An Introduction to DIGITAL SIGNATURES

TRUSTZONE A/S | Phone: +45 88 33 10 00 | Email: sales@trustzone.com | trustzone.com

TRUSTZONE

CONTENTS

INTRODUCTION.

Many organisations have adopted digital workflows to increase efficiency and decrease paper usage. Despite these efforts to go paperless, many still find themselves relying on paper when it comes to applying signatures.

The need for signatures pops up in virtually every department - human resources for employee timesheets and vacation requests, finance signing off on invoices and purchase orders, legal preparing contracts, sales entering new client relationships. Printing every time you need a signature is impractical and inefficient.

Fortunately, there's a better way. Digital signatures allow you to keep your entire workflow online. You can certify and sign documents as needed right from the comfort of your computer.

This introductory guide explains the role of digital signatures in the modern organisation. 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 an overall decrease in paper usage (approximately 41% according to one estimate[1]), organisations still use a ton of paper.

The average office worker uses 10,000 sheets of paper annually.[2]

In addition to not being very "green", relying on paper-based workflows 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).

Average cost per paper form (e.g., printing, distribution, mailing, collection, sorting) is $3.63.[3]

Removing paper-based processes could reduce response speed 400%.[1]

Removing paper-based process could increase staff productivity by 30%.[1]

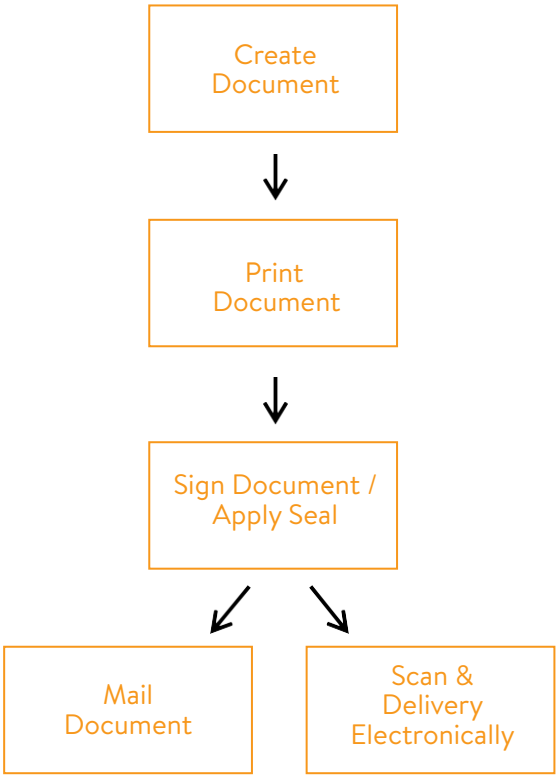
How Digital Signatures Can Help

One of the main reasons for continuing to rely on paper is the need for signatures.[4] 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?

Fortunately, with legislation like ESIGN in place, digital signatures are a legally viable alternative in most situations. Digital signatures are the virtual equivalent of a wet-ink signature. Using digital signatures allows you to keep your files electronic, saving you significant time, money, and resources.

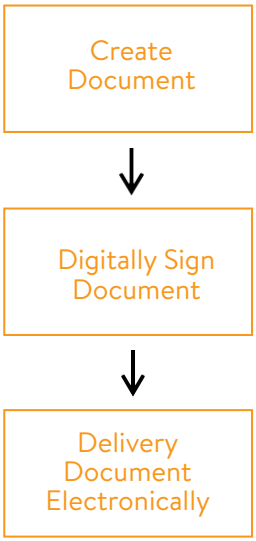
Comparing workflows

Typical workflow for paper-based signing



- It can cost up to 31 times the original cost to send information on paper (printing, copying, postage, storage, filing, recycling, etc.)[2]
- 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



- On average, digital signatures reduce the time it takes to sign documents by 30 percent[5]
- Create tamper-evident, timestamped, legally-binding documents
- Reduce paper waste and time spent printing, mailing, archiving, etc.

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 Microsoft Office 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.

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.

