A Practical Deployment Strategy for Digital Signatures and Seals in Fully Electronic AEC Processes

May 2012
A Practical Deployment Strategy for Digital Signatures and Seals in Fully Electronic AEC Processes

An Overview of Digital Signature Technology and a Guide to Deployment

May 2012
# Table of Contents

- Acknowledgements .................................................................................................................................................. iii
- Preface ....................................................................................................................................................................... iv
- About This Guide .......................................................................................................................................................... v
- Executive Summary .................................................................................................................................................... vi
- Introduction: Vision ....................................................................................................................................................... 1
- The Problem with Wet Signatures: Archaic, Burdensome, and Costly ................................................................. 4
- The Solution: Keeping an Otherwise Electronic Process Electronic ..................................................................... 13
- The Digital Signature Primer: Understanding Digital Signature Standards and Technology ...................................... 15
- How-To: Practical Strategies in Application, Deployment, and Employee Use ......................................................... 19
- Summary ................................................................................................................................................................... 30

## Appendices

- A. General Legal Statutes, Local Guidelines, Practices, and Regulations ................................................................. 31
- B. Vendors Offering Digital Signature Aware Applications ..................................................................................... 34
Acknowledgements

I would like to thank the members of the Fiatech Digital Signatures and Seals Project Committee as well as the Fiatech Board of Advisors and Fiatech membership for their support and input in the preparation of this Practical Deployment Strategy Guide. In particular, I’m grateful to the following Fiatech member and partner organizations for their leadership in driving this initiative forward in the industry.

- American Institute of Architects (AIA)
- ARX
- Avolve Software
- Hatch
- Target Corporation

This publication is the first in a series of publications designed to encourage the adoption and use of digital signatures and seals throughout the building design, construction, and regulatory processes in nations across the globe.

Raymond E. Topping, PE
Director, Fiatech
Preface

Fiatech (www.fiatech.org) is an industry-led consortium administratively housed at The University of Texas at Austin that provides global leadership in identifying and accelerating the development, demonstration, and deployment of emerging technologies and innovative practices to deliver the highest business value throughout the life cycle of all types of capital projects.

Fiatech is member-driven and is comprised of approximately 85 companies and partner organizations that include owners and operators from the industrial, power, and retail markets; leading providers of engineering, design, and construction services; software and equipment suppliers; and technology providers, research institutes, and universities.

Fiatech is a clearinghouse for innovative ideas where members can quickly learn about new processes, methods, and materials; it also collectively funds and executes development, demonstration, and deployment projects. Project teams are formed to identify and accelerate the adoption of technologies and systems; demonstration projects are conducted to validate and perfect new approaches or methods; and teams are formed to aid and facilitate the deployment of those breakthrough initiatives that have been identified.
About This Guide

In the following pages you will find detailed information on digital signatures, including critical points to think about when assessing a potential solution. An overview of signatures and their effect on the bottom line is included to help you gain a complete understanding of how digital signatures bring the capital project industry forward—toward more efficient, cost-effective, and faster project delivery.
Executive Summary

Wake up, architecture, engineering, and construction firms! As you emerge from a rough economic slumber, new industry-wide efforts set ambitious goals to streamline business processes, increase operational efficiency, and adopt innovative technologies. To coincide with and support these efforts—and to show how simple it is to accomplish them—the Fiatech Regulatory Streamlining Subcommittee on Digital Signatures and Digital Seals has compiled this guide in cooperation with digital signature solutions providers, design firms, and other organizations in the capital projects delivery industry.

Serving as both an educational primer and a practical strategy guide for deploying digital signatures and digital seals, this publication outlines the problems associated with wet-signing as the status quo. It then provides compelling reasons to adopt a standard digital approach as an alternative to the current print-scan-mail workflow that prolongs high inefficiencies and unnecessary expenditures for its stakeholders. To address these problems, we introduce digital signature technology as a critical element of business process automation. In addition, we discuss the far-reaching benefits, including cost avoidance and expedited project delivery, of deploying this technology within organizations.

Digital signature technology is straightforward and quick to comprehend; digital signatures (also known as standard electronic signatures) are rooted in open, vetted, and peer-reviewed standards including the National Institute of Standards and Technology (NIST), International Telecommunications Union (ITU-T), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards bodies.

Through tamper-evidence and digital user ID certificates, digital signatures ensure that all parties can rely on the integrity of a document’s contents as well as the signer’s identity and intent.

Within a practical strategy for deploying digital signatures, we outline seven elements which you should consider prior to and during signature automation. First, the digital signature solution should maintain the integrity of the document, record, report, or calculation to which the signature is applied. Next, the solution should be compatible with your content-authoring applications. To address customization needs, the solution should have accessible standard interfaces if integration may be needed under larger workflow and collaboration solutions. An integral part of the solution requires: 1) binding the signatory to the document itself, and optionally when needed; and 2) binding any digitized
professional seals to the document and to the signatory. Further to your organization’s mode of operation, the solution should be compatible with your current governing policy as well as your procedure for user enrollment and authentication. Lastly, the solution should offer comprehensive controls over who has signature privileges, digital signature credentials, and digitized seals.

Practical, standard, and scalable digital signature deployment strategies are urgently needed. Wide deployment of digital signature technology will allow the global AEC (architecture, engineering, and construction) industry to take another critical step away from paper intensive overhead within organizations’ business processes.

The authors of this guide look forward to the day when digital signatures have been adopted ubiquitously. We hope this guide will help architects, engineers, construction personnel, and AEC industry regulatory bodies understand how digital signatures can benefit diverse work environments. Above all, we encourage you to consider deployment within your own organization.
Chapter 1
Introduction: Vision

Where Are We Today? Current Signing and Sealing Practices in AEC Firms
As AEC firms move to digital workflows to improve efficiency and reduce project cycles, they encounter bottlenecks at the point of obtaining a signature. Signatures interrupt electronic workflows and increase time requirements. When architectural drawings, engineering designs, and construction specifications, among other documents, require signatures and seals, the resulting project delays affect the industry as a whole.

In an increasingly digital world, AEC firms are challenged to keep current by eliminating time consuming, paper-based processes. The reliance on signed and sealed paper documents contributes to costly delays in project delivery and is a hindrance to the economic viability of the industry as a whole.

Today, AEC documents change from digital to print format several times over the duration of a project. Documents are created electronically, printed for review or approval, then signed, scanned back to electronic form, and printed again when needed for use in the field or for permanent storage in physical archives. There are several ways to cope with this inefficient and expensive paper-heavy life cycle, as more and more AEC firms are turning to electronic document and content management solutions, field-friendly mobile applications, and electronic workflow and approval processes.

While these solutions all help to reduce reliance on paper routines, they do not completely eliminate the need for paper. Ultimately, when signatures are required, pens are drawn. When professional credentials are necessary, ink stamps and seals are taken out from their desk drawers.

