An Introduction to

DIGITAL SIGNATURES

For the AEC Industry

CONTENTS

Introduction.

Many in the Architecture, Engineering, and Construction industry have already adopted digital workflows for creating drawings, designs, and other documents to increase efficiency and decrease paper usage. Despite their efforts to go paperless, many in the industry still find themselves relying on paper when it comes to applying signatures.

Since the need for signatures pops up so often in project lifecycles, printing each time they need a signature is impractical and inefficient.

Fortunately for these AEC companies, digital signatures allow them to keep their entire workflow online. Individuals can certify and sign documents as needed right from the comfort of their computers.

This introductory guide explains the role of digital signatures in the AEC industry. We'll take a closer look at the drawbacks to relying on paper, explain what a digital signature is, how they work, and offer considerations to help you choose the right digital signature solution for your company.

Let's get started.

Chapter 1.

Moving to Digital Signatures

Why go paperless?

Despite adoption of digital workflows, the AEC community still uses a ton of paper.

A typical $100m building project generates 150,000 separate documents: technical drawings, legal contracts, purchase orders, requests for information and schedules. [1]

In addition to not being very "green", relying on wet ink signatures can delay project deliverables, add significant overhead and costs, and can lead to error (due to misplaced files or document degradation from multiple print and scan cycles).

40% of engineering time is dedicated to locating and validating information. [2]

Manual reentry, due to the use of paper and electronic files in tandem and receipt of paper design changes from external organizations, has been estimated to cost $463 million during the design phase and $28 million during the construction phase. [2]
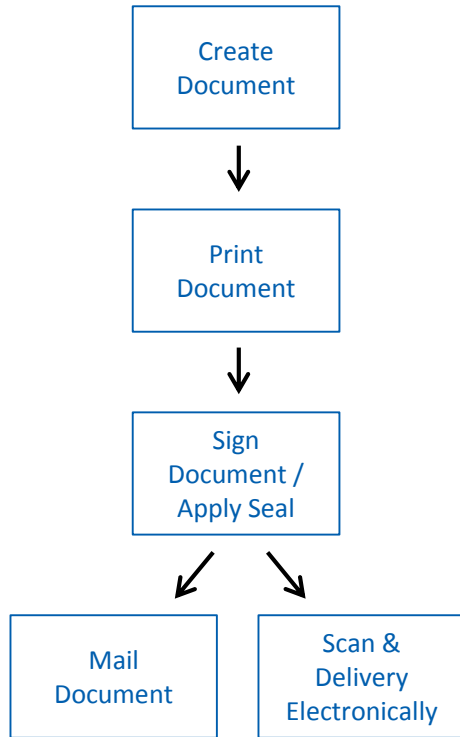
The AEC industry spends an estimated $500 million or more each year moving plans from one discipline to another via such courier services as FedEx. [3]

Printing every time you need a signature is expensive, time-consuming, and just kind of a pain to manage. So what can you do instead?

Here's where digital signatures come in. Digital signatures are the virtual equivalent of a wet-ink signature. Using digital signatures allows you to keep your files electronic throughout the entire project, saving you significant time, money, and resources.

GlobalSign®

Comparing workflows

Typical workflow for paper-based signing

```
Create
Document
   ↓
Print
Document
   ↓
Sign
Document /
Apply Seal
  ↙     ↘
Mail        Scan &
Document    Delivery
            Electronically
```

- It can cost up to 31 times the original cost to send information on paper (printing, copying, postage, storage, filing, recycling, etc.)

- High chances of fraud

- Significant time spent preparing, organizing, and archiving files

- Risk of degradation of documents after multiple rounds of printing, scanning, and signing

Typical workflow for digital signing

```
Create
Document
   ↓
Digitally Sign
Document
   ↓
Delivery
Document
Electronically
```
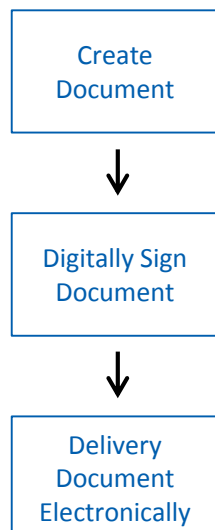
- On average, digital signatures reduce the time it takes to sign documents by 30 percent

- Create tamper-evident, timestamped, legally-binding documents

- Reduce paper waste and time spent printing, mailing, archiving, etc.

