



10 Tips for Selecting the Best Electronic Signature Solution

Avoid the pitfalls of transitioning from paper-based to a paper-less office with an effective digital signature (electronic signature) system.

January 2009

 *Keep Your Business Moving*

ARX | 855 Folsom St. Suite 939 San Francisco, CA | (415) 839 8161 | www.arx.com | sales@arx.com



Introduction

As the traditional “paper-based” world gives way to digital documentation and transactions, enterprises are demanding innovative solutions for digitally signing and authenticating such documents, files, and forms with iron-clad protection against forgery. Solutions must guarantee non-repudiation and promise the same level of security and trust that exists with conventional documentation. At the same time, such a solution should be simple to use, easy to deploy and offer a rapid Return on Investment (ROI).

With the rise of global digital businesses, transactions and documents may need to be signed by many people in different parts of the world. Users should be able to sign documents directly from their desktop or via a zero technology footprint using any web browser.

The best digital signature system can:

- ▶ Verify recipients outside of an organization
- ▶ Enable employees to sign documents while traveling
- ▶ Enable cross platform capabilities
- ▶ Enable the use of numerous applications, such as Microsoft Word®, Adobe Acrobat®, and TIFF images.

When it comes to selecting a digital signature system, an enterprise needs to be aware of several important criteria. This White Paper outlines the 10 most critical scenarios to take into consideration when making this decision.

1. Sealing Documents

The best digital signature system seals the document using standard technology.

A company may choose an electronic signature system that adds a graphical signature image to any document created in Microsoft Word. This signed document can be easily changed by any recipient while the graphical electronic signature remains intact. This security flaw opens the door to fraud and forgery.

The solution used has simply placed a digitized “picture” of the signature on the document, it doesn't:

- ▶ Seal the document
- ▶ Verify the authenticity of the person signing
- ▶ Guarantee the transaction cannot be altered

In the traditional paper world, transactions are validated by signing them either on an accepted form, such as a check, or in front of a trusted third party. A notary or lawyer, then “stamps” the signatures, so that they cannot be changed.



In the virtual paperless world, digital signatures must perform the same function. For example, there must be a guarantee that the signer is legitimate (that signatories are who they claim to be) and that neither the signature nor anything written in the document can be changed without authorization.

In the traditional paper world, transactions are validated by signing them either on an accepted form, such as a check, or in front of a trusted third party. A notary or lawyer, then “stamps” the signatures, so that they cannot be changed.

In the virtual paperless world, digital signatures must perform the same function. For example, there must be a guarantee that the signer is legitimate (that signatories are who they claim to be) and that neither the signature nor anything written in the document can be changed without authorization.

A digital signature must be able to seal any electronic document and guarantee that it is tamperproof. It uses a one-time “fingerprint”, unique to both the signer and the document to ensure that the signer is indeed the originator or owner of the document. This “fingerprint” cannot be reused or reassigned and proves that the message has not been altered in any way. Should the document be changed or altered, the digital signature is automatically invalidated, providing total protection against forgery.

2. Multiple Application Support

The best digital signature system supports multiple applications.

Many electronic signature systems enable the signing of documents created with the most commonly used applications - Microsoft Word and Adobe Acrobat. However, there are some documents produced by ERP systems that also need to be signed, but the electronic signature system does not support this application.

Traditionally, when signing paper documents, it doesn't matter what type of document it is, be it a form, an invoice or a typed contract. Now, the paperless world requires the same flexibility.

There are a number of different applications and document management systems that offices are using. It is important to select a digital signature solution that not only supports different applications, such as:

- ▶▶ Word, Excel®
- ▶▶ Outlook®
- ▶▶ PDF®, TIFF
- ▶▶ AutoCAD®
- ▶▶ InfoPath®
- ▶▶ Other third party applications

Users should be able to add an electronic signature to any document type. One way to guarantee support for any file format is provided by digital signature systems that convert any documents from any system into a “signed” PDF file.

3. Graphical Signatures

The best digital signature system offers the possibility of "seeing" the signature.

Traditionally, once a document has been signed with a "wet" signature, it is easy to identify who signed the document and the capacity in which it was signed. For example, when renting an apartment, the parties involved sign a lease. The contract clearly displays the signatures and identifies who is the landlord and who is the tenant. Anyone looking at the document can easily identify the signatories and their roles.

In the virtual paperless world, digital signature systems offer trust and security but they do not offer easy identification. Visual graphical signatures do not add any security to the document, but they are important from a user's acceptance point of view, as they provide a natural user indication that the document is indeed signed.