In order to realize the full potential of electronic processes in AEC firms, digital signatures can be deployed, converting this cumbersome paper-based process to a secure electronic one.

The aspiration to convert the AEC industry to all-electronic workflows is about more than just saving time and money. Corporate promises to adhere to sustainable practices are unable to be kept when paper plays such a large role in day-to-day activities.

“*The AEC/O industry spends an estimated $500 million or more each year moving plans from one discipline to another via such paper courier services as FedEx.*”
*Source: Cadalyst*

“A typical $100 million building project generates 160,000 separate documents: drawings, contracts, purchase orders, RFIs, and schedules.”
*Source: The Economist*
Sustainability does not only mean "green" environmentally friendly practices; it also means being a resilient, flexible machine that flourishes in changing economic climates and adapts to rapidly advancing technology. Deploying digital signatures enables AEC firms to make good on their paperless commitments while increasing efficiency and organizational collaboration.

The Paperless Building: In an Ideal World...

Imagine a new building project during which no paper is used from planning to ribbon cutting. No paper to negotiate contracts. No paper to plot designs. No paper to issue changes. No paper to sign off on final delivery.

The annual value in time saved, less resources consumed, and trees left standing amounts to millions of dollars when counting salaries, supplies, and signatures. In order for a building project to be truly paperless, buy-in from local regulatory authorities, permitting agencies, and other regulatory bodies must be obtained. In parallel, project stakeholders must take advantage of widely available technologies; everything from ubiquitous office productivity software, CAD applications, document management and electronic workflow solutions, PLM (product life cycle management), and other inventory solutions.

The pieces are not as difficult to assemble as you may think. In 2009, the Osceola County (Florida) Growth Management Building and Document Management Offices successfully permitted the construction of a hotel using an almost completely paperless process. The project was “submitted, reviewed, and issued completely paperless, except for the permit application.” Containing more than 700 pages, the paper alone would have weighed 100 pounds.¹

¹ http://poinciana.wordpress.com/2009/05/18/osceola-county-issues-first-paperless-building-permit/

Perspective from a Design Professional

The current model that blends paperless processes and paper copies - one for timely communication and the later for binding documentation – can result in a false sense of confidence in what should be understood as the latest contract document for construction.

It is better to recognize the traditional model of schematic, design development and construction or contract documents as the foundation of the digital signature format. This means that the design professional in responsible charge is the one to verify, certify or elevate a design solution to the level of binding legal status by inclusion of his digital signature.

Since there can be any number of versions for a particular design solution, it is the digital seal which should communicate to all stakeholders a binding final version. This effort, to present a practical deployment strategy for digital signatures and digital seals, has the potential to bring the industry closer than ever to buildings and structures coordinated comprehensively in both design solution and regulatory compliance.

Even today our perception is that of test writing, the “pencils down” approach that assumes a halt to document development only followed by formal revision to “previously approved” documents. The same can be said regarding requests for information or proposal and the communication of that information from the design professional back to the field; the digital seal establishes a confidence in all documents exchanged and communicated from day one.

- Henry Kosarzycki, AIA, Wisconsin Department of Health Services
In May 2011, Steve Folk documented the massive paper savings achieved by initiating a construction streamlining project for new student housing at the University of Washington. According to his count, about 80 archive boxes and 147 trees were saved by using email to manage workflows and construction project collaboration software.²

At the time of this publication’s creation, Henry Kosarzycki, AIA and a reviewer at the Wisconsin Department of Health Services, is taking the first and simplest steps to recognizing a paperless submittal while working with the current statutes and construction industry. The paper submittal covers all documents, from plans to specifications to calculations. These documents are accepted in an Adobe® format on a read-only CD. The ink seal and wet signature required by statute is received on a paper document, usually letter size, which binds the CD with the representing seals and signatures. This method effectively reflects the traditional model of the coversheet (previously stapled).

Projects such as these are underway across the globe as green building rises in popularity. Increasingly, local counties and other jurisdictions are embarking on streamlining missions that almost always include a call for reduction of paper. At the end of so many paper chains is a dotted line waiting for the symbolic “John Hancock” to demonstrate approval, consent, agreement, or acceptance. In order for these initiatives to realize their full potential, they must be joined with a digital signature solution.

**Movement in the Industry**

Another driving force for the use of digital signatures and seals comes from the advent of increased use of digital technology within the regulatory side of the building design and construction process.

The Fiatech Regulatory Streamlining Committee has completed the first phase of its AutoCodes Project Proof-of-Concept (POC) effort, which demonstrates the ability to apply automated code checking technology to Building Information Models (BIM). This project in the coming years will further reduce the need for a paper-based system for signatures, seals, and approved construction documents. (See Fiatech website at [www.fiatech.org](http://www.fiatech.org) for more information on AutoCodes).

Chapter 2
The Problem with Wet Signatures: Archaic, Burdensome, and Costly

The Basics: Establishing Definitions

Defining a Signature
Traditionally, a signature is a handwritten depiction of someone’s name, a cursive scribble of identity, or even a simple “X” written on a document. A signature is essentially any mark on a document for the purpose of expressing authenticity. The writer of a signature is called a signatory.

Signatures serve two related functions:

1. Providing evidence regarding the origin of a document (a person’s identity).
2. Providing evidence of the intention of that person with regard to the document.

The purpose of a signature on an agreement is not solely to provide evidence of signatory identity, but also to provide evidence of the signatory’s informed consent. Indeed, in business, many functions are derived from signatures. Common reasons include signing to express approval, acceptance, acknowledgement, or agreement. As in other industries, engineering-related businesses have distinct and fundamental uses of signatures. Specific to the AEC industry, for example, design professionals may sign to express ownership, source, or custody of technical documents including drawings, reports, or calculations for projects, studies, estimates, designs, or analysis.

Another function associated with a signature is evidence of the integrity of the signed item. Conventionally, the media carrying the signature, whether plain paper, an embossed seal, or a wax stamp, are assumed to provide some level of integrity by showing any attempted tamper or alteration.

Defining a Professional Seal
A professional seal is evidence of professional accreditation that conveys the undertaking of an independent and successful examination or verification of one’s education, experience, and skills.

In engineering-related businesses, the seal is applied to a document to express the fact that the design professional (or their company) has the competency and the legal authority to take responsibility for any work to which the seal is affixed. The seal is assumed to convey that the design professional is competent, their work meets regulatory requirements, and the design professional or their company is assuming liability for the work product.
Professional seals can take the shape of an actual circular seal, applied by a crimping or rubber-stamp device, or inserted into an electronic document as a graphical representation of the ink seal. In some cases, professional accreditation is demarked simply by a license number; no visible seal is affixed to the document.

