



WHITE PAPER

Paperless-Signatures® for the Paperless Office

Talk of the paperless office has been around for the past 20 years. While no one expects paper to disappear, new technologies are making it possible to move more and more applications to digital storage and retrieval systems. The benefits are huge: reduced storage space, reduced paper handling, faster document retrieval, faster workflow processing and remote retrieval.

A problem for many applications is the hand-written signature, the primary means of identification and authentication of documents for the past several thousand years. These papers are important to every business and include such things as contracts, purchase orders, non-disclosure agreements, medical records and other legal documents.

This paper looks at how paperless digital documents can be created, using the Cyber SIGN Inc, Enterprise **Paperless-Signature®** hardware and software that have the same impact as today's signed legal papers.

The Cyber SIGN Inc, Enterprise system consists of a signing tablet and software that captures the dynamics of a signature as it is signed. In addition to the shape we normally associate with a signature, the data includes pressure, timing and air-strokes (movement of the pen off the tablet) information*. These signatures can be verified against previously stored signatures (called templates). The dynamic data in these signatures makes forgery almost impossible.

** The term "biometrics" is used to refer to the identification of a person by a physical attribute. In addition to signature, some common biometrics are voice, fingerprint, hand geometry, retinal scan and face recognition.*

Paper Non-Refutable Documents

For a document to be legally enforceable, it must be non-refutable. That is, we must have an assurance that the document is authentic and the signature is genuine. Characteristics include:

- **The signature is genuine.** It is not a forgery or a copy of a previous signature.
- **The signature is deliberate.** The signer intended to sign the document to which it is affixed.
- **The signature is not reusable.** Future documents could not make use of the same signature.
- **The document has integrity.** It has not been tampered with or modified since it was signed.
- **Tampering can be detected.** It would be difficult to tamper with the document and/or signature without being detected.

Your mortgage papers are a good example. These papers represent a contact between you and the bank. To invalidate these papers you would have to prove that the signature is not yours or that the document had been altered after you signed. Should you elect to challenge the document, the bank would retain the services of a document examiner to authenticate your signature and the document.

Digital Non-Refutable Documents

The digital non-refutable document is the electronic equivalent to a signed paper document and must also have the characteristics listed above. Normal computer files such as word processing, spreadsheet, and bitmaps are **not** non-refutable as they can be easily copied, edited or modified. Pasting a signature on them, even the ID-007 signatures, does nothing to alter this situation. It is very easy to copy signatures from one document and paste them to others. To make a digital non-refutable document it is necessary to attach the signature in such a way that the signature is

valid only with the document to which it is associated. This is done by encrypting the signature using a key calculated from the document (there are a number of ways to generate a key).

Using the Enterprise **Paperless-Signature®** in this way does two things. First, it provides a signature that is difficult to forge. Secondly, it provides a signature that cannot be reused.

The resulting documents have all the characteristics of non-refutability previously discussed:

- **The signature is genuine.** The signature contains biometric data that can be used to conclusively connect the signature with the signer. It cannot be a copy, because non-encrypted signatures are not available. A signature from another document cannot be used since it is encrypted with a different key.
- **The signature is deliberate.** Application software can ensure that the document is presented to the signer before a signature is entered.
- **The signature is not reusable.** Encryption of the signature makes this impossible.
- **The document has integrity.** Any changes to the document change the calculated key and invalidate the signature.
- **Tampering can be detected.** Discussed later (see section **Beating the System**).

Digital non-refutable documents have additional traits that are not available from their paper counterparts:

- The biometric **Paperless-Signature®** attached to the document contains information in addition to shape (timing, order, pressure, airostrokes).
- All copies are originals. There is no need to sign multiple documents. The documents can be copied and/or transmitted over the Internet or Intranet.
- Signature verification can be used:
 - During signing to determine that it is the correct person.
 - During signing to determine if the person is authorised to sign.
- Post verification can be used to authenticate the signature.
- The document itself is not modified or encrypted, and can be viewed at any time.
- The procedure will work with any document, regardless of file type or application origin. The only requirement is that the information content of the document be viewable. Eligible files include word processing, spreadsheet and bitmap documents.

There are other issues that may invalidate a document that are beyond the scope of this paper, such as: did the person actually read and/or understand the document; is the document ambiguous; is it in conflict with other non-refutable documents?

