Digital Signatures in the Legal Market:
How to Select the Right Solution for Your Firm or Legal Department
Introduction

A shift is taking place in the relationship between the legal market and technology. While law firms, legal departments and legal organizations once viewed technology as an obstacle to getting their work done, today they are realizing that they can- and indeed, must- use technology in order to work efficiently, stay competitive and satisfy client needs.

At the most basic level, the technology being embraced across the industry includes content authoring solutions such as Microsoft Word and PDF, which allow documents to be created and maintained in electronic format. Going a step further, legal organizations are also embracing automation tools for their workflows, cases, and overall business processes. All of these solutions, from the most basic to the most advanced, aim to eliminate the reliance on paper as much as possible while easing access to information. This enables legal professionals to streamline their work processes, enhance their internal and external collaboration, and shorten document turnaround times.

One of the main obstacles many organizations encounter in trying to fully achieve these outcomes is the need for signatures, which arises in most of the document-centric processes lawyers handle on a regular basis. Without the ability to securely sign electronic documents, employees are forced to resort to paper each time a signature is required. This results in wasted staff time, lengthened turnaround times, and increased spending on paper-related resources such as paper, printer ink, postage, courier fees and archiving. Meanwhile, clients are left wondering where they can find legal support that’s more efficient and cost-effective.

Digital signatures solve these problems quickly and efficiently by enabling lawyers and other legal professionals to add secure and compliant signatures to electronic documents in any format, and quickly deliver these documents to any recipient. Bypassing the costly and time-consuming “print-sign-scan” process, they can quickly provide clients with signed electronic records that can be easily validated to ensure signer identity and content integrity.

Digital signature technology has never been more affordable or easy to deploy and manage. In fact, a recent report from AIIM, the Association for Information and Image Management, shows that 81% of organizations that deployed digital signatures reached ROI (return on investment) in less than a year.

In this white paper, you’ll find the information you need in order to properly evaluate your options for implementing a digital signature solution in your firm, in-house legal department or other legal organization. Topics addressed include:

- What are digital signatures and how do they work?
- Challenges and opportunities for digital signatures in the Legal market
- How do I make the business case for digital signatures?
- How do I select the right digital signature solution?
What are digital signatures and how do they work?

The short answer is that digital signatures are the most advanced form of electronic signatures—the most secure, most flexible, and most compliant with laws and regulations both in the United States and internationally. For the longer answer, you need to understand the differences between digital signatures and electronic signatures.

**Electronic signature** is an umbrella term for any technology used to associate a person with the electronic content they are trying to sign. It is defined by [ESIGN](https://en.wikipedia.org/wiki/ESIGN) (the Electronic Signatures in Global and National Commerce Act of 2000) and [UETA](https://en.wikipedia.org/wiki/Uniform_Electronic_Transactions_Act) (the Uniform Electronic Transactions Act) as “an electronic sound, symbol, or process.” Examples include a scanned image of a signature, the “I Accept” checkmark on a website, and a signature captured using an electronic pad at a grocery store. By themselves, most electronic signatures cannot ensure signer identity or content integrity, nor do they eliminate the risk of signers denying that they signed the document.

**Digital signatures**, on the other hand, are the most secure form of electronic signatures. They are based on Public Key Infrastructure (PKI) technology, the only signature standard published, maintained and accepted by governments around the world, including the US, Canada, the European Union and Latin America, as well as by independent bodies such as ISO, OASIS, IETF and W3C. When legal entities explore their options regarding electronic signatures, they typically decide that digital signatures are the best option because of their non-proprietary nature, global acceptance, compliance with local regulations, security assurance, and ability to work with the most commonly used document authoring applications.

Through the use of cryptographic operations, digital signatures create a “fingerprint” unique to both the signer and the content, thus ensuring both signer identity and content integrity, while preventing the risk of deniability (non-repudiation). Because they are based on international PKI standards, digital signatures can be easily validated by anyone using widely available applications such as Microsoft Word and Adobe Reader, without the need for proprietary verification software.

When it comes to laws and regulations, only digital signatures are compliant with the most stringent requirements set by government agencies, including major regulations such as ESIGN, UETA, EU directives and VAT law, FDA 21 CFR Part 11, HIPAA and SOX. For entities requiring a higher level of security, some digital signature solutions also offer FIPS 140-2 Level 3 systems that have been certified by the National Institute of Standards and Technology (NIST).
Challenges and opportunities for digital signatures in the Legal market

Digital signatures are already being used by millions of signers around the world. Within the legal market, they are being used to sign a wide variety of documents including correspondence, billing, contracts and agreements, client onboarding, annual review documents, invoices, NDAs, IP documents and more.

The reasons that law firms and legal organizations use digital signatures include:

➤ Increasing value to clients:

Today, clients expect lawyers to understand and embrace technologies that enable them to work better and faster. An ALM survey conducted in May 2014 which focused on digital signature usage among legal professionals found that 49% of all documents are printed for the sole purpose of adding signatures. The survey also found that processes requiring physical signatures were extended by 1.24 days on average. By using digital signatures, law firms and other legal organizations prove that they are forward-thinking and not resistant to technological change while delivering better results faster.

➤ Document security and control:

By using digital signatures, law firms and legal organizations increase the security of their electronic documents and the control they have over them. Long-term accountability is ensured by creating documents that are completely transparent, easily auditable, and fully compliant. Any change applied to an electronic document that has been digitally signed immediately invalidates the signature, providing visible proof that the content of the document cannot be trusted. Further, lawyers can digitally sign and deliver documents without ever needing to save or deliver them through third party servers, thus enabling them to maintain complete control over their data.