**What is the Problem with Pens?**

Design firms are awash with a wide variety of technology options, all promising fast project delivery and even faster return on investment. From 3D modeling to 5D BIM to the latest product life-cycle management (PLM) deployment to fully integrated project management software, these technologies transform cumbersome workflows into fast electronic ones to help firms move faster, with more efficiency, and to save money.

As much as these technologies promise electronic workflows, however, the documents and projects they benefit often end up in the physical realm—printed and plotted—only in order to obtain signatures and at times to be stamped with a design professional's seal.

Printing documents and drawings for reviewing, code checking, or submitting is a waste of paper, time, and money. Other problems related to submittals are verification of the signature and seal of the design professional in charge, confirmation of the date of submittal, or the most recently approved design solution.

To understand how to address wet signature problems adequately, we must first understand why it exists and what factors are motivating forward-thinking firms to address the problem once and for all.

**How Big is This Wet-Signature Problem?**

The size of the problem depends on the company, the industry, and the region of the world in which a company operates. As an example, a company might have a strict quality-check process that relies on the signature of an employee to verify, ensure, and take responsibility that examinations were carried out. This quality-check process occurs repeatedly and the need for signatures is high. In another example, a local regulatory might require a licensed professional to sign documents submitted for official records, building permits, or planning purposes. Every time documents of these types are submitted, they must be signed and/or sealed by licensed professionals. These two examples illustrate the diverse needs for signatures and highlight the nature of signature-dependent processes to be both recurring and numerous.

All of the reasons previously mentioned (including the cost of printing and plotting on paper, the paper itself, and the time to route documents from one location to the next) are
factored into the real costs of wet signatures. Additionally, the number of signatures required and the sequence in which they are required adds to the overall cost of signing documents with a pen.

To better demonstrate these costs, Figure 1 compares a typical workflow using wet signatures with digital signatures. The workflows are quite similar, except for three major differences:

1. Printing the drawings a final time only for signing.
2. Delivering the drawing set or having people come to the drawing set for signing instead of electronic notification.
3. Scanning the signed drawings for electronic issue.
1. Drawing generation and development by project team

2. Final checking process is carried out by the assigned checker (reviewer) with typically a check print yellowed off a drawing history file that contains all design information and history.

3. In 3a the drawing is printed for wet signatures. In 3b the drawing is either converted to PDF format or left in the native file format for signing electronically.

4. In 4a wet signatures are applied one at a time by the appointed people, in this case we are showing the Author or Original Designer, Checker, Engineering Manager and Project Manager. In 4b digital signatures are applied either one at a time or all at once in a batch process.

5. In 5a drawings are delivered for signing or signers come to a designated place. In 5b an e-mail, text message or phone call can be used to inform them the drawing are ready for them to review and sign electronically.

6. Drawings are scanned if they are to be issued electronically with the wet signature or copied if issued by courier.

7. In 7a drawings are issued electronically through e-mail or portal. If by courier the transmittal and drawing are bundled up and taken to the mail room for courier pickup. In 7b drawing are issued electronically via e-mail or portal.
These three differences contribute to the majority of the cost savings in going from wet signatures to digital. Cost items that can be attributed to wet signatures include:

- Printing costs
- Time to get multiple signatures in sequence
- Time delays due to availability of individuals
- Scanning costs
- Uploading costs back into an Electronic Document Management System (EDMS)
- Shipping costs if scanned documents are not of the required high-resolution or clarity or if the regulatory body will not accept electronic copies
- Storage costs of originals if scanned versions were issued.

The sample cost analysis provided in Figure 2 incorporates the above cost and illustrates the significance of the problem. Derived from three different projects in one engineer-procure-construct (EPC) firm, this example shows how the cost of wet signature approvals can approach $80 per drawing. If a typical project contains 5,000 to 12,000 drawings, it is easy to see how signing with a pen contributes to high project costs.
## Cost of Wet Signature Approvals

<table>
<thead>
<tr>
<th></th>
<th>PROJECT A</th>
<th>PROJECT B</th>
<th>PROJECT C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering Drawings</td>
<td>11987</td>
<td>12533</td>
<td>7545</td>
</tr>
<tr>
<td>Engineering Drawing Transmittals</td>
<td>5213</td>
<td>1310</td>
<td>2277</td>
</tr>
<tr>
<td>Average Drawing/Transmittal</td>
<td>8.2</td>
<td>8.8</td>
<td>10.5</td>
</tr>
</tbody>
</table>

**Cost of Wet Signatures (Assume $100/Hour Employee Time)**

**Printing**:  
\[ \text{PRINTING} = \frac{5213 \times 8.2 \times 2}{100} = \$854.932 \]

**Obtaining Signatures**:  
\[ \text{OBTAINING SIGNATURES} = \left( \frac{40/60 \times 5213 \times 0.2 \times 2}{100} \right) = \$69,506 \]

**Scanning**:  
\[ \text{SCANNING} = \left( \frac{12/60 \times 8.2 \times 5213 \times 2}{100} \right) = \$854.932 \]

**Capturing**:  
\[ \text{CAPTURING} = \left( \frac{3/60 \times 8.2 \times 5213 \times 2}{100} \right) = \$213,733 \]

**Storing**:  
\[ \text{STORING} = \left( \frac{5213 \times 8.2}{80} \right) = \$40,181 \]

**Total Cost**:  
\[ \text{TOTAL COST} = \$1,263,845 \]

**Average Cost per Drawing**:  
\[ \text{AVERAGE COST/DRAWING} = \$105.40 \]

**Average Wet Signature Approval Cost per Drawing = $80.00**

---

**Footnotes**

1. Data is taken from existing projects at a large EPC firm.
2. Assume average paper size is A2 (conservative) and 8:1/plot.
3. To expedite the approval process, the design coordinator places the drawings in a room and fetches the approvers. He normally waits while they approve the drawings. This takes about 60 minutes on multiple approvals for a set of drawings. This time-consuming task will occur only on the first official release which is about 20% of the transmittals.
4. Cost of scanning, renaming files, reducing file size in Adobe, and adding as a version to DM is assumed to take 12 minutes for each drawing.
5. It takes DC 2 minutes to capture/compare/update drawing title block information in DM.
6. Office space for paper approval copies: $75.20/plot for 20 years. On tube can contain 80 drawings.
7. In general, average cost/drawing is a function of approval matrix (more approvals are required for certain processes) and number of drawing revisions.
**Why Are Paper Printouts Still Being Used?**

Despite advanced technology and the creation of documents in a digital format, paper is still being used for printing and plotting. In an all too familiar workflow, documents are printed, signed, and then scanned back into a digital format for archiving or for attaching to reports. Even with mobile technology and on-site computers, documents and large format drawings are still being printed again for reference.

