. The Department of Justice approved both the forensic utilities, and the whole project. The forensic tool called "SigView™" can be purchased as part of the InkTools® Development Kit from CIC. Thus, meeting the standard of "capable of verification."

CIC's Sign-It® is fully integrated within the Adobe Acrobat 4.0, 5.0 architecture. This architecture ensures that the "tamper evident" condition is satisfied by invalidating the signature if the document is altered. If any data in the document is altered after the person signs it, Acrobat will keep a permanent record of the tampering, and provide a clear audit trail. Furthermore, Acrobat supports a "roll-back" option that allows someone to view any alteration in the document step by step. Adobe protects the integrity of the document using the Secure Hash Algorithm (SHA) as well as strong encryption. This feature meets the requirement of "linked to data in such a manner that if the data are changed the digital or electronic signature is invalidated."

Satisfying the above requirements address the definition of the electronic signature, but adhering to the electronic process is vital. It is only when both of these criteria are met that the signer can be assured that they are indeed entering into a secure contract. The collection of biometric data of the signatory, the dynamic characteristics such as pen velocity, acceleration, and stroke sequence, as well as the image of the signature creates a highly secure means of confirming the user's identity and ensuring against signature forgeries. The integration of CIC's signature technology into Adobe Acrobat 4.0, 5.0 assures that a user will

be informed of any tampering done to the data or the signature on the document. Binding the signature to the document using the NIST standard Secure Hash Algorithm (SHA) prevents the person's signature from being electronically validated if somehow copied into any other document for the purpose of abusing a person's authority. All of these capabilities are important to ensure the electronic validation of a signature throughout the electronic process of a document.

CIC's Sign-It product family provides the user with signature capture, document binding, and signature verification. This product is fully integrated plug-in for Adobe Acrobat 4.0, 5.0 It captures an electronic signature from a digitizer, touch screen or PDA and binds it with an Adobe Acrobat document. The signature is encrypted with the PDF document using standard DES encryption, a hash of the document content is done using SHA1 and the message digest from the hash is then encrypted.

This document is meant to provide a brief summary of the enacted and pending legislation related to electronic signatures, and to address how certain aspects of CIC's technology fit into the broad developing framework of electronic signature law. This summary only addresses enacted and pending legislation of which CIC is currently aware, and is not necessarily complete or comprehensive regarding electronic signatures or related subjects. CIC does not provide legal interpretations or advice and directs you to your legal counsel to assess the potential impact that such legislation may have upon you and to determine if there is other legislation enacted or pending which may effect you. Additional information may also be obtained at www.bakerinfo.com/ecommerce, a site maintained by the law firm Baker & McKenzie.