

# Electronic Signature Capture with Biometric Verification



**The CSC Group**

# Electronic Signature Capture with Biometric Verification

## INTRODUCTION

Capturing a signature electronically and verifying its authenticity presents both legal and performance issues that must be resolved if complete electronic flow in today's e-business environments is to be achieved. Whether for an enterprise or consumer application, the electronic signature (E-Signature) solution must be simple to use, secure, meet legal and regulatory requirements, and operate with any system environment. This paper presents the legal definitions of e-signatures – both federal and state – explore different types of electronic signatures and in particular the role biometrics plays in eliminating fraud. Additionally, some key benefits are highlighted as well as applications for use.

## E-SIGNATURE DEFINED

The definition derived from legislation is: *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, capable of verification, under the sole control of the person using it, and linked to data in such a manner that if the data is changed the digital signature or electronic signature is rendered invalid.*

Pen-based signature pads are used to electronically capture a written signature. The technology enables a person to sign electronic document files with a handwritten signature. After signing, the electronic signature is attached to the document in a manner that maintains the document's integrity and permanently binds the signature to it. Each time the document is re-opened, its contents are compared to the original document. If any change is detected, the electronic signature is rendered invalid.

Because the signature is bound to the document permanently, it cannot be transferred into another document or used fraudulently. In addition, the electronic signature includes the date, time and location of the signature along with the reason the document was signed. This confirms a person's consent to and understanding of the responsibility toward the document's contents.

## NOT EVERY TECHNOLOGY CAPTURES SIGNATURE INFORMATION THE SAME WAY

A **digital signature** is an electronic signature that can be used to verify the identity of the sender of a message or the signer of a document, and possibly ensure that the original content of the message or document being sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message,

encrypted or not, so the receiver can be sure of the sender's identity and that the message arrived intact.

However, a digital signature has nothing to do with an actual handwritten signature. Its purpose is for use in encryption systems, called "public key infrastructure" or PKI. Encryption systems assign individuals a pair of public and private "keys". The public key is stored in a central place and used by the sender to encode messages that are sent to the recipient. The private key is stored on the recipient's computer and is used to decode messages. An individual's digital signature normally resides on his or her computer, but it can be stored on a card similar to a banking card. When someone wishes to encrypt an electronic document, they use a password or PIN that in turn allows the digital signature to be used. Although secure once encrypted, digital signatures are only as safe as the medium where they reside. The use of a digital signature does not guarantee the identity of the originator. Anyone obtaining access to the password, PIN or computer where it resides can potentially make unauthorized use of it.

Alternatively, a **dynamic or biometric signature** is based on an individual's unique handwriting characteristics and can be used to confirm a person's identity. E-Signature software that uses biometrics technology for identity verification adheres within certain boundaries that are unique to the individual, called biometric characteristics. A biometric signature is a term used to refer to a handwritten signature that has been recorded/captured using a variety of input devices such as digitizing tablets, personal digital assistants (PDA), computer displays or other contact sensitive technologies. This method allows real handwritten signatures to be incorporated into electronic documents during electronic transactions.

Not every technology captures signature information the same way. Some systems have a static approach and will record an image of a signature without recording the unique behavioral elements associated with the execution of a signature. In a biometric system, both the geometric and dynamic characteristics of the signing *process* will be recorded and incorporated in an electronic document.

Most of the elements that make a signature unique and identifiable can be derived from digital signature data. Furthermore, the data that is incorporated in an electronic document can be used to lock and protect the contents from being altered. The value of biometric signatures is their use in preventing fraud, providing increased security and controlling access to buildings, networks, computers, documents and databases.

# Electronic Signature Capture with Biometric Verification

## E-SIGN LEGISLATION

The Federally enacted **Electronic Signatures in Global National Commerce Act (E-SIGN)** became effective October 1, 2000 and positions E-Signature systems as the standard for signed business documents. The Act defines an electronic signature as *"data in an electronic form, attached to or logically associated with an electronic record, and executed or adopted by a person or agent of a person, with the intent to sign a contract, agreement or record."*<sup>1</sup>

Additionally, many individual states<sup>2</sup> have a **Uniform Electronic Transactions Act (UETA)**, some of which have been in place since 1999. Each state's UETA is similar to E-SIGN in that the same legal acceptance is given to electronically created records and signatures as paper records and ink signatures, but a UETA also outlines parameters for the creation of a valid electronic signature and the maintenance of electronic documents.

*Why both?* UETA validates electronic transactions at the state level. However, not all states have adopted a UETA. Moreover, each state's version varies to some extent from the model statute. E-SIGN was enacted to validate electronic transactions at the national and global level. As a federal law, to ensure national uniformity in the treatment of electronic transactions, E-SIGN closely parallels UETA's model statute and provides expressly that it (1) preempts both a state's version of UETA to the extent it is inconsistent with E-SIGN, and (2) other inconsistent state law. The laws and regulations may differ, but there are several clear patterns:

- Electronic signatures are legally binding.
- Electronic signatures must be "technology neutral".
- E-SIGN confirms that states must allow the use of electronic signatures if the two parties involved agree to this method of signing. Each state is empowered to legislate its own electric signature requirements, recognizing that to be legally binding it must be:
  - Unique to the person using it
  - Capable of verification
  - Under the sole control of the person using it
  - Linked to data in such a way that if the data is changed, the signature is rendered invalid.

