

**Any method.
Any popular format.**

**The key to paperless
business processes.**



Sign-it® for Word

Multi-Modal Input for Electronic Signatures with Microsoft® Word Documents

Sign-it is a software application designed to give Microsoft Word users the ability to embed legally compliant electronic signatures in documents. The binding and analysis features of Sign-it allow the document recipient to check the document for modifications and ensure secure document management.

When an electronic signature is captured using Sign-it the signature is bound to the document using a cryptographic hashing algorithm. The algorithm used within Sign-it is based on the National Institute of Standards and Technology (NIST) approved Secure Hashing Algorithm (SHA-1). This algorithm is used to create a one time key based on the data in the document, the signatory information and the signature itself.

The signature information and hashing key are also encrypted using the Triple DES 128bit encryption algorithm to prevent tampering. As a result of this process, a signature can only be validated within the original document it was bound to.

Signature Methods

A signature can be added on-the-spot or a signature field can be pre-created for the signer to sign later.

- Live Signature – A handwritten signature of the signer
- Voice Recording – A recording of the signer's intent and approval of signing
- *Signature Stamp – A handwritten signature stamp of the signer released from a SignatureOne Profile Server with a password

Contents

- Signature Methods
- Sectional Signing
- Digital ID
- eSeal
- eKey
- Validation
- SignatureOne® Profile Server



Setup Requirements

- Microsoft® Word 2003 SP3 or 2007 SP1
- Windows® 2000 SP4, XP SP2, or Vista®

Optional

- A pen input device for signature capture
- Windows setup for microphone and speakers for voice signing
- SignatureOne Profile Server setup for signature verification, stamps, and passwords
- SafeNet iKey™ 2032 for eSeal or Digital ID storage
- Third-party Digital IDs (.PFX or .P12)

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 AIG, Charles Schwab, Prudential, Nationwide (UK) and Wells Fargo chose CIC's products to meet their needs. CIC is headquartered in Redwood Shores and its products are sold and supported globally.

Contact:

1-650-802-7888

sales@cic.com

www.cic.com

Cont'd

- *Verified Signature – A handwritten signature of the signer verified against the signer's signature template on a SignatureOne Profile Server
- *Password – An approval from the signer with a password verified against the signer's template on a SignatureOne Profile Server
- Click2Sign – An acknowledgement and agreement of signing from the signer with a click of the mouse

* Requires SignatureOne Profile Server

Sectional Signing

A signature can be set up to approve sections of a form or document. This signature will be invalidated if any of the associated sections are modified.

Digital ID

A Digital ID (also known as a digital certificate) is a form of electronic credentials for the Internet. Similar to a driver's license, employee ID card, or business license, a Digital ID is issued by a trusted third party to establish the identity of the ID holder. The third party who issues certificates is known as a Certification Authority (CA). The purpose of a Digital ID is to reliably link a public/private key pair with its owner. Just as when a government issues you a passport it is officially vouching for the fact that you are who you say you are, when a CA issues you a digital certificate it is putting its name behind the statement that you are the rightful owner of your public/private key pair. For more information on Digital ID's, visit the VeriSign® website.

Sign-it uses the Digital ID to encrypt or digitally sign the signature data. Only valid certificates at the time of signing are allowed to be used with Sign-it for encryption. No attempt is made to validate the signer's identity or check the revocation status of the certificate.

eSeal

An eSeal is an electronic image of a company logo, a company seal, or a personal seal. Sign-it allows you to attach one to a signature block. File formats supported are JPEG, TIF, BMP, GIF and PNG.

eKey

An eKey is a USB Authentication Token, also known as a hardware USB security token. It plugs directly into the USB port and is used in public key infrastructure (PKI) environments for secure log-on, email and web access, and file encryption. Sign-it currently supports the iKey™ 2032 from SafeNet, Inc. Sign-it allows you to access the Digital ID or eSeal that are available on the eKeys.

Validation

Only signatures that can be validated are considered viable electronic signatures. Validating signatures provide a check to insure that the document and signatures have not been altered.

SignatureOne Profile Server

SignatureOne Profile Server is a separate product from CIC which hosts signature templates used to verify signatures or passwords against user information prior to releasing a signature or signature stamp onto the document.

User profiles and signature templates are required to be created in a controlled environment to insure that user information cannot be altered by other users.

Signature templates can also be exported to a local system for users to insert signature stamps or verify signatures against their templates. These local templates provide the same capabilities for users who do not have connections to the local network, Intranet or Internet.