GlobalSign®

Chapter 2.

Digital Signatures 101

What is a digital certificate?

You need a digital certificate to digitally sign a document, so it's helpful to start here first. Digital certificates can be used for a variety of use cases, including SSL and email encryption, but for simplicity's sake, we'll just look at how they fit into the document signing use case.

You can think of a digital certificate as kind of a virtual passport - a way of proving your identity in online transactions. Just as your local DMV needs to verify your identity before issuing you a passport, a third party verification entity known as a Certificate Authority (CA) needs to vet you before issuing a digital certificate. Since your certificate is unique to you, using it to sign a document is a way for you to prove, "yes, it's really me signing this document."

What is a digital signature?

Much like digital certificates are the online equivalent of a passport, digital signatures are the online equivalent of a notarized signature. In this case the CA serves as the notary in terms of verifying your identity, while a trusted timestamp verifies the date and time the signature was applied.

When you apply a digital signature, a cryptographic operation binds your digital certificate and the data being signed (in this case, a PDF or other document) into one unique fingerprint. The uniqueness of the two components of the signature are what makes digital signatures a viable replacement to wet ink signatures.

Unique to the signer

Authentication – since your third-party validated certificate was used to apply the signature, recipients know it was actually you who signed it

Non-repudiation – since your certificate was used to sign the document, you cannot later claim that it wasn't you who signed it

Unique to the document

Message integrity – when the signature is verified, it checks that the data in the document matches what was in there when the signature was applied. Even the slightest change to the original document would cause this check to fail.

GlobalSign

Chapter 3.

Digital Signatures in Action

Sample signing scenario

Applying a digital signature is a very simple process. Let's take a look at a real world scenario.

Scenario: Leslie has a drawing she needs to submit to Joe. There are a number of programs that can be used to apply the signature (e.g., Adobe LiveCycle, BlueBeam, etc.), but in this example, we're going to use Adobe Acrobat. Per this project's specifications, Leslie needs to certify the document and insert her Professional Engineer seal.

There are two components to the signature process – creating the signature and validating it. We'll start with the first part – Leslie applying the digital signature.
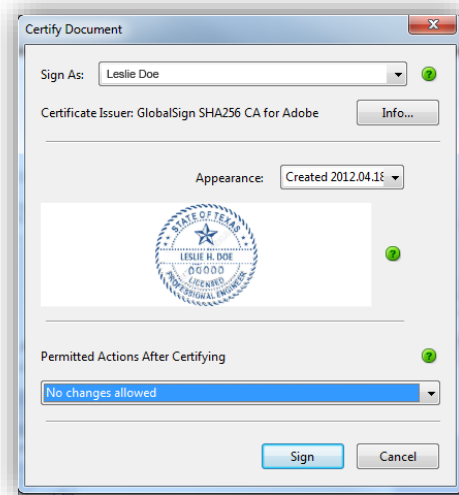
Applying the signature

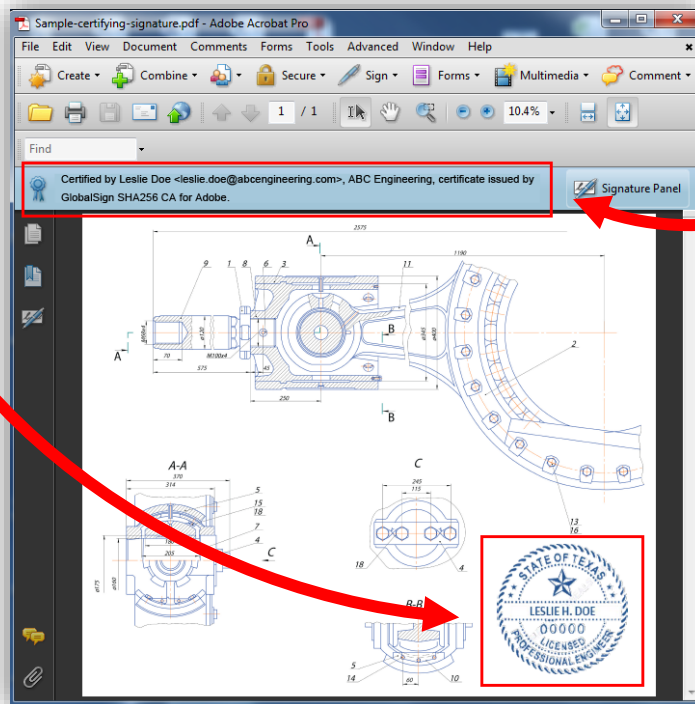These are the steps Leslie will go through to apply the digital signature.

