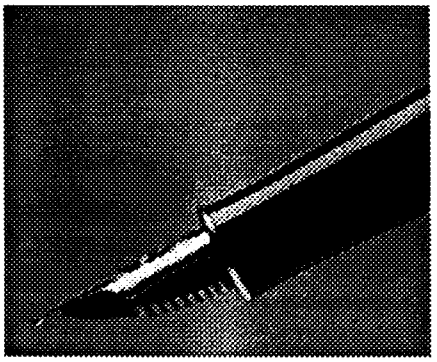
Understanding Signature Verification



Signature verification is the process used to recognize an individual's hand-written signature.

Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer user. This is done by analyzing the shape, speed, stroke, pen pressure and timing information during the act of signing. Natural and intuitive, the technology is easy to explain and trust.

As a replacement for a password or a PIN number, dynamic signature verification is a biometric technology that is used to positively identify a person from their handwritten signature.

There is an important distinction between simple signature comparisons and dynamic signature verification. Both can be computerized, but a simple comparison only takes into account what the signature looks like. Dynamic signature verification takes into account how the signature was made. With dynamic signature verification it is not the shape or look of the signature that is meaningful, it is the changes in speed, pressure and timing that occur during the act of signing. Only the original signer can recreate the changes in timing and X, Y, and Z (pressure).

A pasted bitmap, a copy machine or an expert forger may be able to duplicate what a signature looks like, but it is virtually impossible to duplicate the timing changes in X, Y and Z (pressure). The practiced and natural motion of the original signer would required to repeat the patterns shown.

There will always be slight variations in a person's handwritten signature, but the consistency created by natural motion and practice over time creates a recognizable pattern that makes the handwritten signature a natural for biometric identification.

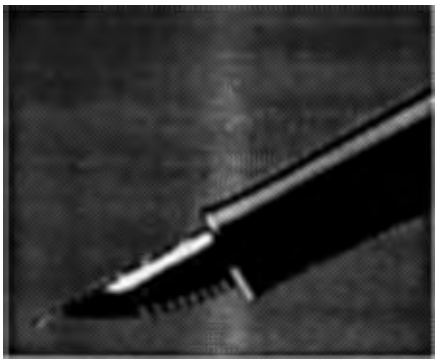
Signature verification is natural and intuitive. The technology is easy to explain and trust. The primary advantage that signature verification systems have over other types of biometric technologies is that signatures are already accepted as the common method of identity verification. This history of trust means that people are very willing to accept a signature based verification system.

Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer user. Unlike the older technologies of passwords and keycards - which are often shared or easily forgotten, lost, and stolen - dynamic signature verification provides a simple and natural method for increased computer security and trusted document authorization.

back

Showcases
Fingerprint
Iris Recognition
Hand & Finger
Facial Recognition
Voice/Speaker
Consultants
Smart Cards/Multimodal
Signature/Keystroke
2D Bar Codes

The Distinction Between Biometric and Digital Signatures



Handwriting has been around since the beginning of civilization and the 'signature 'or the act of sign-ing a document,has long been accepted by nearly every culture as one 's recognition and agreement on the contents and implications of written words.

The increasing recognition of electronic signatures by lawmakers is bringing to the forefront concerns over electronic security for privacy and protection of individuals.

For many now conducting business transactions over private networks or the Internet,some form of offcial acknowledgement is now essential and legally binding.The security implications of producing or recognizing 'original 'electronic documents will be more important than ever before.In this respect, it is important to understand the distinction between the terms "Biometric " and "Digital " signatures.

A digital signature is a term used to describe a long numerical code that has been uniquely assigned to one person,hence the reference to 'signature '.It has nothing to do with a real signature.Their purpose is to be used in encryption systems.Asymmetric encryption (or PKI)is an example of a popular encryption approach.A digital signature is issued to an individual by what is called a Certificate Authority.This is a group or organization responsible for maintenance and safekeeping of digital signatures.Because of their length no one actually remembers or even knows their digital signature.

An individual 's digital signature will normally reside on his or her computer,or can be stored on a card (similar to banking cards).When someone wishes to encrypt an electronic document,they will 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.Anyone obtaining access to your password,PIN or computer can potentially make unauthorized use of your digital signature.The use of a digital signature does not guarantee the identity of the originator. Handwriting results from a highly complex series of dynamic neuromuscular tasks from brain to fingertips.A naturally developed signature represents the most often reproduced and habitual act of writing.

Although we never sign exactly the same way twice,the signature adheres within certain boundaries unique to each individual.This natural variation is an essential component of handwriting.It also means that each signature is unique in that no two will be identical in all discrete features.Unlike fingerprints,retinal or DNA patterns which remain constant over time,the execution of a person 's signature will be unique and individual at that particular moment.Handwriting remains one of the most powerful human identifiers that exist today.Identical twins will have the same DNA pattern while their

Showcases
Fingerprint
Iris Recognition
Hand & Finger
Facial Recognition
Voice/Speaker
Consultants
Smart Cards/Multimodal
Signature/Keystroke
2D Bar Codes

handwriting and signatures remain distinctively different.

Biometric signature is a term used to refer to a 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 e-documents during electronic transactions.Not every technology captures signature information the same way.Some systems have a static approach and will only record an image of a signature and as such do not record the unique behavioral elements associated with the execution of a signature.In a biometric system such as CIC 's SignItÔ,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 the digital signature data.Furthermore,the data that is incorporated in an electronic document can be used to lock and protect the contents from alteration.Biometric signatures can also be used to provide and control access security to buildings,networks,computers,documents and databases.

For the layperson,the pictorial appearance of a conventional signature can be convincingly imitated. Forensically,when there is a question of whether or not the signature on a document is genuine, expert visual and microscopic examination is required.This involves evaluating and comparing the general and discrete features of the contested signature with known signatures.With biometric signatures,the authentication can be done 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 to similar forensic investigation and analysis to verify the authenticity of the signature.

In fact, some of the biometric data that is captured such as speed,acceleration,deceleration,and the amount of time the pen is on and off the paper is accurately measured.This data is either unavailable or qualitatively assessed at best in conventional forensic examinations of signatures.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 convention of signing a document and the need for electronic documents to be uniquely recognized by individuals.This application provides individuals with security and control on documents originated,transacted and stored in the digital domain.

by:Marc Gaudreau,Manager, Forensic Sciences Division, Laboratory and Scientific Services Directorate, Canada Customs and Revenue Agency www.cic.com

back

authentication using fingerprints. The solutions replace keys, PINs and passwords in three areas: IT security, physical access and embedded solutions.

Targus
Targus offers two of the most popular Biometrics devices on the market today: The DEFCON Authenticator with USB Hub and the DEFCON Authenticator PC Card Fingerprint Reader.