

The Distinction Between Biometric and Digital Signatures

Handwriting has been around since the beginning of civilization and the 'signature' or the act of signing 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 official 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 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 digitising 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 Sign-it](#), 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*