

## **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](http://www.bakerinfo.com/ecommerce), a site maintained by the law firm Baker & McKenzie.