Software Development Requirements

Creating a non-refutable document requires that either the Cyber SIGN Inc, Enterprise Paperless Signature software be integrated into the application or a viewing program be developed. However it is done, the program must do the following:

1. Display the document. It must ensure that the entire document is viewed by the user. This may require that the user page or scroll through the document.
2. Present the user with a "Sign your signature" button. This indicates to the computer that the document has been read and the user is ready to sign.
3. Request a signature from the Enterprise **Paperless-Signature®** system. The user is prompted to enter their signature on the special signature capture tablet.
4. The application could verify the signature against a previously stored template (this is optional). It could even verify that the signer is authorised to sign the document. For example, a purchase order program could be written that accepts only certain signatures for POs above \$1000.
5. Calculate the key. One of a number of methods is used to generate a key from the document.

6. Encrypt the signature. The key is applied to the signature.
7. Document and encrypted signature are stored. They can be combined onto one file or stored as two separate documents. The program is not responsible for the storing the original document, but it would be a good idea to make a copy of the file or at least write-protect it. Remember, any changes to this document nullifies the signature.
8. A viewing program is required to authenticate the document. This program re-calculates the document key and uses it to validate the signature. It would also be used to view and print the document.

Beating the System

The concern most often raised about digital non-refutable documents is the possibility that someone could make fraudulent use of signatures. Unencrypted signatures files should never be allowed to exist on the system. This precludes someone attempting to feed a signature to a document.

The most serious breach would be from someone who has knowledge of how the document key was generated. This could allow them to decrypt the signature, modify the document and/or use it on other documents. Preventive solutions include:

1. Have the encryption portion of the program written by a trusted third party who has no interest in the documents created with the system.
2. Use a trusted 3rd party to authenticate and store documents.
3. Even greater security can be provided by implementing a private/public key scheme such as RSA. This allows anyone to have a copy of the document, verify its authenticity and yet make it almost impossible for anyone to decrypt the signature.

Before getting too excited about someone breaching the system, it is important to consider;

1. Cost of a breach.
2. Motivation to breach to the system. Who would gain or lose?
3. Difficulty in breaching the system.
4. Who has the knowledge and access to breach the system?
5. Is the current paper system any more secure than this system?

There is a tendency to make the problem worse than it really is.

Legal Standing

Current laws do not guarantee the legal status of hand-written digital signatures. While they are not illegal, until they are challenged and tested in court, the issue will remain somewhat cloudy. Mathematicians would probably find the digital non-refutable document to be statistically superior to the current paper system. The problem is that the complexities are beyond the average judge, lawyer and jurors. However, laws have been proposed that would recognise hand-written digital signature and most legal experts expect electronic biometric signatures and digital documents to eventually be accepted in the same way that paper documents are today.

Other Uses for Non-Refutable Documents

Forms as non-refutable document

Many applications involve forms that are filled in and signed. Since much of the form is boilerplate and never changes, it would be desirable if only the filled in data and signature are saved as the non-refutable document. The form must be considered as part of the document (if the form changes the field data may not be valid). However, it is only necessary to have one (1) copy. The document key used to encrypt the signature must include both the data and the form. If either changes, the signature will be rejected.

Paper equivalents of a Digital Non-Refutable Documents

It is possible to create a paper version of the digital non-refutable document by adding the signatures biometric data, represented in printable ASCII, to the paper document. The method is actually quite simple. The document could be faxed or copied. Authenticating the document would consist of scanning the document, performing an OCR on the text and biometric signature data, and submitting this data to the viewing program. This requires some care as the OCR'd document would have to exactly match the original. This might require that the document key be calculated based only on text with all white space and other formatting data ignored. As an alternative the entire document could be printed as a 2D bar code, and converted back to digital form by scanning and a conversion program.

Using these methods would be awkward. Sending the document over the Internet would be far superior. One advantage is that it allows someone who does not have a computer to have a paper copy of a document that could, if necessary, be authenticated.

Note:

*There are considerable references to **digital-signatures**® in articles and books about computer security. A digital signature is data that is attached to a electronics message or document to provide authenticity. Note that this has the same purpose as a hand-written signature. However, digital signatures are not necessarily based on hand-written signature. In fact, they are usually based on a private key (password), a public key and a mathematical relationship between the two. The bottom line - the word "**signature**" in the computer world does not necessarily refer to a hand-written signature.*

#####

Cyber-SIGN® biometric signature verification software may be licensed for application and development use from Cyber SIGN Europe, Sophia Antipolis, France. SEAL (Signature Enabled Application Library) – a developer's toolkit, an MS Word Non-Refutable Document application and the needed client/server software is available. For stand-alone desktop use Cyber-SIGN Personal® and a Cyber-SIGN® Screen Save r are offered

For further information contact:-

**Cyber SIGN Europe
AREP Center
1 Traverse des Brucs
06560 Sophia Antipolis
France**

Tel : +33 492 969 611

Fax : +33 492 969 911

Mail : info@eu.cybersign.com

Web : www.cybersign.com