Introduction to Digital Signature

What is a digital signature?

You can use a digital signature for many of the same reasons that you might sign a paper document. A digital signature is used to authenticate digital information — such as form templates, e-mail messages, and documents — by using computer cryptography. Digital signatures help to establish the following assurances:

- Authenticity The digital signature helps to assure that the signer is who he or she claims to be.
- Integrity The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.
- Non-repudiation The digital signature helps prove the origin of the signed content to all parties. "Repudiation" refers to the act of a signer denying any association with the signed content.

To make these assurances about a form template, you must digitally sign your form template. You can also enable digital signatures for your form template so that your users can make the same assurances about the forms that they fill out. In either case, the following requirements must be met in order to digitally sign a form or form template:

- The digital signature is valid.
- The certificate associated with the digital signature is current (has not expired).
- The signing person or organization, known as the publisher, is trusted.
- The certificate associated with the digital signature is issued to the publisher by a trusted certificate authority (CA).

Digital signatures are the digital equivalent of regular ink signatures. Just like ink signatures signal your approval or involvement in a paper document and its contents, a digital signature does the same on digital documents. And they do it far better than ink signatures can.

Digital signatures use a Public Key Infrastructure (PKI), a standard format that provides high security and acceptance to your document. This combination of a public key and a private key is what makes a digital signature so safe.

Through the PKI and the processes involved in creating electronic signatures and storing digitally signed documents, you can be sure that your signature cannot be forged, and once signed. The document cannot be altered.

This makes a digital document with an e-signature secure enough to be valid worldwide, including anywhere within the United States and the European Union.

Furthermore, A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), two keys are generated, creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated.

Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder.

What are the benefits of digital signatures?

Security is the main benefit of digital signatures. Security capabilities embedded in digital signatures ensure a document is not altered and signatures are legitimate. Security features and methods used in digital signatures include the following:

Personal identification numbers (PINs), passwords and codes. Used to authenticate and verify a signer's identity and approve their signature. Email, username and password are the most common methods used.

Asymmetric cryptography. Employs a public key algorithm that includes private and public key encryption and authentication.

Checksum. A long string of letters and numbers that represents the sum of the correct digits in a piece of digital data, against which comparisons can be made to detect errors or changes. A checksum acts as a data fingerprint.

Cyclic redundancy check (CRC). An error-detecting code and verification feature used in digital networks and storage devices to detect changes to raw data.

Certificate authority (CA) validation. CAs issue digital signatures and act as trusted third parties by accepting, authenticating, issuing and maintaining digital certificates. The use of CAs helps avoid the creation of fake digital certificates.

Trust service provider (TSP) validation. A TSP is a person or legal entity that performs validation of a digital signature on a company's behalf and offers signature validation reports.

Other benefits to using digital signatures include the following:

Timestamping. By providing the data and time of a digital signature, timestamping is useful when timing is critical, such as for stock trades, lottery ticket issuance and legal proceedings.

Globally accepted and legally compliant. The public key infrastructure (PKI) standard ensures vendor-generated keys are made and stored securely. Because of the international standard, a growing number of countries are accepting digital signatures as legally binding.

Time savings. Digital signatures simplify the time-consuming processes of physical document signing, storage and exchange, enabling businesses to quickly access and sign documents.

Cost savings. Organizations can go paperless and save money previously spent on the physical resources and on the time, personnel and office space used to manage and transport them.

Positive environmental impact. Reducing paper use also cuts down on the physical waste generated by paper and the negative environmental impact of transporting paper documents.

Traceability. Digital signatures create an audit trail that makes internal record-keeping easier for business. With everything recorded and stored digitally, there are fewer opportunities for a manual signee or record-keeper to make a mistake or misplace something.

How Do Digital Signatures Work?

1. The digital signing software

To properly use a digital signature, you can’t just get a JPEG of your signature and paste it on a Word document. You need an electronic signature app to do the job.

Electronic signature solutions, like:

1. Adobe Sign - Tracking and document management
2. Secured Signing - With video confirmation
3. DocuSign - Handles multiple recipients
4. OneSpan Sign - For large and small organizations
5. SignEasy - Reusable templates
6. Signaturely

Make your digital signatures effective by becoming a TSP and certifying the document for you, keeping it safe.