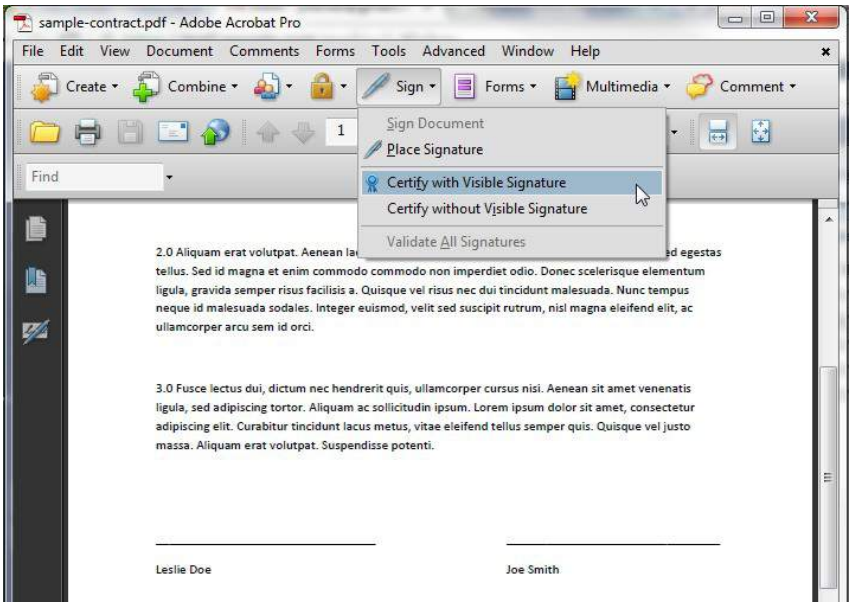
Scenario: Leslie has a contract to deliver to Joe, a new client she's acquired. Rather than printing it and physically signing, she can use a digital signature to certify the document and add an image of her handwritten signature. There are a number of programs that can be used to apply the signature (e.g., Adobe LiveCycle, custom iText solutions, Microsoft Office), but in this example, we're going to use Adobe Acrobat.

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.

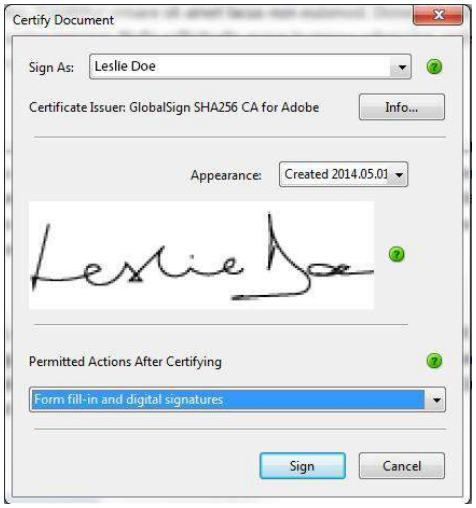
Applying the signature

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

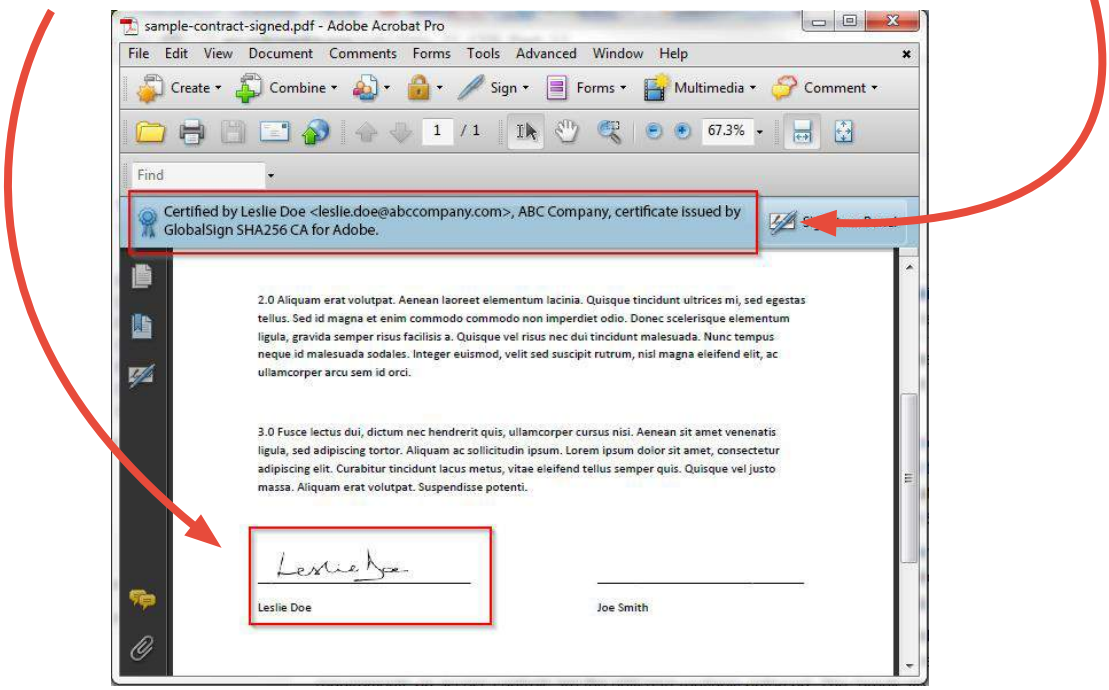
1. Leslie opens her drawing in Acrobat. She clicks "Certify with Visible Signature".