It is therefore important to include the digital signatures, which preserve the data integrity of the document, as well as the digital signer's authenticity, and the graphical image of the signer's handwritten signature, which is a familiar form of identifying the signer.

4. Multiple Signatures

The best digital signature system enables documents to be signed by more than one person in more than one place.

There are some electronic signature systems that only allow one signature and when the document has been signed and sealed, it is impossible to add more signatures.

Traditional document-intensive organizations, such as insurance companies or financial institutions, have large volumes of many different types of documents that must be processed every day. Many of these documents must be reviewed, approved and signed by more than one person. In some cases, one part must be approved by one signatory while another section needs approval by a different person. With a traditional "wet" signature, it is a simple matter of signing or initialing any place in the document.

In the virtual world, an effective digital signature system should enable "sectional signing", which allows signatories to edit and sign their portion of the document. For example, in Microsoft Excel, the digital signature solution should be flexible enough to allow multiple users to sign an entire workbook. Different users should be able to sign single worksheets or even support different digital signatures for different ranges of cells in the spreadsheet.

5. Zero IT Management

The best digital signature system is easily installed, intuitive to use and does not require a dedicated support staff - it will work from the moment it is installed.



In the traditional world of paper documents, all that is needed to sign and manage documents is efficiency and ink.

In the virtual world, installing a new software system can generally be lengthy and resource-intensive. Some systems require extensive and expensive customization to integrate with current or legacy software. They often take more than a year to get it working and require additional support staff and even a separate help desk to support the electronic signature application.

Users want to be able to use the solution intuitively, without the need to go through a long and lengthy learning cycle, or to be forced to employ a wizard process every time they want to sign a document. If the system is bulky and difficult to use, people will find a way to avoid it.

6. Compliance

The best digital signature system complies with all legal requirements.

To be considered legally binding, documents and transactions – paper-based or electronic – must meet many basic requirements and strict standards. A digital signature solution must meet the same criteria as a “wet” signature. These include the following basic requirements:

- ▶▶ Authenticity – the signature can be authorized by a secure process.
- ▶▶ Integrity – any tampering during transmission can be detected
- ▶▶ Privacy – the signature cannot be accessed by unauthorized sources
- ▶▶ Enforceability – the signatures must be verifiable by all parties
- ▶▶ Non-refutability – the signature cannot be denied or disavowed.

The first two requirements prove that the recipient and the sender are authentic and authorized to perform this transaction. The next two, provide methods to prove that the message content is authentic and that the recipient can be certain that the data has not been altered or lost in transit. The last important requirement is that the message must be able to “stand up in court”. Referred to as “non-repudiation”, this means that the digital signature must ensure that the parties involved in the transaction cannot deny sending the message or its contents.

In addition to the above general requirements, some industries such as finance or pharmaceutical have specific requirements. For many organizations, it is critical to protect their data at all times with standard-based PKI methods that meet the toughest regulations rather than a proprietary solution.

To avoid returns and force the organization to prove that the solution is good enough, a digital signature system must meet the most stringent internationally recognized regulations, for example:

- ▶▶ FDA's 21 CFR Part 11
- ▶▶ Health Insurance Portability and Accountability (HIPAA)
- ▶▶ Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley)
- ▶▶ Sarbanes Oxley
- ▶▶ FAA's CFR Title 14
- ▶▶ and legislation, including:

- ▶ Uniform Electronic Transactions Act (UECA)
- ▶ E-sign (Electronic Signature in Global and national Commerce Act)
- ▶ EU VAT Directive
- ▶ EU Directive for Electronic Signatures

Only PKI based digital signatures meet all these requirements. Other solutions may meet some but not all requirements.

7. Transportability

An effective digital signature system should ensure transportability.

If a company implements a digital signature solution and sends a signed document to a client who has not installed the same digital signature system, they will not be able to verify the document.

In the traditional paper world, signed documents sent to third parties can be read and understood without a problem.

In the paperless world, however, documents must be recognized by the software application. To be truly versatile, a sender must know that a digital signature will arrive unaltered anywhere in the world and that it can be easily verified without the need for complicated, proprietary third party applications.

For example, if a document had been electronically signed in PDF, then the recipient should be able to validate the document using the free Adobe Acrobat Reader without any further software installations. Another example is when a Microsoft Word® or Excel® document is signed, then it should be possible to verify it on the receiving end without the need to install any special software or plug-in for verification process.

8. Seamless User Sign-Up

The best digital signature system offers simple-to-use, transparent sign-up.