Signaturely, for example, uses ISO 27001 and FIRMA certified data centers managed by Amazon. This allows Signaturely to access AWS data centers to securely store all your data on the cloud, ensuring only your signer's eyes can access it. The data you send to or from Signaturely is also encrypted in transit through 256-bit encryption. Signaturely also gives you the power further to protect your data through 2-Factor Authentication (2FA) to ensure you are the only person accessing your Signaturely account. Electronic signature platforms like Signaturely also handle all parts of the digital signing process for you, ensuring everything about the digital signing process is valid and legally binding.

2. Signing up for a platform for electronic signatures

Since e-signatures are only valid when using the right software, you'll need to choose one that works for you. There are a few options available for digitally signing documents, but you can get started for free by creating a an account.

Any E-Signature application offers a forever-free account allowing you up to three sent documents for free per month.

Start by creating a new account with your name, email address, and password, or sign up with your Google login for an even faster process. Within seconds you'll be able to access platform to create your new document.

3. Create or upload your documents

E-signature applications like Adobe, SecureSign, or Signaturely varies on the processes in signing your document, these processes differs but you will still get the same result. You can get started immediately with the contracts you have. There are no unnecessary processes so that you can set up your contract immediately.

Simply upload your document, and use the editor to add the signature fields. That's it.

You can either upload them directly from your computer or import them directly by connecting your DropBox, Google Drive, OneDrive, or Box accounts.

When the document has been uploaded, simply open it with the editor to add the signature fields, positioning them exactly where someone would sign if they were using an ink signature.

4. Send signature requests

When your document is fully digitized and ready to be signed, it's time to send a signature request to your signees. This process can be completed entirely in-app, letting do the heavy lifting for you.

All you need to do is to add the signees' names and email addresses. If your contract needs to be signed by people in a specific order, you can have the app send the document to them one after the other as each individual signs the agreement.

The e-signature app will then guide your signees through each step of the signing process, starting with creating their e-signature and continuing through the whole signing process step by step until each signature has been added to the document.

5. Wait for your digital documents to return

It is understandable that it can be nerve-wracking to wait for a document to be returned. The longer you wait, the more questions you ask yourself, like: "Have they seen it yet?" When did they see it? Should I call them and ask why they haven't signed the document?

Other application uses dashboard, so you can easily track your documents as they progress. It lets you know who has signed, when, and who has yet to sign. Other apps will remind the signee that their signature is still required, so you don't have to get directly involved. This gentle reminder is usually enough to nudge someone into signing without pressuring them into it.

Using powerful encryption and security keys to protect your document

When your signees open a document, their only option will be to sign it. They can't alter, edit, or change anything on the document. When a user signs the document, the signature records a timestamp. Once all users have signed, the document automatically locks itself, preventing further edits. You and your signees can know that the document you're signing cannot be altered in any way.

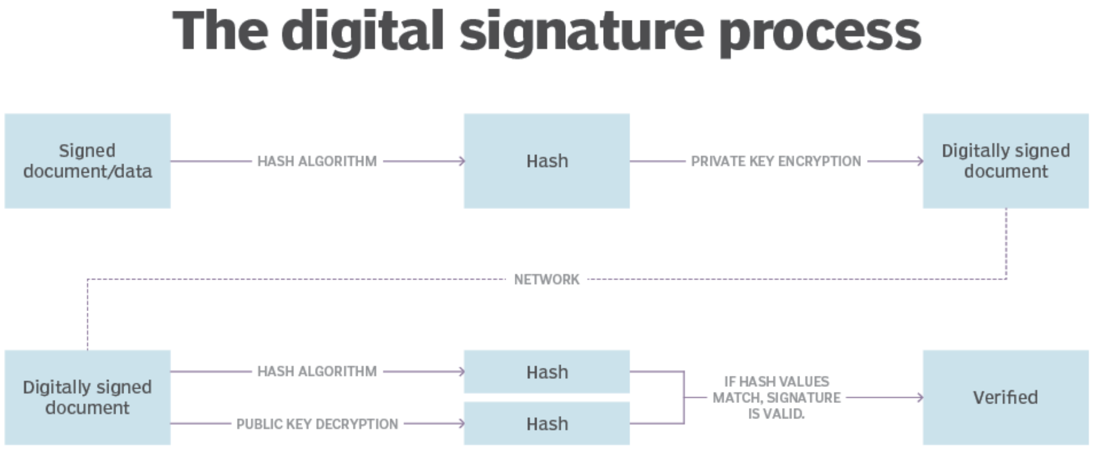
The digital signature signing software, such as an email program, is used to provide a one-way hash of the electronic data to be signed.

