www.arx.com

10 Tips for Selecting the Best Digital Signature Solution

Avoid the Pitfalls when transitioning from paper-based to electronic signatures

Sept 2007

Secure Simple

CoSign

Digital Signatures **Made Simple**

ARX • 855 Folsom Street • San Francisco, CA
www.arx.com • (925) 7980901 • 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 ROI.
In addition, with global digital business now the norm, 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 need for verification by recipients outside an organization, the ability of employees to sign documents while traveling, and cross-platform capabilities – enabling the use of numerous applications, such as Microsoft Word®, Adobe Acrobat®, and TIFF images – all mean that, when it comes to selecting a digital signature solution, 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. Seals Documents

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

Digital signatures take the concept of traditional paper-based signing and turn it into an electronic "fingerprint" or coded message. This is unique to both the document and the signer and binds both of them together. The digital signature ensures the authenticity of the signer. Any changes made to the document after it is signed invalidate the signature, thereby protecting against signature forgery and information tampering. Digital signatures help organizations sustain signer authenticity, accountability, data integrity and non-repudiation of electronic documents and forms.
For more information, please visit www.arx.com

Your company has chosen an electronic signature solution that ads an image of your graphical signatures to documents; you can now attach a graphic representation of your signature to any document created in Microsoft Word. This is all well and good, until you discover that even though you have apparently signed the document, it can be easily changed by any recipient – while the electronic signature[1] remains intact, just as you appended it. The door to fraud and forgery has been opened wide!

The solution used has simply placed a digitized "picture" of the signature on the document: it doesn't seal the document, it doesn't verify the authenticity of the person signing it, nor does it guarantee that 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, who then "stamps" the signatures so that they could not be changed.

In the virtual paperless world, digital signatures must perform the same function, i.e. 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 is a one-time "fingerprint", unique to both the signer and the document and ensures 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.

[1] An electronic signature simply captures a graphic image while a digital signature performs a cryptographic algorithm that appends a message digest or "fingerprint" to the document.

ARX • 855 Folsom Street • San Francisco, CA
www.arx.com • (925) 7980901 • sales@arx.com

2. Multiple Application Support

The best digital signature solution supports multiple applications.

You are operating an electronic signature solution that enables the signing of documents created with the most commonly used applications – Microsoft Word and Adobe Acrobat.

But there are some documents produced by your ERP system that also need to be signed and your electronic signature solution does not support this application because the ERP application is not supported by the chosen electronic signature solution.

Traditionally, when signing paper documents, it didn't matter what type of document it was; a form, an invoice or a typed contract. Now you need the same flexibility in a paperless world.

A number of different applications and document management systems are available. It is important to select a digital signature solution that not only supports different applications, such as Word, Excel, Outlook, PDF, TIFF, AutoCAD, InfoPath and other third party applications, you should be able to add an electronic signature to any document type. One way to guarantee support for any file format is provided by solutions that convert any documents from any system into a "signed" PDF file.

3. Graphical Signatures

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

Traditionally, once a document has been signed (with a "wet" signature), the signatures are visible. It is possible to identify who signed the document and the capacity in which it was signed; when renting an apartment, for example, the parties 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 solutions 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 both the Digital Signatures, which preserve the Data Integrity of the document and 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 solution enables documents to be signed by more than one person in more than one place.

There are some electronic signature solutions 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 solution 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 to sign single worksheets or even support different digital signatures for different ranges of cells in the spreadsheet.

ARX • 855 Folsom Street • San Francisco, CA
www.arx.com • (925) 7980901 • sales@arx.com

5. Zero IT Management

The best digital signature solution is easily installed, intuitive to use and does not require 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 solutions require extensive – and expensive – customization to integrate with current or legacy software; often taking more than a year to get it working, additional support staff and even a separate help desk to support the 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 solution 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 and most important 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[2] 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 solution 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 (UETA);
- E-sign (Electronic Signature in Global and national Commerce Act)

2 Public Key Infrastructure (PKI) is the basis for standard electronic signatures today. It provides each user with a Private Key and a Public Key, used in every signed transaction.

ARX • 855 Folsom Street • San Francisco, CA
www.arx.com • (925) 7980901 • sales@arx.com

- 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 solution should ensure transportability.

Your company has implemented its digital signature solution and has sent signed documents to a client. But because the client has not installed the same digital signature solution, he is unable 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 virtual 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 solution 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: a signature card signed in person at the bank, a photo ID or personal recognition.