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 (an image of her handwritten signature), and specifies which changes she will allow to occur after her signature is applied. In this case she'll allow digital signatures to be added, so Joe can digitally sign as well.



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 TRUSTZONE partner GlobalSign) and the image of her signature. The document is ready to send to Joe.

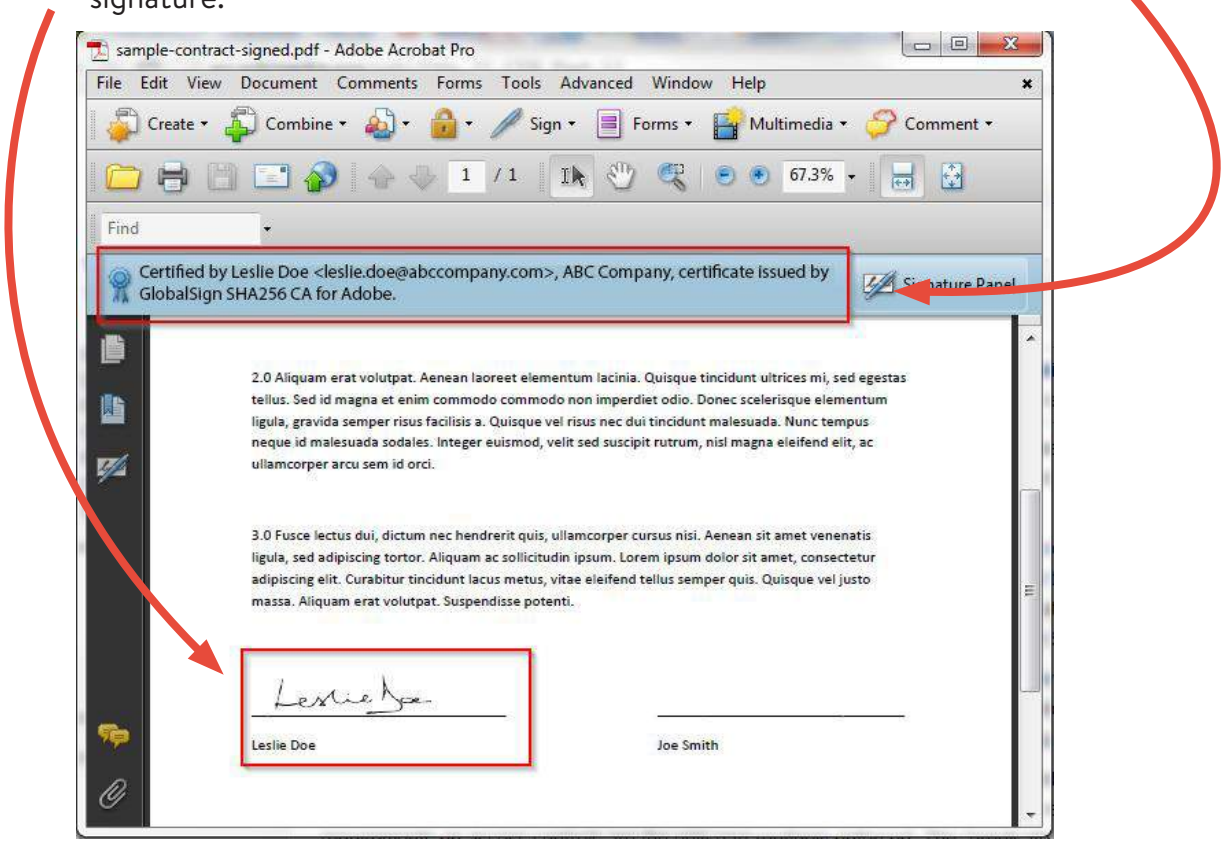


Verifying the signature

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 Adobe 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 signature.



2 Clicking the seal verifies Leslie's signature and reaffirms that no changes have been made to the document since she signed it.

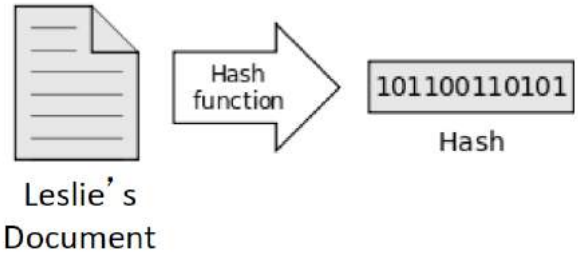
Joe can view "Signature Properties" for more information, including a timestamp of when the document was signed.

