

How to Choose a Digital Signature Solution

There are 10 simple points to consider when choosing a Digital Signature Solution (standard electronic signature) for your organization. While not all are obvious, they are critical make-or-break factors for the smooth implementation, management and use of such a system, impacting on every aspect of your business processes. To ensure a low Total Cost of Ownership (TCO) and a speedy Return on Investment (ROI) from your Digital Signature solution, read on.



Seals Documents - This is the basic building block of a true digital signature solution. It guarantees the document is sealed from changes, whether incidental or the result of a late night hacking of your network.

Tip: Only digital signatures based on Public Key Infrastructure (PKI) technology can truly seal a document. Any other type of solution can be easily forged.



Multiple Application Support - Many digital signature solutions support only PDF and Word applications, which may be sufficient support for some. However, if your organization needs to digitally sign in additional programs such as Excel, AutoCAD, and web applications, this type of solution will fall short of your needs.

Tip: Make sure the applications you intend to sign in your organization are supported by the solution you choose.



Graphical Signatures - Of the standard applications that have digital signature capacity, almost all lack graphical signature support. This is a major shortcoming. Graphical signatures ensure the signature is visually noticeable, and

have a psychological impact: the signer is reassured they have signed the document and that it is legally compliant.

Tip: Occasionally, different graphical signatures are required (e.g., initials, full signature). Verify that your solution has this capability.



Multiple Signatures - Many digital signature solutions do not allow altering the document once a signature is applied. This is good in terms of sealing the document, but problematic if the technology also prevents additional users from adding their required signatures to the document.

Tip: If your company requires several people to digitally sign a document, ensure that your solution offers this feature.



Zero IT Management - Be aware that the time to deploy a system is typically lengthy and resource-intensive. IT staff can find themselves spending weeks every year managing the selected digital signature solution. Then again,

the company may opt to employ an additional staff member to manage the task, or implement a help-desk just to ensure users can digitally sign their documents. Costs can skyrocket.

Tip: Ensure your solution is operational the moment it is deployed on your network, and that the "Zero-Management" requirement on your checklist is met.



Compliance - Each regulation has its own specific requirements pertaining to electronic documents. For example, the FDA 21 CFR Part 11 regulation for the Pharmaceutical market has numerous requisites that are not

met by most digital signature solutions.

Tip: Review the regulations for your industry and make sure the solution covers all of those requirements.



Transportability (Worldwide Verifiable) - Do you want your customers or partners to be able to validate files you've signed electronically? This seemingly trivial task is not so trivial at all. Not every digital signature may be transportable outside of your organization. In fact, digital signature technology is not always embedded in your document.

Tip: Make sure your documents can be validated by external users without them having to install a 3rd-party application.



Seamless User Registration - Implementing your digital signature solution must be as simple as possible. Make sure that the moment the solution has been deployed, staff at your organization can start digitally signing documents without having to start a "wizard" to enroll or call on the IT department for support.

Tip: Make certain that your solution is capable of automatically and seamlessly updating user profiles from the company's user directory.



Simple-To-Use - Be sure to choose a system that is easy-to-use. You don't want staff to run a wizard application when they A) load the signature application onto their PC and then B) every other time they want to sign a document. IT staff involvement should be kept to a minimum.

Tip: It should take a single click to ensure your document is sealed and legally compliant.



Total Cost of Ownership - Not everyone considers TCO when purchasing a digital signature solution. But to ensure you don't pay too much in the long run, take the following costs into account: initial product cost, deployment, help desk, digital certificates (which may be a recurring annual cost), and development of support for the application you're going to sign with.

Tip: Project your TCO three years into the future to reveal any hidden costs, such as renewal of annual certificates.