1 Leslie opens her drawing in Acrobat. She clicks "Certify with Visible Signature".
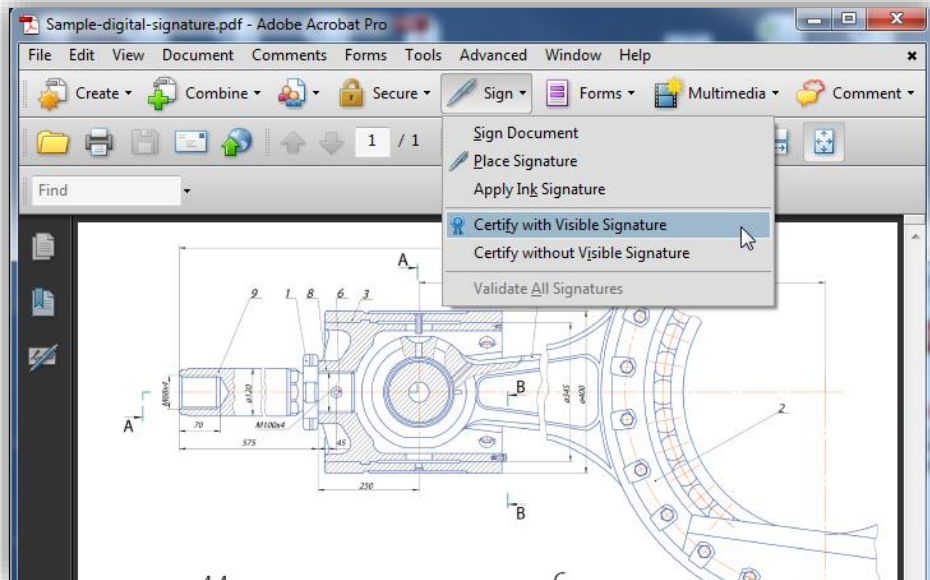
2 After she chooses where she would like the visible signature to appear, she selects the certificate she wants to use to sign the document, chooses how she wants the signature to appear (her PE seal), and disallows any changes to be made to the document after the signature is applied.

3 Finally, she enters her password and the signature is applied. The document now includes two key trust indicators - a notice at the top of the document stating that it has been certified by Leslie, whose identity was verified by a third party CA (in this case GlobalSign) and her PE seal. The document is ready to send to Joe.

GlobalSign®

Verifying the signature

These are the steps Joe will go through to verify Leslie's signature.