As today’s project schedules become increasingly compressed, paper is an unnecessary hindrance on project efficiency. With firms’ multiple design centers generating information electronically, information must be able to travel within and outside the firm, whether to clients, regulatory bodies, or simply to other branches. Paper makes this an onerous process. Signing requirements vary from region to region, but most if not all companies have an internal quality assurance process that requires sign-off, frequently with a specific hierarchy of signatories.

Plotting, gathering people around a table to sign paper plots, and then scanning the plots for issue simply does not align with today’s compressed schedules and multiple work centers. So why are we not signing the electronic files *electronically*?

**Context and Inhibitors in Converting from Paper to Electronic Signing**

Signing requirements vary, depending on factors within a particular company as well as on the regulatory environment in which they exist. In some regions, signatures by licensed design professionals are required by regulatory bodies. A professional seal also must be affixed. In other cases, a design professional may not be required to sign and/or seal a document. Regardless, many companies will have their own internal processes requiring a series of signatures. Internal processes can include various checkpoints: verification of certain criteria, assurance that the document is fit for its purpose, and/or that the document meets project requirements.

Such fluctuations in signature and seal requirements complicate signature-heavy processes. In addition, multiple signatures required in sequence are time consuming, can lead to bottlenecks in project schedules, and slow down document flow between multiple work centers.

Another hurdle can be traced to regulatory bodies firmly rooted in generational and experienced-based paradigms. Current paper-based practices highlight the future potential of greater compliance and accuracy in built solutions. For processes and individuals requiring paper submittals, those submittals effectively fall out of date shortly after printing. The argument can be made regarding an electronic version, but the subtle difference is found where industry departs from the regulatory requirement. The
regulatory model requires submittal of an absolute hard copy, physically handed off only to be unrolled and reviewed; the construction industry continues to share and exchange non-paper representations of the same project. This begs the rhetorical question: Which version is not only the latest but also acceptable under the current approval or permit?

Because these are the current operating procedures and employees are familiar with them, the idea of converting from a paper-dependent signature process to an electronic one can stir up concerns. Some are psychological fears, others are based on force of habit, and others are rooted in a lack of understanding of the technology’s deployment.

Concerns are diverse and include:

- Fear of the new system.
  - Loss of control or decision-making power.
  - Loss of signatory’s mindfulness: concern over automation without deliberate thought.
  - Generational: unfamiliar with technology and reliant upon existing methods.
- Preference for paper: tactile fixation for paging through documents.
- Loss of easy readability.
  - Using a limited-view screen for details, but missing larger issues.
  - Difficulty in reviewing multiple documents side by side.
- Uncertainty of how the technology fits in with other parts of the workflow.
  - Unsure of necessity to get complementary solutions to convert.
  - Unsure of how to carry out electronic document review processes.
- Lack of understanding regarding document storage.
  - Unsure of how to carry out digital archiving systems.
  - Unsure of compatibility with existing programs such as Documentum™ or LiveLink™.
  - Uncertainty on the part of regulatory bodies regarding how copies of submittals are retained.

In order to successfully effect change, these concerns must be addressed appropriately. Companies will need to carry out thoughtful educational campaigns and relevant training sessions to introduce the technology to employees.

Suggested tactics for addressing the above list include:

- Company-wide announcements in advance of the technology deployment.
- Demonstrations of the system to be deployed with opportunities to ask questions and make feature requests.
- Awareness activities to address different working groups’ concerns.
• Adequate training sessions for educating employees on correct usage, before and after deployment.

Proper planning, education, advocacy, and exposure to the selected technology will all aid in abating users’ concerns.
Chapter 3
The Solution: Keeping an Otherwise Electronic Process Electronic

Reducing Paper Contamination

Today, work processes are paper based. Wet signatures provide proof of acceptance at each stage of the work process. Unfortunately, as industry implements electronic workflows, paper-based wet signatures become a sticking point. Electronic documents requiring proof of acceptance via signatures must be printed, signed, and re-entered digitally. Paper causes friction in this otherwise electronic workflow, thereby hindering many of the benefits that are possible: improved response time, better record retention, reduced paper filing, increased efficiency, faster output, and others.

Magnifying the problem is the signing of multiple documents, which often is required. Frequently, the signatories are located remotely. Routing time is needed to obtain proper signatures. In addition, paper must be physically stored. Once signed, paper documents become “documents of record” and must be retained and protected to serve their purpose. This requires infrastructure: storage, protection, maintenance, access control, and eventually, disposal to control storage costs. Search and retrieval costs for documents of record can be substantial.

Electronic workflows promise much faster processes if they are entirely electronic. Mixing paper with electronic workflow results in inefficiencies and provides minimal if any improvement in time required to issue documents. However, once the need for paper is eliminated, the friction is reduced and speed is increased.

Digitally signed documents offer faster cycle times for issuing documents while still maintaining the control and traceability of paper-based workflows. Digital documents are more efficient to store, maintain, protect, trace, and search. To counter the paper-based friction of wet signing, digital workflows should be coupled with digital signatures.

Direct Benefits of Digital Signatures

The digital signature solution provides a verifiable electronic process that replaces the need for wet signing documents by hand. The benefits are:

- The ability to sign multiple documents efficiently.
- The ability to sign in sequence when required or in parallel, providing flexibility.
- The ability to sign from anywhere in the world without degrading the quality or clarity of the document due to scanning (as is the current case with wet signed drawings).
• Strengthens the validity/verification of internal quality processes required to be undertaken and completed as per the project procedures by having someone signing their name rather than having it applied electronically in a box by the CAD operator, without impacting productivity to any significant degree.
• Allows the signing intent to be attached to the digital signature.
• Allows electronic forwarding, thereby minimizing costs, improving scheduling, and providing receipt of confirmations (if using EDMS). Wet signed drawings must be couriered or scanned.
• Reduces costs to the project and client.
• Reduces the time/duration in the issue process of these documents improving project schedules.

The result of the above benefits increases project efficiencies and reduces project schedules concurrently.
Chapter 4
Digital Signature Primer: Understanding Digital Signature Standards and Technology

What Must be Considered for Signature Automation?
Automation means applying signatures to digital documents, drawings, or records. Such signatures need to maintain the same evidence as their paper-based counterparts, i.e., proof of:

a) signatory identity.
b) signatory intention.
c) document and signature integrity.

A Standards-Based Approach
Fortunately, a set of standard information technology techniques makes the translation and effectiveness of these elements possible for digital documents. These standard techniques are broadly known as public-key infrastructure (PKI). Public key techniques (known as the Diffie-Hellman Key Exchange) were first developed at Stanford University in 1977 by Whitfield Diffie and Martin Hellman. About a year later, an advancement known as the RSA Algorithm directly enabled digital signatures. The RSA Algorithm resulted from joint efforts between MIT and the Weismann Institute by Ron Rivest, Adi Shamir, and Leonard Adleman.