## USING BIOMETRICS FOR IDENTITY VERIFICATION

Handwriting still remains one of the most powerful human identifiers today. Handwriting characteristics are absolutely

unique to an individual and virtually impossible to duplicate, making fraud essentially impossible. A signature has at least three attributes: form, variation, and movement. Since moving a pen on paper produces the signature, this movement is perhaps the most important part of a signature because it is based on the person's unique muscular dexterity (aka "muscle memory"). Once a person is used to signing his or her signature, the brain without any particular attention to detail, controls these nerve impulses.

Biometrics technology<sup>3</sup> is software that supports virtually any form of pen-enabled device on which a signature is written. During the act of signing a signature is captured, 250 biometric measurement points are analyzed, and in less than a minute a person's identity can be verified. Measurements analyzed during the act of signing include timing elements (speed, acceleration), sequential stroke patterns (in which direction was the "t" crossed, did the "i" get dotted at the very end), and off-table motion. The signature and data collected are then bound to the single document – meeting the legal requirement that an electronic signature is *"unique to the person using it"*. Once captured, the signature cannot be copied or altered. The data is encrypted and stored as part of the record. The signature and encrypted data are then bound to the single document. If the document or data is tampered with, the electronic signature is rendered invalid. The resulting accuracy is comparable to and less intrusive than other types of identification.

For the layperson, a graphical picture of a handwritten signature can be convincingly imitated. However, when questions of fraud arise as to whether or not the signature on a document is genuine, time-consuming expert forensic examination may be required. Biometric signatures can be authenticated in real-time or after the fact. In the event that a biometric signature is contested, the signature data can be extracted from the document and submitted for similar forensic analysis to verify the authenticity of the signature. The additional behavioral features recorded from biometric signatures make them even more difficult if not impossible to imitate.

Biometric signatures represent an ideal bridge between the long-recognized practice of signing a document ("wet ink" signature) and the need for electronic documents to be uniquely recognized by individuals. Applying biometrics technology to electronic signatures can help eliminate fraud, providing individuals with enhanced security and control over the documents and transactions that are originated, transacted and stored in today's e-business environments.

<sup>1</sup> S.761 Electronic Records and Signatures in Global and National Commerce Act (E-SIGN)

<sup>2</sup> As of December 4 2002, 41 states have enacted a UETA.

<sup>3</sup> Communication Intelligence Corporation.

# Electronic Signature Capture with Biometric Verification

## MULTI-PLATFORM TECHNOLOGY

Toolkits for MS Windows and Java allow applications to be developed and/or integrated to existing systems on any platform that will support Windows or Java programs.

The value of multi-platform scalability is critical to cost effective ROI. Integrating compatible software into an enterprise-wide solution is very costly and often forces companies to adopt a plan that has more to do with managing the integration than deploying the technology. Open architecture allows organizations to build on their existing enterprise value, rather than replace it.

## KEY BENEFITS

**Instant Access to Information.** Today's business world needs instant access to information. Electronic signature capture allows that same instant access to legal, robust signed documents, contracts, and receipts. Electronically signed documents eliminate duplication costs, multi-part forms, workflow inefficiencies and unnecessary storage. In organizations that process a lot of signed paper contracts and forms, electronic signatures can significantly reduce overhead costs. Electronic signatures can also be authored practically anywhere for many kinds of applications: applying for a job, signing in at the doctor's office, enrolling in an office insurance plan, even signing a traffic ticket.

**Significant Reduction in Expense.** The key incentive driving corporate and government 'buy' decisions is not just security, but also the significant reduction in expense attributed to automating electronic documents.

According to The Wall Street Journal<sup>4</sup>, the financial services industry – banks, insurance, and brokers – has been an early adaptor of biometric e-signature technology, realizing significant cost savings:

- Chase Manhattan Bank and Ginnie Mae capture and verify electronic submission and processing of mortgages.
- Prudential USA reported its deployment to 6,000 of their insurance field agents using laptops allowed automating multiple signature enrollment processes for new insurance applications with a two-thirds reduction in processing time, 60 minutes down to 20 minutes, and a 93% acceptance among users.

- Another large insurance company saved \$30 million on a million and a half contracts over 1½ years. An insurance contract will have an average of three signatures that have to be collected from a customer as well as other approvals throughout the company. The average cost of \$32 per form was reduced to under \$2.
- A county court in Florida uses biometric e-signatures to electronically file court documents.

