Digital Signature vs Electronic Signature - What's the big difference?

The Electronic Signatures in Global and National Commerce Act (E-SIGN) officially gave electronic signatures the same legal standing as handwritten pen and paper ones. That much is clear. What isn't is what solutions on the market today will actually allow people to duplicate a legally enforceable contract, let alone electronically sign documents using a more efficient process than they would with pen and paper.

Organizations have become increasingly confused about their options in the wake of U.S. Congress adopting the Act, and the terminology itself is partly to blame. Buzz words like PKI, digital signature and electronic signatures, to name a few, have all been used interchangeably, whereas the technologies inherent to each are actually sub-sets of one another, not their equivalent.

In addition, concerns with security issues have helped promulgate the widespread misconception that all authentication technologies meet e-signing expectations and duplicate a real-world approval process, whereas in truth, they don't. Ultimately, the question comes down to what users expect of an e-signing solution and what the courts will accept as legal evidence.

A Traditional Signing Process

A paper-based signing process typically begins in the electronic world, by creating a document in the most appropriate software application – Word is ideal for straight text like legal contracts, Excel works for budgets, form packages like FormFlow handles sectional forms as in an application or claim, and XHTML is used for Web forms. Then they print the document to paper and apply their signatures.

It seems simple enough, but the meaning behind that signature is quite significant. That signature illustrates consent and identifies the signer. The ink permanently binds the signature to the paper so that it's virtually impossible to remove it. These factors are the foundation of the legal requirements for signing; in other words, in a court of law, that signature makes for a legally enforceable contract.

But most business processes require much more than a single signature. If only it were that easy. More often than not, however, people are asked to fill in their name, add the date, and the city they've signed in. Even more complicated are the times that a document needs to be sent to other signatories for additional signature approvals. In the cases of sectional forms, as in an insurance claim or mortgage application, it gets particularly tricky as each person has to add information into their respective section, and then sign.

With these kinds of complex signing processes at work in most organizations today, it's no wonder that making the shift from paper to electronic methods comes up against some roadblocks. It doesn't help matters either that what people expect, and what they actually get, from various products on the market often differ as drastically as the signing processes they're trying to move on-line in the first place.

Digital Signatures

Take digital signatures. While the term certainly lends the impression that it produces an electronic version of your handwritten signature, digital signature technology is actually the core technology used by many authentication solutions, PKI among them.

On its own, digital signature technology doesn't come anywhere near emulating a legally binding signing act, not to mention a real-world approval process. Rather, digital signatures encrypt data (represented by a series of numbers), identify who did the encryption, and then validate and detect whether changes have been made. Contrary to what most people expect, a digital signature alone doesn't display an image of your signature or a mark to illustrate your consent regarding a document, nor is it part of the document at all. Instead, the digital signature is often linked to a document by a database application that a company typically creates to store it.

And it gets more complicated: should you wish to reproduce a signing process requiring three signatures in a sectional form with digital signature technology, you'd have to store three separate documents containing the three different data with their corresponding signatures. Talk about re-engineering the process you're used to on paper. You might as well stick to pen and paper.

Electronic Signatures

Digital signature technology requires that a software application be developed to produce a real-world signing process. That said, digital signature technology is a sub-set of electronic signature technology which has greater functionality and comes closer to emulating the "sign on the dotted line" tradition.

Digital signature technology still does what it does best when someone signs with an electronic signature: encrypts the data and detects if changes have been made. Meanwhile, electronic signatures produce what digital signature technology stops short of: it actually displays an image of your handwritten signature or a visual mark within the document to illustrate your consent towards a document's contents and uniquely identify you as a signer. In addition, it's permanently attached to a document – just like our handwritten, pen-inked signature would be in a traditional, paper-based signing act.

Sounds perfect, doesn't it? Not only do you get the visual demonstration of your signature and consent, but you also get digital signature technology that verifies signed data and detects changes. And, on top of it, it meets the legal requirements of signing.

Unfortunately, though, electronic signatures only really work for documents requiring a single signature. Unlike a paper-based model, where the second signer in an approval chain can make authorized changes to a document and take responsibility for the changes, or add information to his respective section of a document without invalidating the process, electronic signature technology would invalidate the first signature. That's because the technology doesn't recognize the content of signed data and is programmed to detect any all 'changes' made to the document by subsequent signers.

Use electronic signature technology alone to reproduce a multiple signature, sectional signing process and you'll have to start the signing process all over again and recreate the document form from scratch if you don't want each signature to appear twice. This is when the heightened security provided by electronic signature technology falls short of its promise.

Electronic Approval Management

There is hope, however. Just as digital signature technology is a subset of electronic signature technology, electronic signature technology is a subset of its own accord, this time, of electronic approval management technology. Electronic approval technology is a solution that duplicates the same process you'd follow in a traditional, business process.

Electronic approval management solutions have appropriated the nuances of real-world approval processes as closely as possible. It duplicates a legally binding signing process by visibly displaying our signature and demonstrating your consent towards a document's content, and allows separate people in an approval chain to add information to their respective sections and signing their names just like they would on paper. All this without invalidating the previously applied signatures.

Electronic approval management solutions recognize content and intelligently authenticate what each person has signed and is responsible for. This allows multiple signatures to be added to a document, additions and modifications to be made, and the same kind of signing flexibility you'd find with paper. And for heightened security, should someone tamper accidentally or maliciously with a document or attempted fraudulent use of the signatures contained therein, it visibly invalidates the electronic signatures.

Electronic Process Signature™

An Electronic Process Signature is a new form of electronic signature technology developed by Silanis for Web-based transactions and electronic document automation. It captures and stores the entire Web sequence of events and content involved in a transaction including the review, signing, acceptance and delivery of documents. The resulting stored Electronic Evidence is linked to the final transaction documents that have signed and/or delivered by an electronic document automation system. The Electronic Evidence can then be used to reliably and accurately reproduce the transaction exactly as it occurred and demonstrate compliance in legal, regulatory or internal proceedings.

The Electronic Process Signature technology can be used with any form of electronic signature in a Web-based application to create its Electronic Evidence. This includes Zero-client click-through, holographic signature capture devices, and digital certificates and credentials.