Since their invention, these techniques have undergone intense academic and industry peer review in an attempt to find vulnerabilities and finally express digital signature techniques as open, common information technology standards. Today, the digital signature technique has been broadly ratified and adopted in global standards from the National Institute of Standards and Technology (NIST), International Telecommunications Union (ITU-T), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards bodies.

This publication references the NIST designation for digital signatures. It should be noted that all of the above standards bodies follow the same digital signature technique and all provide profiles that ensure interoperation (signature recognition) across geographies.

Under NIST, the standard designation is NIST FIPS PUB 186-3 Digital Signature Standard (DSS), and it’s supporting standards: NIST FIPS PUB 180-3 Secure Hash Standard (SHS), and ITU-T Recommendation X.509 (or IETF RFC 3280) Identity Certificate Standard.
The Digital Signature Standard (DSS) specifies algorithms for digital signing, including the RSA Algorithm. It describes the programmatic technique for applying signature keys for the purpose of generating or verifying a digital signature. A digital signature is represented as a string of canonical or distinguished bits, meaning the string has the same representation no matter what application or computer is used to examine it. A digital signature is computed using a set of rules and a set of parameters that allow the identity of the signatory, and the integrity of the document, to be verified. Signature creation uses a private key to generate a digital signature; signature verification uses a public key (that is mathematically related to the private key that makes the signature). Each signatory possesses a private and public key pair. Public keys may be known by the public (everyone); private keys are kept secret and known only by the signatory. Anyone can verify a standard digital signature by employing the signatory’s public key. Only the user that possesses the private key (the signatory) can generate a digital signature.

The Secure Hash Standard (SHS) refers to a hash algorithm and the hash value it produces to be used in the signature generation process. It is used to obtain a unique digital fingerprint (a hash) of the document to be signed. The hash is a unique condensed version of the document, usually 160 or 256 bits in length. This is the primary integrity check used to detect document tampering after a digital signature has been applied. Practically speaking, no two documents will ever have the same hash value.

The Identity Certificate Standard (X.509 v3) refers to an identity certificate and provides a detailed description of the certificate format and its optional extensions. A certificate binds a signatory’s identity to their public key. A certificate contains the Signatory’s Name, Signatory’s Public Key, Validity Period, and Issuer’s Name and Issuer’s Signature. The certificate is used to identify the signatory.

The private key, document hash, and certificate are all used as input parameters to the functions that generate the digital signature. The private key is used to calculate a cryptographic operation over the hash. This operation, involving both the private key of the signatory and the hash of the document, creates a strong binding between the signature and document. The signatory’s certificate is also used as an input to the signature generation process to provide a strong binding between the signature and the signatory. The result is a strong binding between signatory and document. The technique for creating a standard digital signature is illustrated below.
This binding cannot be easily denied, and any tampering of the document or signature will be obvious.

The digital signature (which includes the document hash and signatory ID certificate) is usually embedded in the signed document. Therefore, everything needed to verify the signature and document travels with the document and is available to anyone that wishes to examine signature or document authenticity. An examiner verifies the signature by using the signatory’s public key (contained in the signatory’s certificate) and the same standards, e.g., the hash function that was used in making the signature. Verification of a digital signature provides the strongest and most effective proof of signatory’s identity, signatory’s intent (when expressed)\(^3\), and document integrity.

Most software vendors follow these standards to make their applications digital signature aware. That is, when implemented within an application by a software developer, these standards provide the functions that allow application users to digitally sign documents and also to digitally verify those signatures.

**What are the Direct and Indirect Benefits of a Standard Digital Signature Approach?**

Standard digital signatures are superior to electronic signatures in many ways. “Electronic signature” refers to a broad and inconsistent set of nonstandard proprietary approaches. Proprietary techniques are risky from the viewpoint of durability (e.g., Will the vendor that supplies the technology survive? If not, how can signed documents in a records archive be verified? Can others recognize a signature without buying the same solution?) and vulnerabilities to forgery and tampering. Among regulated businesses, proprietary approaches are no longer acceptable. Digital signatures by contrast follow a public standard.

The digital signature standards are openly vetted and peer-reviewed by experts for vulnerabilities and are improved over time. This consistent reviewing ensures that

\(^3\) While the digital-signature standard does not directly address proof of signatory’s intention, some standard off-the-shelf solutions provide features that allow the signatory to express their intent for signing.
solutions that implement and comply with the standard techniques are not only safe to use, but will be durable over time.

The digital signature standards prevent vendor lock and vendor gridlock. Vendor lock refers to a single source for the technology. Should that one vendor/source go out of business, its customers will suffer from a lack of support and ability to improve/extend the solution. Vendor gridlock refers to one customer (you) purchasing a signature product and then having to wait for everyone that you work with (i.e., customers, partners, regulatory agencies, and others) to also buy from that same vendor before your signatures can have effect outside of your organization (i.e., your signatures can be verified by those outside of your organization). A standard eliminates the issues of vendor lock and vendor gridlock.

The digital signature standards are already implemented or supported to some level by most off-the-shelf productivity applications. Such applications are already ubiquitously used for digital documents, drawings, forms, content authoring, content management, and workflow. Thus, there is no need to develop original solutions. In this way, an enterprise/agency can realize economies from leveraging the solutions already purchased and installed or by purchasing off-the-shelf solutions that support the standards. Today many useful, off-the-shelf applications support the digital signature standards to varying degrees, including: Adobe Reader®/Acrobat®, Agile Frameworks AgileStamp™ and MetaField™, ARX CoSign®, AutoDesk® AutoCAD, Bentley Microstation®, Microsoft Word® and Excel®, Outlook®, SharePoint®, IBM Lotus®, Nintex®, and many others.

The digital signature standards ensure interoperability between different vendor solutions. For example, a digital signature made on a PDF using ARX's CoSign® solution can be verified by the free Adobe Reader®, likewise a CoSign® signature made on an AutoCAD® drawing can be verified by AutoCAD®; and a CoSign® signature made on MS Word® or Excel® documents can be verified by MS Office®.

______________

4 Most applications that support the digital signature standard do not provide a complete digital signature solution. See Appendix B.
Chapter 5
How-To: Practical Strategies in Application, Deployment, and Employee Use

How are Digital Signatures and Digital Seals Used in Practice?

