Electronic versus Digital Signing

Discussing the Differences between Electronic and Digital Signing

Let's start by discussing the term electronic signing. In general, electronic signing covers a very broad spectrum of applicability. Electronic signing is a generic function that can be accomplished in various forms such as:

- A click-wrap acknowledgement of terms and conditions;
- Applying your written signature on a phone or tablet;
- Pasting a facsimile of your signature into an electronic document; or even by
- Applying a signature by using a generic digital certificate.

The most important thing to note is that **electronic signing** does not require any type of validation of the signer's identity, which means that it is a good means of collecting an acknowledgement of something, as long as there is no real need to ensure that the signer is actually the individual who they say they are.

Now let's discuss the term **digital signing.** There are five key concepts that convey the real strength of digital signing:

Number One: Digital signing requires the use of a digital certificate that utilizes a signing algorithm to create a unique electronic fingerprint that can be validated during and following the digital signing process. A digital certificate is a specific type of file that is stored in your browser or on hardware, such as a token or smart card.

Number Two: The digital certificate that is used for digital signing must be an identity-based certificate. This means that the digital certificate is issued to only one individual, for whom his or her personal identity has been independently confirmed through verification of that individual's personally identifying information. Think of it this way: an identity-based digital certificate is a credential that is similar to a driver's license or passport and the process of applying for these credentials is very similar.

Number Three: When a digital signature is created using an identity-based certificate, the "signature" will contain various auditable attributes, such as the name of the signer, date and time stamp, the unique digital fingerprint and the details of the certificate used to create the signature. Optional attributes can be incorporated into the signature, such as a facsimile of the signer's wet signature, a company logo or an electronic professional or agency seal.

Number Four: When using tools such as Adobe for digital signing, the digital signature that has been created using an identity-based certificate can be validated each time the document is opened. If multiple digital signatures are applied to the same document, each signature is validated independently when the document is accessed.

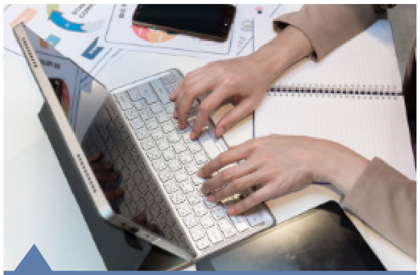
Number Five: Digital signatures that are created with an identity-based certificate are non-repudiable. This means that, from a legal perspective, based on policies that govern digital signing, the signature is recognized as belonging to the individual to whom the certificate is associated.

To summarize, the term **electronic signing** is a generic term that covers various processes, using electronic technology to acknowledge or enter into an agreement of some sort. Depending on the type of electronic signing that is deployed, the signature may or may not be construed as legally binding and it does not create non-repudiation.

Digital signing is based on the use of a digital certificate that has been issued to a vetted individual. Digital signing also creates a unique fingerprint and an auditable digital signature that is non-repudiable and legally binding.

Electronic Signing

- A functional term
- Not technically bound to a specific individual or validation process
- Created options such as typed names, scanned images or a “click wrap” agreement on a web site
- Legal, but not easily audited and can be repudiated
- Cannot be validated through electronic means



Digital Signing

- A legal term
- Tied to a specific individual via a PKI-based digital certificate
- Created using a digital algorithm to bind the document using a certificate, resulting in a unique “fingerprint”
- Non-repudiable and auditable
- A “hash” of the content being signed – any tampering will be evident
- Digital signing is required when using an electronic seal

Understanding the key concepts associated with electronic and digital signing is important as you evaluate your business needs and in assessing your deployment options. IdenTrust offers identity-based certificates that are used in the government, financial, health and public sectors. Our certificates can be used with Adobe® and Microsoft® products that support digital signing.

If you have questions about IdenTrust or our products, please feel free to contact us at **Sales@IdenTrust.com.**