A hash is a fixed-length string of letters and numbers generated by an algorithm. The digital signature creator's private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature.

The reason for encrypting the hash instead of the entire message or document is a hash function can convert an arbitrary input into a fixed-length value, which is usually much shorter. This saves time as hashing is much faster than signing.

The value of a hash is unique to the hashed data. Any change in the data, even a change in a single character, will result in a different value. This attribute enables others to use the signer's public key to decrypt the hash to validate the integrity of the data.

If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way and is compromised or the signature was created with a private key that doesn't correspond to the public key presented by the signer -- an issue with authentication.


The digital signature process

Sample signing scenario

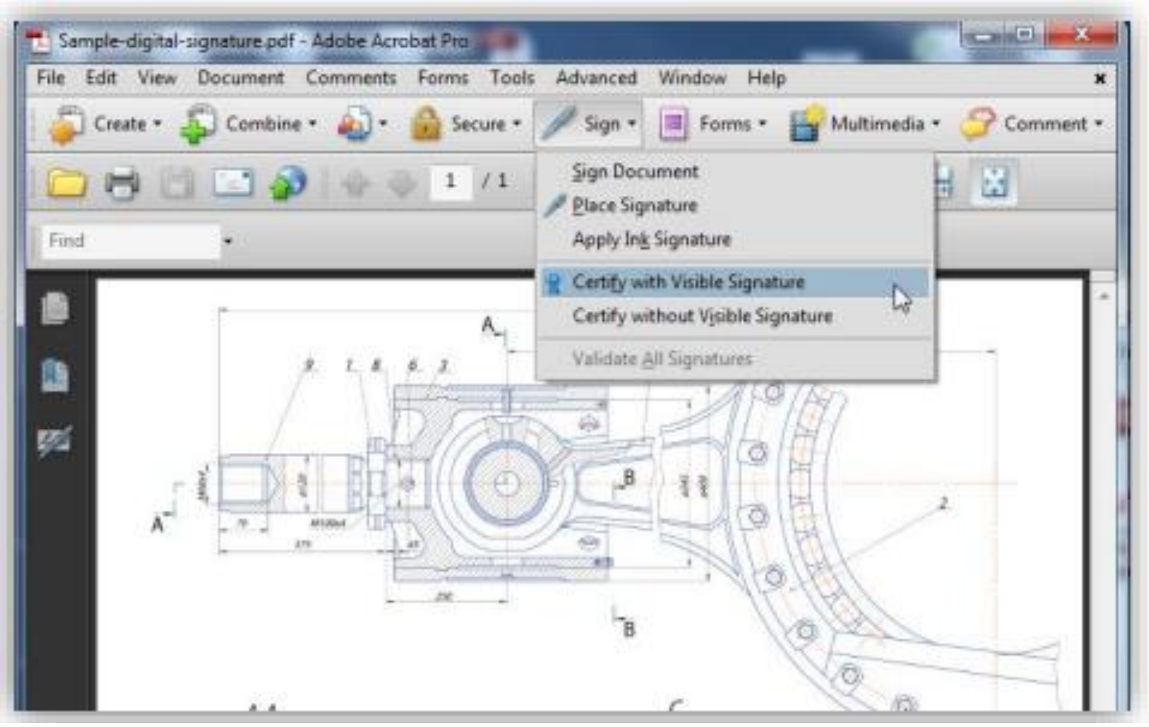
Scenario:

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.

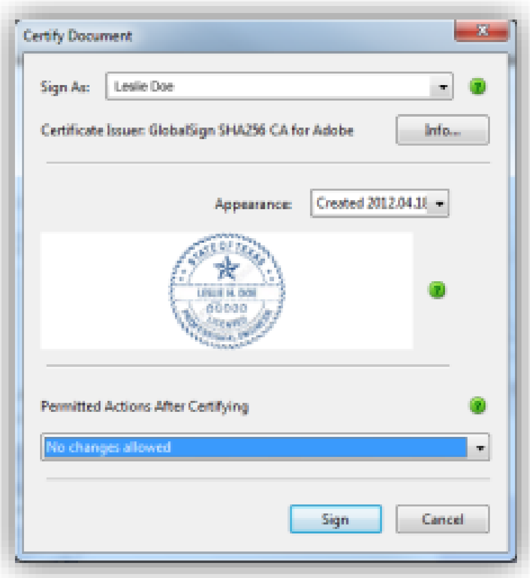
Applying the signature

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”.