Just as an individual would pick up a pen and sign a paper document, so can he or she digitally sign documents in electronic form. Some of the engineering-specific applications of digital signatures are as follows:

- Signing and sealing drawings and designs
- Signing reports
- Signing inspection documents
- Approving designs
- Submitting design calculations
- Engineering change orders
- Archiving records and as-builts
- Estimates – damage, job
- Proposal
- RFPs/RFIs
- Bid documents
- Standard operating procedures (SOPs)
- Code compliance checking

In addition, other business processes can benefit from digital signatures. These include:

- Accounting
- Approval of expenses/reimbursements
- Contracts
- Human resources

For companies that use Electronic Document Management Systems (EDMS), deploying digital signatures and seals is as simple as installing a preconfigured add-on to an existing document management system or through special integration with the digital signature solution’s API (if the chosen solution has an available API). Microsoft SharePoint® and Bentley ProjectWise® are good examples of document management and workflow systems that support digital signatures.
What to Consider Before Deploying a Digital Signature Solution

As discussed earlier, many efficiencies and benefits can be derived from signature automation. Implementing such automation, however, requires careful consideration for the following attributes of the overall system:

- Maintaining integrity of the document, record, report, or calculation to which the signature is applied.
- Compatibility with a company's content authoring applications.
- Accessible interfaces (high level APIs) if needed for larger workflow and collaboration solutions.
- Binding the signatory to the document.
- Compatibility with your current governing policy and procedure for user enrollment and authentication.
- Control over signature privileges, digital signature credentials, and digitized seals.
- Binding digitized seals to the document and signatory.

Maintaining Document Integrity

Digital signatures carry an inherent integrity for every object to which they are applied. This is the purpose of the hash function discussed in the previous section. The hash value is the document’s integrity check and is part of the digital signature. It is hypersensitive to change detection, meaning if you take a document and hash it and then make even the slightest change to that document (i.e., changing a lowercase “b” to an uppercase “B”), then hash the document again, several bits in the resulting hash will have flipped in value indicating a change or tamper.

With this standard technique (NIST FIPS PUB 180-3), no changes will ever go undetected as the document moves from place to place. In addition, as the document ages in the archive, document integrity can always be examined.

Not all standard digital signature solutions provide convenient visual indications of integrity status. A preferred implementation example is presented on the next page. This visual indication makes it easy for any stakeholder or examiner to quickly determine the integrity of the document.
Standard digital signature solutions that comply with NIST FIPS PUBS 180-3 must also comply with NIST FIPS PUBS 186-3 to provide this durable integrity attribute. Therefore, it is important to verify that the solution complies with these standards and also that it provides a convenient visual indication of integrity status.

Some solutions allow for multiple signatures on the same document or content. Others also allow the signatories to control the scope of the information to which their signature is applied. This allows more signatory control, for example in a collaborative workflow, so that each contributor might sign only on their contribution within a shared document. For example, an Excel® spreadsheet or Word® document may have several sections. Depending on the solution, each contributor may then sign only the section to which they contributed. If someone tampers with one section, the other sections may still be considered valid. This type of sectional and independent signing allows each contributor to maintain credit for, or authority over, their contribution and at the same time protects them in case one of their collaborators tampers with their contribution.

**Compatibility with Content Authoring Applications**

Content authoring refers to the class of applications one uses to create, edit, or view documents. Compatibility means that the signatures made with the digital signature solution are applied with the specific application context in mind. That is, the digital signature solution applies signatures in a manner that the native application can recognize and verify. It also means that since no organization is using just one type of electronic content or application (meaning most use multiple applications), the digital signature solution should also support multiple applications; otherwise one may need to buy a separate signature solution for each content type. Thus, the signature solution should support all common content applications such as Microsoft Word®, Excel®, Adobe® Acrobat®, Reader®, Lotus®, AutoDesk® AutoCAD®, Bentley Microstation®, and others.

It is also important that the signature solution have backward compatibility support for these applications. For example, not everyone is using MS® Office 2010; many still use MS® Office 2007 and earlier versions of that software. The signature solution should not force the organization to retrofit or retool their user community with new applications. Those decisions should be made when it best suits the objectives of the organization. The more applications the signature solution supports, the more utility an organization will derive from its investment in that solution.

We have noted that Adobe-centric signature solutions do not allow for support of Microsoft and other applications, and Microsoft-centric solutions do not always provide convenient support for Adobe and other non-Microsoft applications. One should seek to implement a solution that is content- and application-agile so that as one increases access to a digital
signature implementation, or specific requirements evolve over time, it will be less likely to re-invest in yet another digital signature solution.

Accessible Interfaces (High Level Application Programming Interfaces or APIs)

In some cases a workflow or collaboration system may need to recognize when a digital signature is required or when a digital signature has been applied to a document. Such systems might need to recognize a signature request or a signature itself as an event in the workflow. Therefore an application programmer’s interface (i.e., a high level API) for the digital signature solution would be useful. A variety of complicated APIs is available and are used by cryptographic experts for accessing many types of cryptographic functions. If a developer or IT expert is not familiar with the details of cryptography or key management, integration under such APIs as MS® CAPI, PKCS#11®, or JCA® may be a challenge. It is recommended that the API for the signature solution be high level (e.g., an API specific and limited to digital signature features) for the purpose of accessing digital signature features and functions only. This will greatly reduce integration time and the learning curve required of any application developer.

Binding the Signatory to the Document

Inherent or built-in properties of a standard digital signature create extremely reliable and durable bindings between:

   a) signatory identity and their signature keys (known as their key pair).
   b) signatory’s signature and the specific document it is applied to.
   c) signatory’s signature, a specific seal, and the specific document (optional).

The standard mechanism for binding the signatory's identity is known as an ID certificate or more formally an X.509 v2 certificate, where its usage is marked for digital signature purposes. A certificate binds a signer’s identity to a public key.

A certificate contains:

   a) Signatory's Name
   b) Signatory’s Public Key
   c) Validity Period
   d) Key Usage Value (digital signature)
   e) Certificate Issuer’s Name

Think of the certificate as a driver's license, only in this case it is used to convey the identity of the signatory and the identity of the enterprise or government agency that issued the certificate.
While many applications are digital signature aware (that is, they can apply or verify a signature), almost none have the capability to manage signature keys or to issue or manage certificates. Take the case of Adobe® Acrobat®. It allows a user to sign and verify PDF documents and also allows a user to generate their own signature keys and ID certificates, but in an unsupervised manner. This means that any user can leverage the Adobe® software to self-declare their identity and self-certify that identity, also known as their signature credential.

Signatures made with such certificates carry little to no trust, and stakeholders who rely on them take a significant risk that increases exposure to the possibility of loss and/or other adverse or unwelcome circumstances. For an individual keeping their own records for their own use, perhaps the self-managed certificate is adequate (a personal choice). For any enterprise, agency, or business, however, the exposure would not be acceptable to their auditors, regulators, or governance departments. When any user is free to declare any identity he/she wishes, unsupervised signatures made with that identity should not be taken seriously or relied upon by others.

The way to solve this is to connect the certificate issuing and management functions with the pre-existing governance policies, procedures, and systems already established by the enterprise or agency—specifically the policies, procedures, and systems used for screening, provisioning, enrolling, managing, and authenticating users and their credentials.

