



Digital Signatures — Coming soon to a Document near You

How do Digital Signatures fit into your workflow — as a technology, as a solution, and as a set of requirements?

By Ramel Levin

Thinking of all the stacks of papers with wet signatures makes a tree-hugger weep. Companies invested six-figure budgets into automating their business process and workflows, yet find themselves still printing papers for a wet signature. Name any sector or vertical market, and you will find projects that are held up for days while documents are mailed between offices, partners, suppliers, or customers for appropriate signatures.

Tree-huggers have a shared interest with compliance officers who are concerned with how to assure the integrity and accountability of electronic documents and records; COOs who find their company's business processes slowed down due to the approval processes; CFOs looking for ways to cut costs associated with paper handling as well as the IT's growing concerns for information assurance.

Digital signatures are here to stop those tears.

What Are Digital Signatures?

Digital signatures seal an electronic document in a way that it cannot be changed. In other words, they guarantee the integrity of the document and the authenticity of the

signer. Any changes made to the document after it is signed invalidate the signature, thereby protecting against tampering with the signed document and against signature forgery.

For centuries, signatures have been the most accepted means of authentication. Roman law recognized a combination of seals and signatures as the primary source for authenticating documents and legal contracts. The 1830s saw the first signs of electronic communications and legally recognized "electronic" signatures with the invention of the telegraph and Morse Code.

However, it was the introduction of public key cryptography by Diffie and Hellman in 1976 that established the first practical method of distributing cryptographic keys over an unprotected public network, paving the way for digital signatures.

Fast forward twenty years to 1999 where the European Commission passed the "EU Directive for Electronic Signatures" and on June 30, 2000, President Clinton signed into law the Electronic Signatures in Global and National Commerce Act ("ESIGN"), which made signed electronic contracts and documents as legally binding as a paper-based contract.

The Business Case for Digital Signatures

Business around the world started using digital signatures to replace the transitional pen and paper signatures. Take ClinPhone as an example. ClinPhone is a leading provider of Clinical Technology Services in the Life Sciences industry. The company has moved to a complete paperless signature process across a number of offices in Europe and the U.S., thus considerably **reducing the time-to-approval process** while maintaining compliance with the FDA's **regulatory requirement** for digital signatures. "To obtain an approval on a project required us in the past to fax documents between our branches around the world," says Daljit Cheema, senior vice president of Technology at ClinPhone. "This could take anywhere between three to four weeks to get signatures from all the parties. In contrast, today the process is completed in ten minutes. Digital signatures paid for themselves just in terms of increased productivity."

"Electronic signatures are becoming more popular as enterprises strive to streamline the approval process and reduce costs associated with paper-handling," says Gregg Kreizman, research director at Gartner.



“Electronic signatures allow enterprises to get rid of the last paper hurdle in their workflow.”

The initial compliance driver in ClinPhone’s case is no coincidence. If electronic documents are not safeguarded, inadvertent or intentional tampering becomes easier in the electronic world than with pen and paper. In 1997, regulators became aware of these concerns and the FDA was the first to issue regulations (Title 21 CFR Part 11) that specifically mandated using electronic signatures on electronic documents.

Other industries and sectors such as healthcare, government, financial, and others added either direct requirements for using electronic signatures or a “technology neutral” requirement for date integrity of an electronic document (i.e. safeguarding electronic documents against unauthorized changes). While the latter can be satisfied with different means, the only standard technology that offers this is digital signatures.

While most companies move from paper-based documents to streamline the approval process and comply with their industry regulations, other motivations to adopt digital signatures are cutting costs associated with paper handling (printing, scanning, faxing, shipping, and archiving), document security, and corporate “going green” initiatives.

How will Digital Signatures Fit in Your ECM and Workflow Solutions?

A wide variety of desktop applications today have built-in support for digital signatures. These applications include Microsoft Word and Excel, Adobe Acrobat (including the freely available Adobe Acrobat Reader), and many others. This built-in support is enabled once a “signing engine” is plugged into the application to provide the digital certificate and keys used for signing. This digital signature support allows a user of a typical ECM system to check-out a document, apply a digital signature, and check it back in. Some ECM vendors took the support for

• • •

Digital signatures seal an electronic document in a way that it cannot be changed. In other words, they guarantee the integrity of the document and the authenticity of the signer.

• • •

digital signatures a step further and integrated digital signature functionality as an integral part of the ECM system. This integration provides the ability to sign files directly from within the ECM system’s front panel (without having to open the file and sign at the application level); a user-indication of where the document is in terms of signature process is also added to the front panel. The digital signature information might also be part of the metadata for each document for various search criteria.

Digital Signatures Beyond Workflow

While the most visible and significant advantages are seen in workflows, digital signatures benefit ECM and other areas as well.

- **Version Control** – Add the user’s signature to any changes made throughout the document’s lifecycle. With digital signatures, non-repudiation of changes made in documents is no longer an option.
- **Audit Trail** – Digital signatures can be added to any transaction being recorded in the audit trail.
- **Capture** – Add system signing to capture a document (e.g., an incoming fax) or user signing for a capture done by a user (e.g., a user capturing a news clip from a website to be added to the DM).
- **Deliver** – Add system signing to documents that are sent/distributed out of the company (e.g., invoices). Note

that in some cases, due to legal requirements, such an example might actually require a user signing.

- **Record Management** – Sign and seal records that must be retained to assure the record’s integrity.

If your company already migrated to a paperless environment, yet you find yourself printing documents for signing, you will want to join thousands of companies who are already reaping the benefits of digital signatures. Digital signatures can eliminate this last hurdle, expedite the approval process, and workflow system, as well as save on additional costs. ■

Ramel Levin (ramel@arx.com) is the Director of Marketing at ARX (Algorithmic Research, www.arx.com), a company specializing in digital signatures.