Note: Adobe Reader automatically verifies the signature, so Joe doesn't actually need to do anything beyond open the document in Reader. Here we'll walk you through what to look for in a digitally signed document and show you how you can find details about the digital signature.
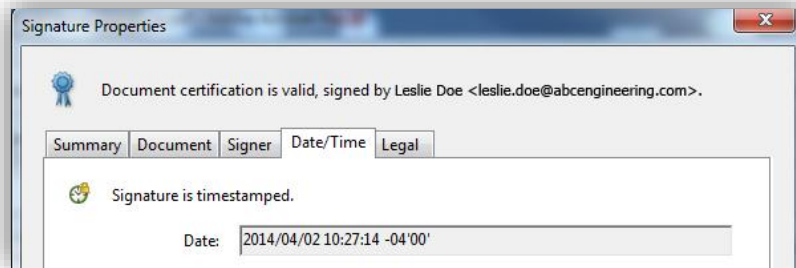
1 Joe opens the PDF in Adobe Reader and sees the same two trust indicators explained above - the notice at the top of the document and Leslie's engineering seal..
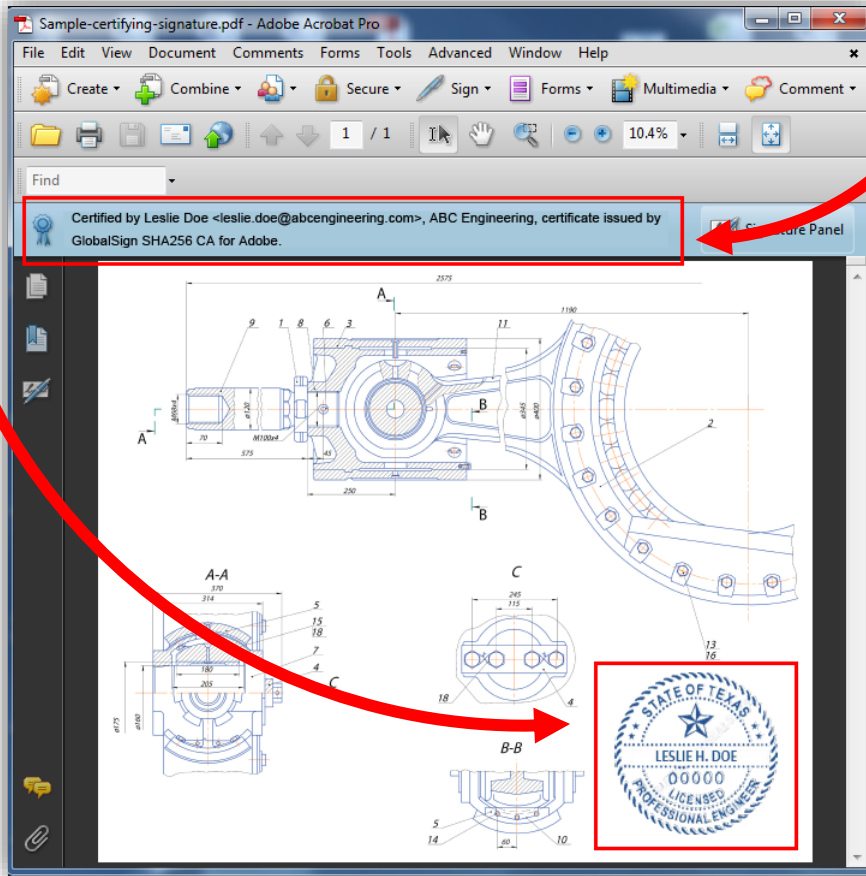
2 Clicking the seal verifies Leslie's signature and reaffirms that no changes have been made to the document since she signed it.

Signature Validation Status

Document certification is valid, signed by Leslie Doe
<leslie.doe@abcengineering.com>,
- The Document has not been modified since it was certified.
- The signer's identity is valid.

Legal Notice...   Signature Properties...   Close

Joe can view "Signature Properties" for more information, including a timestamp of when the document was signed.

Signature Properties

Document certification is valid, signed by Leslie Doe <leslie.doe@abcengineering.com>.

Summary   Document   Signer   Date/Time   Legal

Signature is timestamped.

Date: 2014/04/02 10:27:14 -04'00'

Behind the scenes of the signing process

Let's take a look at what's actually happening when Leslie signs her PDF and when Joe verifies her signature.

Applying the Signature

1 When Leslie clicks "sign" in Adobe Acrobat, a unique digital fingerprint (called a hash) of the document is created using a mathematical algorithm. This hash is specific to this particular document; even the slightest change would result in a different hash.