A centralized Certificate Authority (CA) establishes and maintains an accurate binding between the public key pair and the attributes contained in the certificate. The CA does this according to a governing procedure and without interference from end users.

**Compatibility with Current Governing Policy and Procedure**

Today most organizations have well-established policies and procedures for provisioning and managing employees, contractors, or partners who either interact with or have access to that organization’s resources. These governing policies have been defined according to the governing (business risk) and/or regulatory (legal risk) requirements set for the organization by a governing board or a regulatory authority. Aspects of governing policy that relate to digital signatures are:

- a) The manner in which the identities of individuals are proofed.
- b) The processes for assigning their privileges (i.e., signature privileges).
- c) The method for authenticating an individual before they act on behalf of the organization (i.e., before they are permitted to sign).

The goal is to lay in a signature solution that does not cause the standard operating procedures (SOP) to be rewritten or the IT infrastructure used to enforce these policies to
be retrofitted or replaced. Central to this concept is a deployment approach that allows the translation of routine operations for user management policy into key and certificate management operations. For example, when the policy allows a new user in the system, the signature credentials for that user should be immediately provisioned; likewise, when the policy mandates a user is to be removed from the system, their signature credentials should be immediately revoked. The local policy of the domain (i.e., the enterprise or the government agency) must govern and drive the provisioning and management of its users, and therefore also those users’ signature privileges and signature credentials (keys and certificates).

Not only does each domain have established policies and procedures for user management and user authentication, they typically have in place systems by which to enforce these policies. Domain directories are usually deployed to manage the domain’s users and the authentication scheme those users must follow for accessing resources in the domain. Such systems are usually user directories like Microsoft® Active Directory®, Oracle OID®, IBM Tivoli®, or generic LDAP-enabled databases. These directories manage who is active in the domain as well as their access credentials (e.g., access credentials are usually a user name and password combination). When the user wants to access a domain resource, they must be an active user and also must login to the domain with the correct access credentials (user name and password).
Digital signature credentials are rightly viewed as one more domain resource that the user (signatory) must conditionally access per the domain's policy, and the domain (enterprise or agency) must manage. Continuity, therefore, must be ensured between the system that manages users and the system that controls digital signature credentials. An example is indicated in the figure below, where the system used to manage signature credentials “listens” to the system used for enforcing user policy. When a new user is added to the domain, that user is detected by the signature credential management system and its keys and certificates are then issued. Likewise, when a user is removed from the domain, the signature credential management system is still “listening” and immediately revokes that user's signature credentials. This results in the best control characteristics possible for signature privilege management. Control remains with the domain authority; signature-privilege provisioning and, more importantly, signature-privilege revocation are immediate. Very tight control can then be realized by the organization that permits digital signing by its users.

The signatory (user) must control the use of his/her signature credentials. The digital signature system also must challenge the user with an identity check each time they request to use their signature credentials. Once again, the domain (enterprise or government agency) has established both a policy and a scheme for user authentication (an identity challenge); thus, the digital signature system should recognize and reuse this scheme to maintain continuity between the signature capability and the policies by which user authentication is governed. In many cases the identity challenge is a user name and password combination enforced by the domain directory. Other schemes use dedicated...
authentication servers that employ one-time password tokens (e.g., YubiKey® or SecurID®). Regardless of the specific authentication scheme, the signature solution should be capable of leveraging it without forcing the expense of deploying a new authentication scheme for accessing only the digital signature resource in the domain. The figure below depicts options for user authentication based on local policy. The schemes depicted include user name plus password or user name plus one-time password token (2-factor) authentication.

![User Authentication for Digital Signature Creation](image)

**Control over Digitized Seals**

Unlike signatures, seals do not have an associated information technology standard that addresses their conveyance in digital or electronic form. When digital seals are applied under a standard digital signature, however, they can be used to convey the same properties in electronic form or content as their paper-based counterparts.

Leaving control of enrollment or an over-signature privilege solely up to an individual is a risk most organizations do not accept. Therefore, the same departments established for individual screening (e.g., the human resources), privilege assignment (e.g., a specific department head), and enforcement (e.g., the IT department) should all continue in those roles under their currently established governing policies and procedures—little to nothing should change here just because the organization is adopting digital signatures.
Also, once an individual has been provisioned and assigned signature privilege, they should have control over when to apply their specific signature credentials to any specific document or work product.

The above guidelines must be extended to the management and use of digitized professional seals. That is, the local policy determines when a user/signatory/engineer is provisioned with a digitized seal within their domain. Furthermore, it is recommended to combine the enforcement of managing digitalized seals with the same enforcement policy and system that manages and controls access to digital signature credentials. Digitized seals are to be treated as one more credential (or domain resource) that is afforded the same protection and controls as the digital signature credentials.

In addition to storing and managing digital signature credentials, the digital signature solution should consider storing and managing digitized seals as depicted below.

The organization should have very tight control over when to revoke all privileges not only for signing but also for use of digitized seals. The tighter control the organization has over this aspect, the lower its risk profile becomes. Likewise the engineer (signatory) should have the same control over when all of his/her credentials are used. Combining the access and secure storage of the signature credentials with digitized seal credentials allows this extension of controlled use/access and protection to the digitized seal.
**Binding Digitized Seals to Document and Signatory**

The standard digital signature is to be used for binding together document and digitized seals and, of course, the signatory. Only one step is added to the signing process to include the digitized seal: the engineer-signatory is allowed to choose the appropriate seal at the time of signing. The seal thus is added in the visible signature block and is protected with the same standard integrity check (the hash) as the document. So doing causes any tampering with a digitized seal to be reliably detected. Furthermore, a digitized seal combined with a digital signature carries this active integrity check, which is not available with a digitized seal alone.
Implementation and Employee Use

As mentioned in the section titled “Context and Inhibitors in Converting from Paper Signing to Electronic Signing,” user experience plays a large role in any change. Addressing these concerns through a robust deployment plan will play a significant role in ensuring employee adoption. The process itself must appear simple and flexible and be capable of providing a tangible benefit.

A well-conceived implementation process will usually be comprised of a few steps:

1. Introduction – Introduce that a change is coming as early as possible. Garner users’ interest, initial feedback, and questions to address.
2. Education –
   a. Detail what is being deployed. Describe what the technology is, why it is coming, and the benefits for the user, the company, and the clients.
   b. Describe where the new technology fits in with the company or with the company’s overall strategy for technology.
   c. Raise awareness on what changes will happen as a result of deployment. Identify who will be affected. Describe the vision for how digital signatures will be used in the company.
   d. Directly address fears or other obstacles preventing or inhibiting people from adoption.
3. Implementation – Whenever possible, select a well-timed opportunity to implement the process. The sooner some short-term wins are achieved, the better for user adoption.
4. Conduct training as close as possible to the time of implementation.
5. Follow up with surveys to monitor adoption of the change and gain feedback for future improvements.
Chapter 6
Summary

Automation strategies that are scalable and that consider how design professionals work are needed in order to drive the industry forward while keeping up with larger technological advances. The recommendations for digital signature and digital seal deployment describe in this guide emphasize a standards-based approach. This approach takes into consideration existing policies that govern user-management, authentication, privileges, and the existing application infrastructures already deployed to enforce these policies. It offers more access to automated processes and workflows for the engineering industry than alternative, fragmented, proprietary, or ad-hoc approaches.

