

The Real Difference Between Electronic Signatures and Digital Signatures

August 2, 2016 By [John Harris](#)

Whether the paperless office has actually arrived is debatable, but there's no question that almost every business today is at least leaning towards the digital direction. For many companies across the industry spectrum that includes changing the way their staff – and their clients – sign contracts, forms and other documents.

As to *how* companies implement the change to e-signed documents, well, the similarities stop there.

There are different types of electronic signature technologies available to do the job. Though the e-signature language may sound the same – “digital signature,”

“electronic signature,” etc. – they may be marketed in a similar way by various vendors. However, it's important to know that they're not all the same. In fact, the *real* difference between an electronic signature and a digital signature could make the difference in effective compliance, security and customer trust.

The great e-signature divide

To understand the differences between electronic signatures and digital signatures, you must first understand that a digital signature is a very specific *type* of electronic signature, which in turn is a broader term encompassing simple click-to-sign signatures as well as any other method of signifying one's approval via electronic means. Electronic signatures are generally captured with the click of a mouse or a surface-level tracing of your name.

A digital signature is a highly sophisticated type of electronic signature that encrypts documents using public key infrastructure, permanently embedding all signature information into the document. [Public key infrastructure](#), the protocol that provides public-key encryption, allows users and computers to securely exchange data and verify the other party's identification.

One way to compare a digital signature with an electronic signature is to imagine them on a balance scale. They both offer signing capabilities through technology, but the levels of security and integrity make the digital signature a much weightier option.

Why?

Digital signatures can prove the integrity of both the signature and the document. When a document is signed digitally, a unique identity credential, the digital certificate, is permanently embedded into the document. This ensures that if the document is changed or tampered with, it can be proven, in addition to accurately identifying the signer and time of signature.

Digital signatures can also produce a comprehensive audit trail that tracks and records every action of the digital signing process. This includes the initial creation of the transaction, the user's method of authentication, when documents were sent and signed by each party and more. This ensures the utmost level of security surrounding a document and the undeniable ability to prove its integrity.

The real difference? Independence

The heart of what defines a true digital signature is independence.

Digital signatures adhere to strict, published international and industry standards and are more widely accepted globally than electronic signatures. Digital signatures are legally-binding and can be **verified independently**—without any reliance on the vendor. Because you have permanent ownership and control of the legal evidence, whether you still have a relationship with your e-signature vendor is irrelevant. Your signatures can be proven valid for years to come. This is critical in certain industries, such as healthcare, real estate and financial services, as signatures must often be legally verified decades after being signed.

Basic electronic signatures are not regulated by universal standards, nor can they be verified independently. Many basic e-signature vendors link signatures to a server, rather than embedding it in the document itself. To verify a basic electronic signature, you must rely on your e-signature vendor to prove a document's legitimacy, which can be a complicated and unreliable process. Digital signature technology ensures that signatures and their legal evidence will travel with the document for its entire life.

A good test to determine if your company should adopt digital signatures instead of electronic signatures is to ask yourself, "If my electronic signature vendor disappeared, could I prove a document's validity on my own?" If there's any hesitation in your response, then digital signatures are your answer.



John Harris

CTO at SIGNiX

John Harris is the Chief Technology Officer at SIGNiX, a Chattanooga-based digital signature solutions provider that makes signing documents online safe, secure, and legal for any business. SIGNiX offers the only independently verifiable, cloud-based digital signature solution, which combines workflow convenience with superior security. Learn more about what makes SIGNiX different at www.signix.com



THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com