Behind the scenes of the signing process

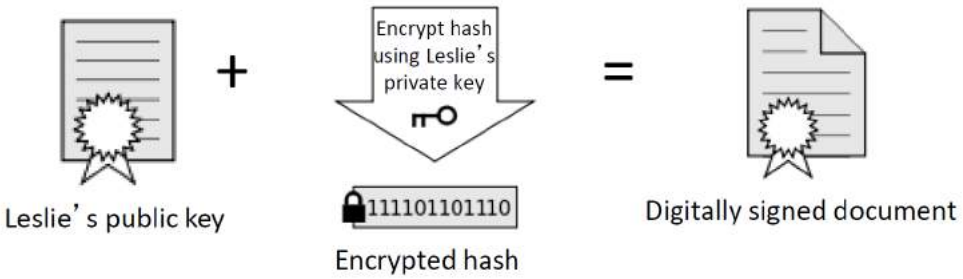
Let's take a look at what's actually happening when Leslie signs her PDF and when Joe verifies her signature.

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.



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.

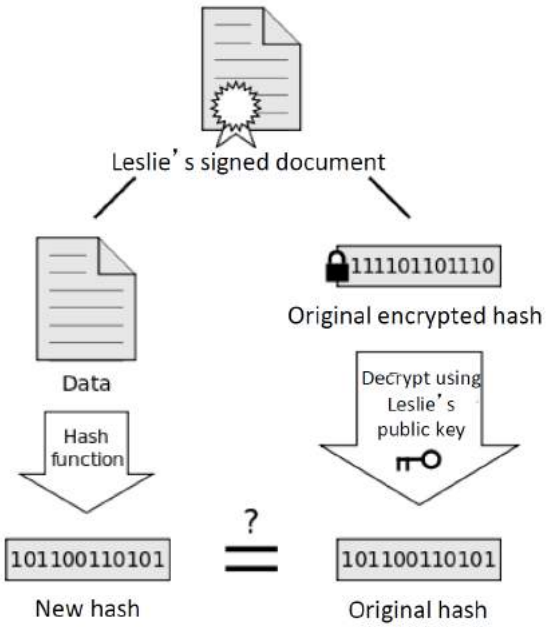


3. Leslie can now share the digitally signed document with Joe.

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 it was certified."



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.

Other signing scenarios

We ran through a basic scenario, in which Leslie simply needed to send a certified PDF with an image of her physical signature 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 official seal or stamp

- Instead of an image of her handwritten signature, Leslie could have added an image of a professional seal or stamp.

No changes allowed

- Since this was a contract between two parties, Leslie chose to allow digital signatures to be added to the document after she signed it. She could have disallowed any further changes, which would have locked down the document completely after signing.

Sign multiple pages of the same document

- Leslie could have added the image of her signature to multiple pages to the document.

Sign other types of documents

- Leslie could have applied her signature to a Microsoft Office (e.g., Word, Excel) document.

Chapter 4.

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 organisation (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 organisation's existing policies, procedures, and technologies

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 document?
- How many users?
- How many signatures?
- What types of regulations does my signature solution need to meet? (e.g., the FDA's Title 21 CFR Part 11, many state regulations require 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 organisation 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 industries like healthcare and architecture, engineering, and construction for years. Easy to use and with benefits like reducing paper waste, decreasing overhead costs, and speeding up document delivery, 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.trustzone.com | sales@trustzone.com

REFERENCES.

[1] Winning the Paper Wars, AIIM Industry Watch Report, July 30 2013, http://www.aiim.org

[2] The True Costs of Paper, Triple Pundit, http://www.triplepundit.com/2012/05/true-costs-paper/

[3] The Paper Free Office – dream or reality?, AIIM Industry Watch Report, http://www.aiim.org/pdfdocuments/iw_paper-free-capture_2012.pdf

[4] Jump-start your paper-free journey, AIIM Industry Watch Report, http://www.aiim.org

[5] Digital Signatures Survey and Best Practices Guide, Fiatech, http://www.fiatech.org/project-management/projects/457-digital-signatures-survey-and-best-practices-guide

Easily add digital signatures to your documents with TRUST-ZONE

TRUSTZONE's PDF Signing solution allows you to quickly and easily add certifying and approval signatures to your invoices, plans, bids, contracts, and other project documents. Sign up for a free a webinar from TRUSTZONE's partner GlobalSign to see how easy digital signatures can be.

TRUSTZONE A/S | Phone: +45 88 33 10 00 | Email: sales@trustzone.com | trustzone.com

TRUSTZONE