Following these guidelines can lead to:

- Affordability—there is no need to retrofit or re-engineer policy or system infrastructure.
- Control—lower risk for the implementing organization because the organization remains in control.
- User protection—better protection for users due to standard mechanisms employed for information integrity.
- User adoption—better user adoption because users can continue to use the applications with which they are most familiar.
- Robustness—durability over time because its leverages open standards.

The members of this committee hope that readers will both internalize the benefits of digital signatures as they are laid out in this guide and consider adopting the technology as set forth in this practical deployment strategy.
Appendix A
General Legal Statutes, Local Guidelines, Practices, and Regulations

Fiatech is providing the following information for reference only. Fiatech is not a law firm, is not providing legal advice, and is not acting in the capacity of lawyers or legal advisors. As such, it makes no warranty, expressed or implied, concerning any interpretation of laws and regulations as presented here, including their continued efficacy or the content of the websites cited below.

U.S. Statutes and European Legislation

In the U.S., two statutes give legal force and effect to digital signatures: the Uniform Electronic Transactions Act (UETA) – 1999 (State level); and the Electronic Signatures in Global and National Commerce Act (E-Sign) – 2000 (U.S. Federal level).

In the European Union (EU), a similar statute was put in place in 1999: the EU Directive for Electronic Signatures. That directive also gives legal force and effect to digital signatures.

UETA says under Section 7, Legal Recognition of Electronic Records, Electronic Signatures, and Electronic Contracts:

a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

c) If a law requires a record to be in writing, an electronic record satisfies the law.

d) If a law requires a signature, an electronic signature satisfies the law.

Forty-six U.S. states (plus the District of Columbia, Puerto Rico, and the Virgin Islands) have adopted UETA as is. Illinois, Georgia, New York, and Washington have a modified version of UETA or have other statutes pertaining to electronic transactions (GA: Ga. Code Ann., § 10-12-1; IL: 5 ILCS 175/1-101; NY: NY CLS State Technology § 301 et seq.; WA).

E-SIGN, the U.S. Federal Act, governs disputes controlled by Federal law. E-SIGN mirrors various provisions of UETA (which preceded it) and states that a signature may not be denied legal effect, validity, or enforceability solely because it is in electronic form. In other words, an electronic signature is treated no differently under the law than traditional paper-based written signatures.

Since E-Sign’s enactment in 2000, U.S. courts have routinely admitted electronic signatures written opinion without analysis or comment. In a sense, the statute is doing its job by obviating the need for any court to think twice about whether an electronic signature could be admissible (assuming it met traditional rules of evidentiary procedure).

- The directive indicates standard digital signatures are required, without explicitly saying so (wanting to appear technology neutral).
- All EU Member States have adopted this directive with local legislation, as of 2003.
- EU Member States are not allowed to add additional requirements to those in the directive.

**Other International Legislation Approaches**

Over the past few years, many regulatory initiatives have taken place and, much as they reflect different assumptions on electronic signatures legal status and future, they can be classified into three categories:

1. **The Minimalist Approach**
   - The minimalist approach is adopted by the U.S. and Australia. This approach does not address specific techniques and therefore intends to be technology-neutral.
   
   When a dispute arises in countries following the minimalist approach between parties related to electronic signatures, the integrity of electronic signature must be shown to be reliable in a court of law. This is a similar legal approach for normal handwritten wet signatures when in dispute.

2. **The Digital Signature Approach**
   - The digital signature approach is adopted by Singapore, Germany, Italy, India, Chile, Japan, and the Netherlands. This is a prescriptive approach as it focuses solely on the establishment of a legal framework for the operation of digital signatures as well as of a reflection of formal requirements applicable in offline transactions. International regulations under this approach adopt the PKI as the approved technology of generating electronic signatures, impose certain operational and financial requirements on CAs, prescribe the liability of key holders, and define the circumstances under which reliance on an electronic signature is justified.

   In contrast to the minimalist approach and electronic signature, most countries requiring digital signatures assume digital
signatures are valid in a court of law unless the contrary can be proven.

3. The Two-Tier Approach
The objective of this hybrid method, which is adopted by the EU, is to provide time-resistant regulations by setting requirements for electronic authentication methods with a certain minimum legal power (minimalist approach) and by attributing greater legal effect to certain widely used techniques (digital signature approach). In contrast to the prescriptive approach, the two-tier approach does not specify only one technology, but leaves room for future technologies to develop and comply with extra requirements as well.

(Reference: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/)
Appendix B  
Vendors Offering Digital Signature Aware Applications  

The following vendors offer applications that are capable of applying or verifying a digital signature. This is not an exhaustive list.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Website</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td><a href="http://www.adobe.com">www.adobe.com</a></td>
<td>1-888-649-2990</td>
</tr>
<tr>
<td>Agile Frameworks</td>
<td><a href="http://www.agileframeworks.com">www.agileframeworks.com</a></td>
<td>1-800-779-1196</td>
</tr>
<tr>
<td>ARX</td>
<td><a href="http://www.arx.com">www.arx.com</a></td>
<td>1-650-331-1123</td>
</tr>
<tr>
<td>AutoDesk</td>
<td><a href="http://www.autodesk.com">www.autodesk.com</a></td>
<td>1-800-964-6432</td>
</tr>
<tr>
<td>Bentley</td>
<td><a href="http://www.bentley.com">www.bentley.com</a></td>
<td>1-800-236-8539</td>
</tr>
<tr>
<td>BlueBeam</td>
<td><a href="http://www.bluebeam.com">www.bluebeam.com</a></td>
<td>1-866-496-2140</td>
</tr>
<tr>
<td>Gemalto</td>
<td><a href="http://www.gemalto.com">www.gemalto.com</a></td>
<td>1-888-343-5773</td>
</tr>
<tr>
<td>Microsoft</td>
<td><a href="http://www.microsoft.com">www.microsoft.com</a></td>
<td>1-800-642-7676</td>
</tr>
<tr>
<td>Oracle</td>
<td><a href="http://www.oracle.com">www.oracle.com</a></td>
<td>1-650-506-7000</td>
</tr>
<tr>
<td>SAP</td>
<td><a href="http://www.sap.com">www.sap.com</a></td>
<td>1-800-872-1727</td>
</tr>
</tbody>
</table>