In the virtual paperless world, signatories register electronically and obtain a digital certificate, which 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 a Certificate Authorities (CA) immediately after the identity of the user is validated thus making the certificate a virtual equivalent of a Passport or a Birth certificate.

Once a digital signature solution 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 solution 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 solution has no hidden operation and management costs.

Traditional paper signing leaves mountains of paperwork needing 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 solutions 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 solutions 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 solution. Other costs that need to be checked include registration and renewal fees for digital certificates, cost for smart cards, etc.

The CoSign® Solution

CoSign is ARX's turnkey digital signature solution that delivers an innovative way to digitally sign documents, files, forms and other transactions while ensuring iron-clad protection against forgery. The solution is simple to use and easy to deploy.

With CoSign, any enterprise can easily sign documents using numerous applications, such as Microsoft Word, Adobe Acrobat, TIFF images, etc. CoSign signatures seal an electronic document, ensuring the authenticity, integrity and confidentiality of the electronic transaction guaranteeing non-repudiation.

Key Features of CoSign

CoSign brings at least the same level of security, trust and simplicity that exists in the physical world, to the electronic world with strong, standard signature technology based on encryption technology.

CoSign is a highly-scalable FIPS 140-2 Level 3 certified appliance that enables users to sign documents directly from their desktop or via zero technology footprint using any web browser.

CoSign key features include:

- One-click signature via a user-friendly interface
- Graphical signature – a visible, recognizable graphic that compliments the digital signature
- Quick, easy deployment – within hours of initial deployment users can be electronically signing
- Zero Management – CoSign synchronizes with existing user directories to generate signing keys for all users
- Guarantee of data integrity and signer identity to ensure non-repudiation of documents and transactions
- Transportability – verifiable worldwide by third party recipients without the need for any proprietary software
- Compliance with regulatory rules world-wide; including an audit trail and verification of document sources

ARX • 855 Folsom Street • San Francisco, CA
www.arx.com • (925) 7980901 • sales@arx.com

- Multiple support for applications and documentation management systems
- Central key storage – keys are generated and stored in CoSign's secure appliance, eliminating the need for smart cards, USB tokens, etc.
- Built-in authorizations with multiple authentication methods and user management synchronization
- Support for multiple signatures and batch signatures

CoSign integrates easily with legacy and in-house systems. The SAPI (Signature Application Program Interface) provides support for new applications, third party document management solutions and customized in-house systems. CoSign enhances business processes, reduces costs and creates totally secure documents.

Business Benefits

CoSign offers an "out-of-one–box" digital solution. It solves complex deployment problems and dramatically reduces the TCO of deployment. New users can automatically enroll in the PKI system. CoSign creates the keys, issues certificates and renews them ensuring that the system is always simple and user-friendly. In addition, the CoSign solution allows companies to choose whether to manage their users inside the CoSign application or through an outside user directory, such as MS Active Directory®, Novel NDS® or any other LDAP directory.

The CoSign solution streamlines business processes – such as approval procedures – increasing employee productivity and efficiency. It maintains necessary audit trails eliminating the risk of misappropriation of intellectual property while still providing easy access to information. It provides significant cost savings to enterprises by creating a true paperless environment; documents can be e-archived rather than in the traditional paper manner. In addition, the CoSign solution provides easy deployment, thereby providing a quick ROI.

With CoSign digital signatures, enterprises can be assured that electronic documents are even more secure than paper documents. It will no longer be necessary to print an electronic form on paper and chase after a signature. All it takes is one click on the "Sign" icon to send an electronic document anywhere, anytime.

ARX (Algorithmic Research)

Founded in 1987, ARX provides electronic signature and data-security solutions worldwide. ARX offers financial, commercial, legal, and governmental sectors a wide range of high-end, state-of-the-art products and services designed to simplify, seal, secure and accelerate electronic transactions anywhere, anytime. The company specializes in designing and implementing simple-to-deploy electronic signature and security solutions.

With its large install base and worldwide presence; ARX's goal is to provide customers with simple, yet powerful solutions that drastically reduce the risk to Internet-based communications and transactions. They provide solutions that offer significant savings, increased productivity, expedited results, as well as an enhanced customer experience.

For more information about ARX and CoSign, visit www.arx.com.

ARX • 855 Folsom Street • San Francisco, CA
www.arx.com • (925) 7980901 • sales@arx.com