Sample-digital-signature.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
Create Combine Secure Sign Forms Multimedia Comment
1 / 1
Find
Sign Document
Place Signature
Apply Ink Signature
Certify with Visible Signature
Certify without Visible Signature
Validate All Signatures

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.


Certify Document

Sign As: Leslie Doe

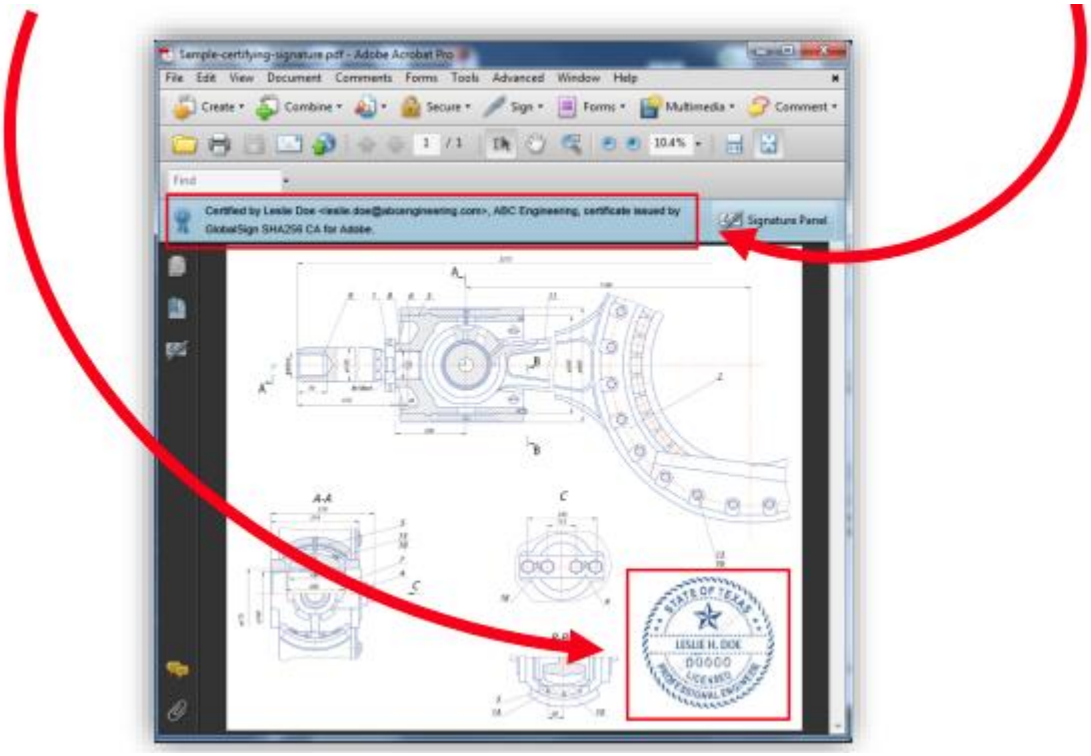
Certificate Issuer: GlobalSign SHA256 CA for Adobe

Appearance: Created 2012.04.1

Permitted Actions After Certifying

No changes allowed

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.

