DocuSign®

Ten Tips for Selecting a Digital Signature Solution

As the traditional paper-based world gives way to global digital businesses, documents often require signatures to be collected from people across the world, both employees and external partners or customers. To address this issue, organizations are demanding innovative solutions that help them get rid of paper altogether.

While many companies are already using document management systems, the final step of getting their documents signed usually breaks the otherwise fully-automated workflows by requiring users to print and sign with pen and paper. Not only does this prevent companies from gaining the full benefits out of their investments in automation, it also adds unnecessary delays and expenses to what can be a completely digital process.

What these organization need to solve the problem are easy-to-use tools for digitally signing and authenticating documents and forms. The solutions they are looking for must be able to quickly transform the organization's paper-intensive processes to paper-free ones by:

- Reducing paper-related costs, such as printing, scanning and couriering
- Speeding up signature-related processes in order ensure prompt turnarounds
- Enabling everyone inside and outside the organization to sign anytime from any device
- Providing iron-clad protection against forgery, guaranteeing non-repudiation
- Promising the same level of security and trust that exists with conventional documents
- Offering a rapid Return on Investment (ROI) and a low Total Cost of Ownership (TCO)

Prior to selecting the digital solution that best suits your organization's requirements, there are several important questions that you need to ask yourself. This white paper outlines the 10 most critical issues that you must take into consideration before making this decision. While not all are obvious, they are make-or-break factors for the smooth implementation, management and use of such a system, impacting every aspect of your business processes.

DocuSign®

1. Does it enable you to sign the file types/content applications you typically use?

The paperless world requires the same flexibility as with paper documents, where the type of document doesn't matter when it comes to signing it - a form, an invoice or a typed contract. The digital signature solution should allow you to sign using the content-authoring applications, document management systems and file types you are already utilizing. From the most commonly used applications such as Microsoft Word, Excel and Outlook, through to standard file types such as PDF and TIFF, and all the way to SharePoint, InfoPath, AutoCAD, and more.

2. Does it provide ease-of-use for digitally signing documents?

The digital signature solution should be simple to use for every member of your organization. A quick and intuitive signing process, which takes no more than 10 seconds or 1-2 mouse clicks, ensures that you will encounter no resistance or reluctance from even the most technophobic signers who are used to the traditional way of signing, and reduce the load on your IT support staff. It should also provide the features that are important to your organization's way of working, such as multiple types of graphical signatures, customizable signatures, multiple signatures on a single document, batch signing processes, and multi-language support.

3. Does it work with your existing content/workflow management applications?

Organizations that have invested in automation can gain the full benefit of their investments by adding a digital signature solution, which eliminates the need to reintroduce paper into the workflow just in order to collect signatures. The right digital signature solution needs to be able to seamlessly integrate with the electronic content/document management and/or workflow automation system you are currently using, such as SharePoint, OpenText, Oracle, Alfresco, Laserfiche, Nintex and K2.

4. Does it enable you to keep your sensitive documents inside your IT domain?

For security purposes, the digital signature solution should ensure that your documents remain inside your IT domain and are never saved on external third-party servers. Solutions that allow the document to be saved externally expose them to the risk of tampering and fraud because they are subjected to third-party controls and service adequacy.

5. Does it to provide you with complete control over its implementation?

A digital signature solution should be able to adapt to the specific processes, technologies, user management and authentication requirements of your organization — not the other way around. This will enable you to easily manage the digital signature solution in a way that best suits your internal regulations, governance policies and standard operating procedures. It should also readily integrate with your organization's HR, IT, security and screening policies, as well as the user-provisioning and user-management systems you already have in place.

DocuSign®

6. Does it comply with the regulations that are relevant to your organization?

The digital signature technology should be based on internationally accepted standards that comply with the country- and industry-specific regulations that are relevant to your organization. If your organization needs higher level security, the solution should be validated by NIST's FIPS regulations. A digital signature system must meet the requirements of event the strictest regulations and legislation, such as FDA's 21 CFR Part 11, HIPAA, Sarbanes Oxley, E-sign, UETA, and the EU Directive for Electronic Signatures.

7. Does it enable anyone to validate the signature even without access to the system?

Digital signatures that are based on standard PKI (Public Key Infrastructure) technology seal the document with a one-time "fingerprint," which is unique to both the signer and the document, thus ensuring that the signer is legitimate and that the document is not altered after signing. Otherwise, the digital signature is automatically invalidated, providing protection against forgery. This also ensures that the signature is transportable so that anyone inside or outside your organization can use widely available software, such as Adobe Reader or Microsoft Office, to verify these parameters - who signed the document (signer identity), why they signed it (signer intent), and that it hasn't been changed since it was signed (document integrity).

8. Does it provide the ability to digitally sign via the web and mobile devices?

Users must be able to digitally sign using any device, anytime and anywhere, whether they are at the office on their PC, at home on their tablet, or in the field using a mobile device. The right solution should enable everyone - including partners, customers and other collaborators - to add digital signatures to their documents without having to install software.

9. Does it offer the option to self-host the system?

Each organization has different business, IT and security requirements when it comes to the way it implements a digital signature solution. Therefore, the best solution should allow you to choose between an on-premises server and a managed cloud-based system so that you can set up the system according to your internal needs. While an on-premises solution ensures maximum flexibility and control, a secure cloud-based system enables you to start small and expand the number of signers as needed.

10. Does it provide cost-effective IT management?

Not everyone considers TCO when purchasing a digital signature solution but it is certainly a parameter to be evaluated, taking into account product cost, deployment, digital certificate renewal fees, training and support. Besides the paper-related cost savings, such as printing, mailing, scanning, couriering and archiving, the solution should provide a low TCO (Total Cost of Ownership) through quick installation, minimal operational impact, and insignificant IT maintenance work. As opposed to traditional digital signature systems, which were based on complex technology making them difficult to deploy and manage, today's systems are much easier to deploy, support and integrate into your existing systems.

In summary, to ensure a smooth transition from paper-intensive to paper-free offices, select a digital signature system that enables you to:

- Sign using the file types/content applications you currently utilize
- Provide all signers, internal or external, with an easy-of-use system
- Work with your existing content/workflow management applications
- Keep your sensitive documents inside your enterprise IT domain
- Maintain complete control over its implementation methodology
- Comply with the regulations that are relevant to your organization
- Allow anyone to validate the signature even without access to the system
- Allow users to digitally sign anytime anywhere via the web or mobile devices
- Select between hosting the system on-premises or using it as a cloud solution
- Manage it cost-effectively with a low overall TCO, leading to a rapid ROI

About DocuSign

DocuSign, Inc. (DocuSign®), helps organizations achieve their digital transformations for dramatic ROI, increased security and compliance, and better experiences for customers, partners, suppliers and employees. DocuSign automates manual, paper-based processes with the only open, independent, standards-based platform for managing all aspects of documented business transactions. DocuSign empowers anyone to transact anything, anytime, anywhere, on any device securely.

For more information on how to choose the most suitable digital signature solution, please visit us at www.docusign.com.