## Speeds Up Business Processes and Improves Productivity.

When used as part of an electronic document management system, E-Signature can speed up business processes and improve productivity by having executed documents and contracts readily available for viewing across networks or across the internet.

**Satisfies E-Privacy Issues.** Handwritten technology also addresses e-signature privacy issues. By using a signature capture pad, people can still sign in a manner they are most accustomed to – with a pen – and automatically establish intent to sign. Because a signature may be changed at will, the individual must ultimately maintain control over its use. Other electronic signature systems, such as password or digital keys, can make changes to an e-signature difficult.

## APPLICATIONS<sup>5</sup>

**Insurance.** Automate contracts, forms and enrollment.

**Loan Escrow & Leasing Services.** Simultaneously complete paper contracts and their electronic counterpart. Use electronic document management for instant paperless storage, transmittal, retrieval and viewing.

**Banks / Credit Union Signature Cards.** Visual or automatic verification. Capture original signatures in the new accounts department and verify them at the teller window instantly.

**Medical Facilities.** Automate patient check-ins, notice of privacy practice, consent forms, ABNs, scripts, and EMRs.

**Pharmacies.** Automate the prescription process end-to-end including fraud detection, customer pick-up and consultation acceptance or denial.

**Human Resources.** Capture applications and records, insurance enrollments and other authorizations.

**Retail Stores.** Electronic filing and retrieval of credit card receipts for bill-back protection and to eliminate fraud.

**Government Agencies** (such as Motor Vehicles) to automate ID cards, badges, etc.

**Web-Enabled Viewing.** Provide Internet access anytime, anywhere to standard signature-ready contracts and forms.

<sup>4</sup> *The Wall Street Transcript*. Interview with Guido DiGregorio, Chairman, President and CEO, Communication Intelligence Corp. July 1, 2002

<sup>5</sup> Electronic Digital Signature Capture Examples, Topaz Systems Inc. <http://www.topazsystems.com/Software/faq.htm#SA>

# Electronic Signature Capture with Biometric Verification

## SUMMARY

1. Electronic Signature Capture is 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, capable of verification, under the sole control of the person using it, and linked to data in such a manner that if the data is changed the signature will be rendered invalid. Technology enables a person to sign electronic document files with a handwritten signature and then have it bound to the document, as expressed intent to sign.
2. Pen-based signature pads are used to electronically capture written signatures. After signing, the electronic signature is attached to the document in a way that maintains the document's integrity and permanently binds the signature to it. Each time the document is re-opened, its contents are compared to the original document. If any change is detected, the electronic signature is rendered invalid. Because the electronic signature is bound to the document permanently, it cannot be transferred into another document or used fraudulently.
3. E-SIGN defines an electronic signature as *"data in an electronic form, attached to or logically associated with an electronic record, and executed or adopted by a person or agent of a person, with the intent to sign a contract, agreement or record."* E-SIGN was enacted to validate electronic transactions at the national and global level. UETA validates electronic transactions at the state level. Not all states have enacted UETA.
4. Applying biometrics technology to electronic signatures can help eliminate fraud, providing individuals with an increased level of security and protection. Biometric signatures can also be used to provide and control access security to buildings, networks, computers, documents and databases.
5. Toolkits for MS Windows and Java allow applications to be developed and/or integrated to existing systems on any platform that supports Windows or Java programs.
6. The key benefits to using electronic signatures today include a) instant access to information, b) significant expense reduction, c) faster business processes and improved productivity, d) satisfies privacy issues.
7. There are applications where electronic signatures can be used including insurance and financial services, signature cards in banks and credit unions, for web-enabled viewing of documents, in medical facilities, pharmacies, human resources, retail and government agencies.

## RESOURCES

1. Digital Signature Guidelines, American Bar Assn., available on line, <http://www.abanet.org/scitech/ec/isc/dsgfree.html>
2. CIC® (Communication Intelligence Corp). OEM partnership 2003. Various papers as reference.
3. Electronic Digital Signature Capture, examples. Topaz Systems Inc., as published on line, <http://www.topazsystems.com/Software/faq.htm#SA>
4. Global E-Commerce Law. *Electronic and Digital Signature Resources* available on line. Baker and McKenzie Global E-Commerce Law, <http://www.bmck.com/ecommerce/uetacomp.htm>.
5. S.761 Electronic Records and Signatures in Global and National Commerce Act (E-SIGN) Oct. 1, 2000
6. The Wall Street Journal, interview of Communication Intelligence Corporation. Company. July 1, 2002
7. 2002 UETA and Electronic Signatures Legislation. National Conference of State Legislatures. June 6, 2002
8. Uniform Electronic Transactions Act of 1999 State-By-State Comparison Table. ITEC Law Alert, McBride Baker & Coles, <http://www.mbc.com/ecommerce.html>

Note: The CSC Group recommends that each organization determine suitability of the technology presented herein to determine compliance with its own internal security and privacy controls.