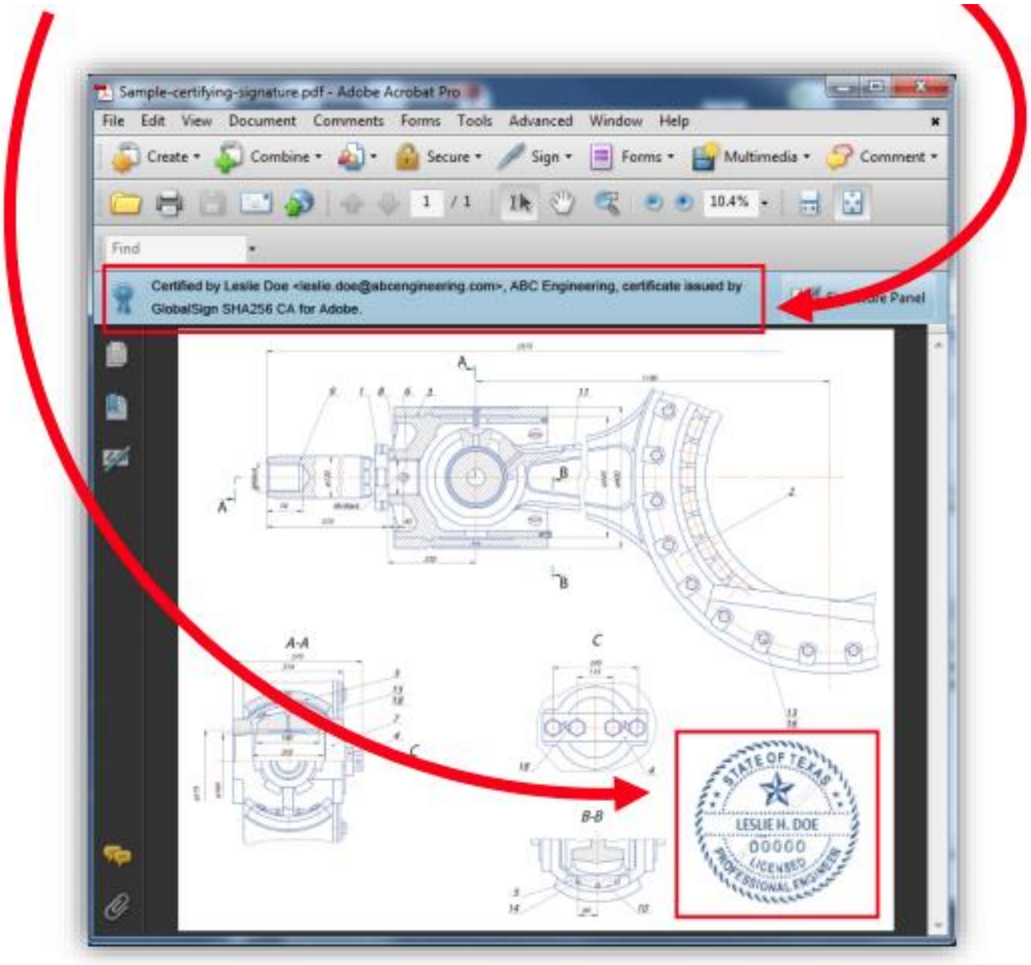

Sample-certifying-signature.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
Create Combine Secure Sign Forms Multimedia Comment
1 / 1
10.4%
Find
Signature Panel
STATE OF TEXAS
LESLIE H. DOE
00000
LICENSED
PROFESSIONAL ENGINEER

Certified by Leslie Doe <leslie.doe@abcengineering.com>, ABC Engineering, certificate issued by GlobalSign SHA256 CA for Adobe.

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.

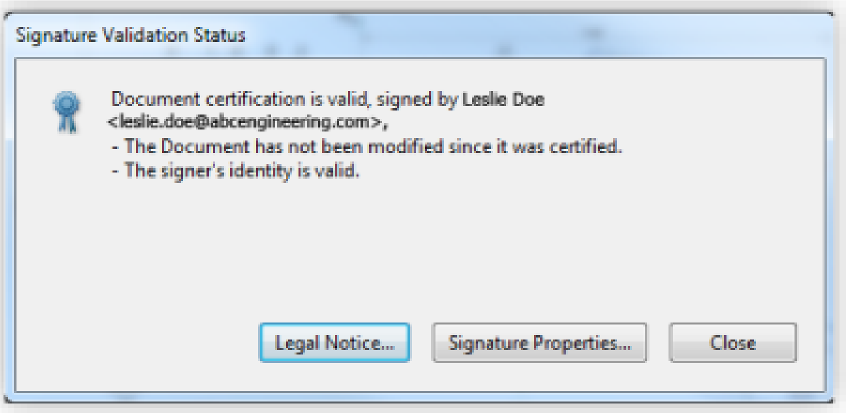
1. Joe opens the PDF in Adobe Reader and sees the same two trust indicators explained above - the notice at the top of the document and Leslie’s engineering seal



Sample-certifying-signature.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
Create Combine Secure Sign Forms Multimedia Comment
1 / 1
10.4%
Find
Signature Panel
STATE OF TEXAS
LESLIE H. DOE
00000
LICENSED
PROFESSIONAL ENGINEER