In the traditional paper world, people who need to sign documents are identified in one of several ways:

- ▶▶ Via a signature card in-person at the bank
- ▶▶ Through a photo ID or personal recognition

In the virtual paperless world, signatories register electronically and obtain a digital certificate. The certificate provides electronic identification similar to a birth certificate or a passport. Digital certificates contain information about the user, such as the certificate holder's name, e-mail address and other specific identifying information. Digital certificates verify that the user is who he or she claims to be. Certificates are generated by the Certificate Authorities (CA) immediately after the identity of the user is validated.



Once a digital signature system has been deployed, it should be both simple to use and as transparent as possible. Neither the users, nor the IT person, should be aware of how a certificate is generated or maintained.

Moreover, users should not need to use a wizard or call the Help Desk to be able to sign documents. It should also be easy for the IT manager to make changes in the users' profile and these changes should be automatically reflected in the users' certificates.

In addition, some systems require employees to re-enroll every year to verify that they are still authorized by the company. Users will find this cumbersome as will the IT and HR departments who need to deal with these registrations.

9. Simple-to-Use

The best digital signature system is technologically simple to use.

In the traditional paper world, signing a document is simple, intuitive and quick.

In the virtual paperless world, signing a document should be just as easy. It should take no more than 10 seconds or 1-2 mouse clicks - to ensure that the document is signed, sealed and legally compliant.

But if your digital signature solution requires the user to go through a tedious wizard-type process to sign a document and each step of the process requires a user interaction making the process complicated and difficult, the inadequacies of the selected solution will soon become apparent. Users should not be required to learn new technologies or require assistance from a Help Desk.

10. Total Cost of Ownership

The best digital signature system has no hidden operation and management costs.

Traditional paper signing leaves mountains of paperwork. This requires physical storage in archives that often mushroom to warehouse proportions. To reduce costs and improve efficiency, companies should move into the world of electronic processes.

Standards-based digital signature systems enable companies to become totally paperless. However, when considering a digital signature solution, it is important to look into the potential hidden costs.

Many traditional digital signature systems are based on complex PKI technology and are difficult to deploy. They involve complicated software requiring a heavy investment in IT support and development. Sometimes, a Help Desk needs to be created or additional staff employed to support the system. Other costs that need to be checked include registration and renewal fees for digital certificates, cost for smart cards, etc.

Learn more about the cost saving for your organization in our [Digital Signatures ROI White Paper](#).



Conclusion:

To ensure a smooth transition from paper-based to paperless offices with a digital signature system that:

- ▶▶ Guarantees non-repudiation
- ▶▶ Offers a high level of security
- ▶▶ Effectively seals documents
- ▶▶ Allows multiple signers to sign on a single document without difficulty
- ▶▶ Is compatible with multiple applications
- ▶▶ Is simple to use
- ▶▶ Offers a rapid return on investment
- ▶▶ Has no hidden costs
- ▶▶ Is transportable without having to install proprietary software

About the Author

John Marchioni, is currently the Vice President of Business Development at ARX - The Digital Signature Company. John has over 20 years experience in US and international high-technology markets creating partnerships through strategic sales, technology licensing and large-scale systems-integration projects. Prior to joining ARX, he held various positions with companies engaged in R&D, software licensing, equipment manufacturing, and worldwide sales of data communications, wireless, and information-security products including: VP Business Development, Celvibe, a Eurofund venture in wireless broadcasting technology; Director Business Development, Cylink (NASDAQ:CYLK); Program Manager Defense Applications, Microsoft (NASDAQ:MSFT); and Chief Compliance Engineer, Retix (NASDAQ:RETX).

John was appointed Visiting Scholar Associate for Informatics at UC Berkeley (2004-2006). He is a member of the Security Council of the Gerson Lehrman Group. He has been a panel speaker for NSF at workshops on Grid Computing and the Cyber Infrastructure, and is a member of the advisory board of UCLA's Center for Embedded Network Sensing (CENS). John also served as Director of Technology Programs and Advisor to Gordon and Betty Moore Foundation of San Francisco from 2002 to 2006. He has a B.Sc. in Computer Science from the University of Pittsburgh, Pennsylvania.

For more information about [Electronic & Digital Signatures](#) visit www.arx.com or contact John at johnmarc@arx.com



About ARX -The Digital Signature Company

ARX is a global provider of digital signature solutions for the life sciences, healthcare, government, engineering, and manufacturing organizations. ARX has over 20 years of experience assisting life sciences, healthcare, governmental, engineering, and manufacturing businesses cost effectively to secure, streamline, and scale their business processes and transactions. The company specializes in enabling organizations of any size to scale digital signature and security solutions at the lowest TCO while retaining proper control mechanisms that are required by legislation, regulation and industry best practice. For more information, please visit www.arx.com.

 *Keep Your Business Moving*