Leslie's
Document
Hash function
101100110101
Hash
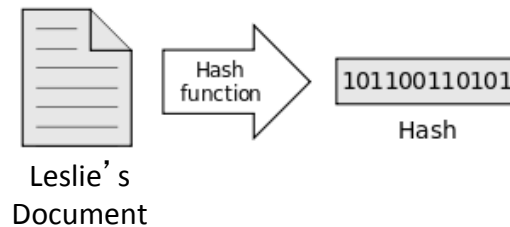
2 This hash is encrypted using Leslie's private key from her digital certificate. The encrypted hash and Leslie's public key are combined into a digital signature, which is appended to the document.
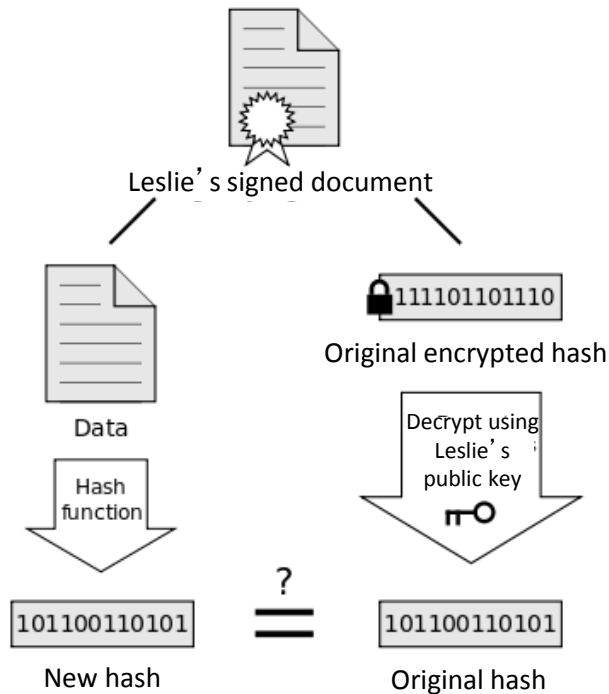
Leslie's public key
+
Encrypt hash using Leslie's private key
111101101110
Encrypted hash
=
Digitally signed document
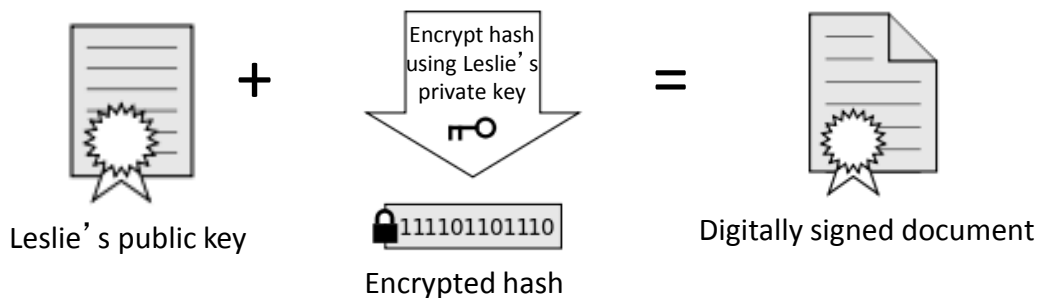
3 Leslie can now share the digitally signed document with Joe.

GlobalSign®

Verifying the Signature

1 When Joe opens the signed PDF, Adobe Reader automatically uses Leslie's public key (which was included in the digital signature with the document) to decrypt the document hash.

Reader calculates a new hash for Leslie's document. If this new hash matches the decrypted hash from Step 1, Reader knows that the document has not been altered and displays the message, "The Document has not been modified since this signature was applied."

Leslie's signed document

111101101110

Original encrypted hash

Data

Hash function

Decrypt using Leslie's public key

101100110101

New hash

?
=

101100110101

Original hash

Reader also checks the validity of the certificate Leslie used to apply the signature (i.e., that it has not been revoked) and verifies that the public key used in the signature belongs to Leslie.

The images above are from "[Digital Signature diagram.svg](#)" by [Acdx](#) used under [CC BY-SA 3.0](#).

Share This Ebook!

GlobalSign®

Other signing scenarios

We ran through a basic scenario, in which Leslie simply needed to send a certified PDF stamped with her PE seal to Joe. There are a number of options when applying digital signatures to fit your specific workflow, document type, or any applicable government regulations.

- Digital version of handwritten signature
    - Instead of a PE seal, Leslie could have included an image of her handwritten signature.

- Multiple signatures within one document
    - Leslie chose to not allow any changes to be made to the document after she applied her signature, but she could have allowed other digital signatures to be applied.

- Sign multiple pages of the same document
    - Leslie could have added her PE seal to multiple pages to the document.

GlobalSign®

Chapter 5.

Selecting the Right Digital Signature Solution

What makes an ideal digital signature solution?