➤ Avoiding vendor lock-in:

Standards-based digital signatures can be verified by any recipient with commonly-used applications such as Microsoft Word, Excel and Adobe Reader among others. Proprietary verification software from a single vendor is not required for ensuring the identity and intent of the signer or the integrity of the signed content.

➤ Competitive edge:

Digital signatures enable lawyers to eliminate the delays and costs associated with “wet ink” signing processes and quickly provide clients with signed, legally enforceable electronic documents they can easily verify for signer identity and content integrity. In addition, lawyers and other legal professionals are using digital signatures for signing internal documents, allowing them to improve collaboration and efficiency.
A “green” and more cost-efficient work environment

By embracing digital signatures, law firms and legal organizations are eliminating paper-related expenses as well as the indirect costs that arise from delays and other workflow obstructions—all while impressing clients with environmentally friendly, faster and more reliable processes.

How do I make the business case for digital signatures?

The legal market is embracing automation technologies that enable lawyers and other legal professionals to work better and faster. This is because today’s legal environment requires law firms, in-house legal departments and legal organizations to streamline their business practices to remain competitive and meet changing client demands.

Law Firms

Lawyers engage on a daily basis with documents that rely on signatures. With digital signatures, lawyers can spend time delivering value in a way clients appreciate, rather than wasting it on outdating paper-based processes.

Legal Departments

Attorneys, investigators, legal secretaries and other employees in the legal department can use secure digital signatures to streamline a variety of processes. Contracts and agreements in particular lend themselves to the use of digital signatures, and organizations are now making use of self-hosted portals that allow external parties to review and sign documents that remain under internal control.

While the benefits digital signatures deliver to operational efficiency are evident, cost savings should also be considered. Today, paper-based signatures are estimated to cost over $5 each from associated expenses (paper, printing, routing, archiving, replacing lost documents, etc.). With this, a firm with only 10 signers who each sign two documents a day can eliminate over $25,000 in organizational costs with digital signatures. Read our ROI white paper to learn more about the return on investment on a digital signature solution.

How do I select the right digital signature solution for my organization?

Here are some considerations to keep in mind to ensure that you select the right digital signature solution:

- Does it comply with digital signature standards and regulations?

The ideal digital signature solution should comply with global digital signature standards, including those recognized, endorsed and adopted by governments, industries, and independent software vendors under standards bodies such as NIST, ETSI, ISO, OASIS, IETF, and W3C. The digital signature
solution should also support compliance with regulations such as ESIGN (Electronic Signatures in Global and National Commerce Act), UETA (Uniform Electronic Transactions Act) and the EU Directive on Electronic Signatures (EU Directive 1999/93/EC).

➤ Does it allow you to keep control in your hands?

Be sure that the digital signature system you choose allows you to control the methods, policies, procedures and technologies that best fit your organizational governance and standard operating procedures. You should not need to re-engineer your business because of the narrow specifications and requirements of an outside party or vendor. The digital signature solution should adapt to your enterprise policies, procedures and complementary technologies—not the other way around.

➤ Can it be integrated with your existing applications and systems?

A digital signature system should not be a workflow solution or a document management solution. Instead, the ideal digital signature solution should be a high performance signature “engine” that seamlessly integrates into your existing applications and business systems, including content management solutions such as OpenText eDOCS and HP WorkSite. The solution should seamlessly allow you to continue using the applications and file types you already have in place.

➤ Does it allow you to keep your data in your domain?

In order to maintain the highest levels of security, the ideal digital signature solution should not require that you deliver your digitally signed documents through, or save them on, third party servers.

➤ Does it allow any recipient to easily verify your signature?

The digital signature solution you choose should be standards-based, allowing any recipient—whether inside or outside of your organization—to use common applications such as Microsoft Word or any PDF reader to verify the signature, rather than requiring the use of proprietary verification software.

➤ Can it be easily deployed and maintained, and does it offer a low total cost of ownership (TCO)?

The ideal digital signature solution should be a turnkey product from a single vendor that can be installed and operated within a few hours, and one that requires minimal IT maintenance work. It should not be a complex solution comprised of a hodgepodge of technologies from multiple suppliers that need to be integrated and maintained, thereby resulting in a high TCO.

➤ Does it offer a variety of deployment options?

Choose a solution that offers both on-premises and cloud-based deployment options to suit your specific requirements. It should also enable users to sign using any device, whether they are in the office using a PC or on the go using a tablet or mobile device.
Conclusion

On a day-to-day basis, lawyers and legal professionals manage a plethora of document-centric processes that require signatures. Without a secure and compliant signing solution, they are forced to spend time and resources printing documents, delivering them for signing, and scanning them back into electronic format or physically routing them to their destination. Relying on “wet ink” signatures also requires that firms have a solution for archiving huge amounts of paper documents and for replacing lost documents.

Digital signatures enable law firms and legal departments to replace slow, cumbersome and expensive paper-based signing processes with fast and fully automated ones, all while enabling users to maintain control over their sensitive data. They improve productivity and efficiency, ensure the security of signed documents, shorten turnaround times and make evident to clients that the legal professionals serving them are doing so with the technologies that enable them to deliver the greatest value.