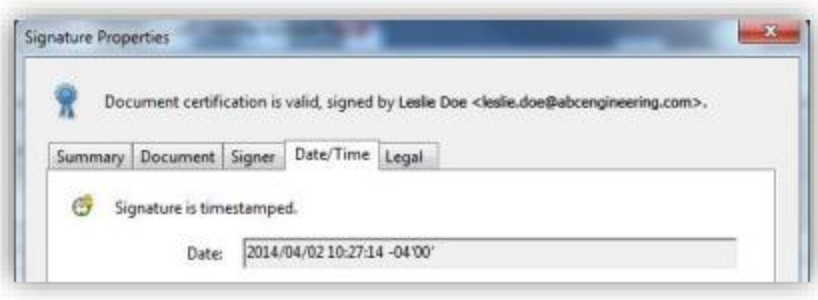
Certified by Leslie Doe <leslie.doe@abcengineering.com>, ABC Engineering, certificate issued by GlobalSign SHA256 CA for Adobe.

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



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.

3. 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>.

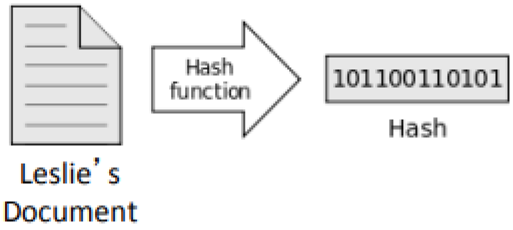
Signature is timestamped.

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

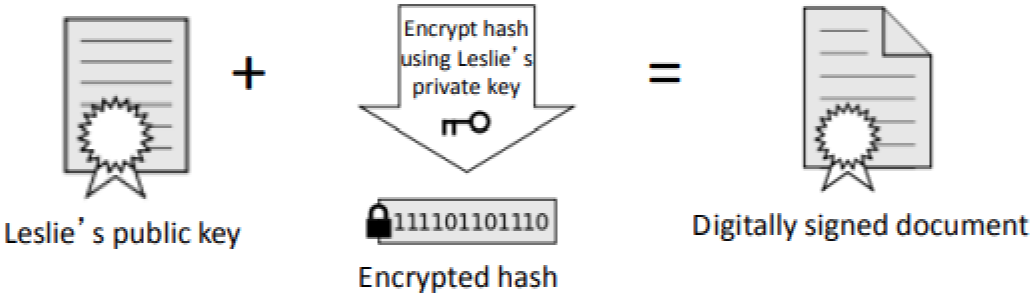
Behind the scenes of the signing process

A. 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.

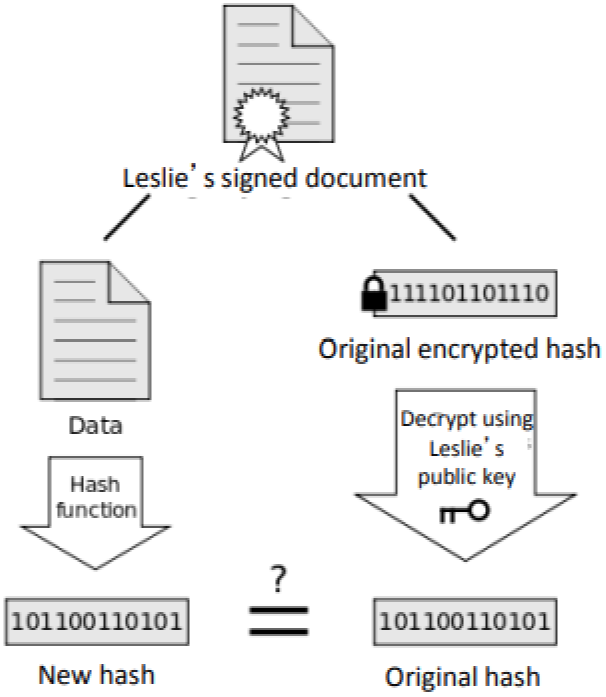

+
Encrypt hash using Leslie’s private key
=
Leslie’s public key
111101101110
Encrypted hash
Digitally signed document

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

B. 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.”



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.

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.

Sources:

How to Create a Self-Signed Digital Certificate in Microsoft Office 2016 (groovypost.com)

What is Digital Certificate? | A Technology Overview from Comodo

PowerPoint Presentation (globalsign.com)

What is a Digital Signature? (techtarget.com)

What Is a Digital Signature (and How Does it Work) | Signaturely

The difference between a digital signature and digital certificate » AET Europe