Now that you know what digital signatures are and how they can significantly reduce your project costs and timelines, let's take a look at what you should be looking for in a solution.

The ideal digital signature solution must:

- Provide cost-effective digital signatures

- Be compatible with the types of documents you need to sign

- Offer easy validation of signatures for document recipients

- Be easy to use with zero or next to no resistance for all users

- Offer multiple signature options (e.g., option to include visible signatures such as PE seals of images of handwritten signatures)

- Comply with state regulations regarding the use of digital signatures for electronic document submissions

- Keep signing processes and procedures inside your organization (a solution that works locally)

- Be easily manageable in a way that best suits your internal processes

- Comply with digital signature standards (e.g., NIST, ETSI)

- Support your organization's existing policies, procedures, and technologies

GlobalSign®

Considerations when comparing solution providers

There are a lot of digital signature solutions and solution providers out there, so we've compiled some questions to keep in mind as you're researching our options.

- What types of documents do you need to sign?

- Do you need to include multiple signatures within each documents?

- How many users?

- How many signatures?

- What types of regulations does my signature solution need to meet? (e.g., Connecticut Department of Transportation requires certificates compliant with Adobe Certified Document Services (CDS))

- What is the implementation process like? Will there be a burden on IT?

- What type of training will be involved for end users?

The bottom line is there are a lot of things to keep in mind when researching solutions, but no one knows your company better than you. The types of documents you need to sign, the workflows you currently have in place, your coworkers who will need to use the solution, regulations you need to comply with - those are all unique to your company and will dictate which solution is the best fit. Every organization is going to have their own requirements and priorities, but we hope the questions above help frame your evaluation.

Conclusion.

Digital signatures are a tried and true technology that have been growing in popularity among other verticals, like healthcare, for years. With more and more states requiring them for project submissions and industry-specific document workflow solutions, like BlueBeam, making them so easy to implement, there are few reasons not to adopt them in place of paper signatures.

You know relying on wet ink signatures is expensive and time-consuming. You've been introduced to a viable alternative. You know what to look for in a digital signature solution. So what are you waiting for? It's time to kick paper to the curb and embrace digital signatures.

Got questions? We've got answers.

www.globalsign.com|sales@globalsign.com

References.

[1] New Wiring, The Economist, http://www.economist.com/node/273886

[2] Digital-Asset Management in AEC/O, Cadalyst, http://www.cadalyst.com/aec/digital-asset-management-aeco-aec-focus-column-3674

[3] Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry, Michael P. Gallaher, Alan C. O' Connor, John L. Dettbarn, Jr., and Linda T. Gilday, http://fire.nist.gov/bfrlpubs/build04/PDF/b04022.pdf

Easily add digital signatures to your documents with GlobalSign

GlobalSign's PDF Signing solution allows you to quickly and easily add certifying and approval signatures to your plans, designs, bids, contracts, and other project documents. Sign up for a free demo of GlobalSign's PDF Signing solution to see how easy digital signatures can be.
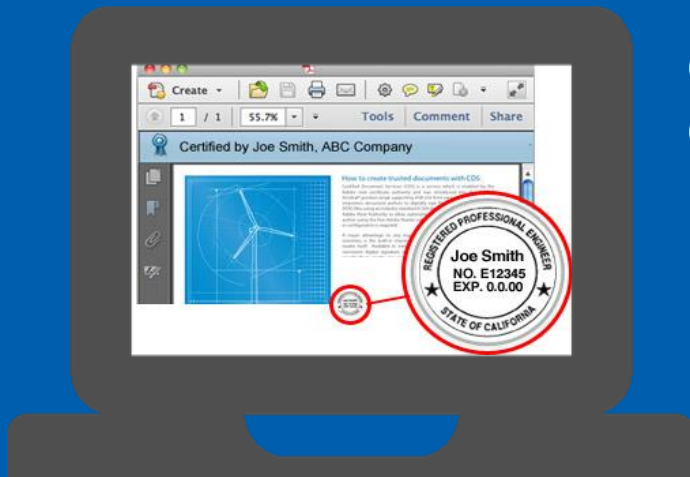
GET A FREE DEMO OF GLOBALSIGN TODAY.

[Sign Up for your Demo Today!](#)

GlobalSign®