DOCSVAULT WhitePaper

# Digital Signatures

Digital Signatures

## Contents

# Overview

Businesses around the world are gradually moving from paper to electronic signatures - it is one of the most important, yet simplest steps one can take to embrace digital transformation. Electronic Signatures (e-signatures) are becoming increasingly standardized, and are becoming essential to global businesses. E-signatures let you shorten business process cycles, increase productivity, reduce costs, and modernize your organization's culture.

US President Bill Clinton made electronic signatures as binding as those on paper by electronically signing the Electronic Signatures in Global and National Commerce Act (ESIGN Act) into law in the year 2000. This groundbreaking law addresses e-signatures and electronic records, both of which are commonly used in commerce today.

This paper covers digital signatures in Docsvault and discusses several factors relating to the legality of e-signature with ESIGN Act and many worldwide legislations.

Digital Signature, which is available as an optional add-on in Docsvault, allows authorized Docsvault users to digitally sign documents on demand or within an electronic workflow process. The Digital Signature module also allows authorized Docsvault users to request Digital signatures remotely from anyone outside the organization using the Signature Requests feature.

# Digital Signatures vs Electronic Signatures

Digital Signature and Electronic Signature are both used to sign documents using modern technology, but the truth is that these two concepts are somewhat different. An electronic signature is an electronic symbol attached to a contract or other record, used by a person with the intent to sign. In contrast, digital signatures guarantee that an electronic document is authentic and is authorized by certification.


**The key differences between Digital Signature and Electronic Signature**

| Digital Signature | Electronic Signature |
|---|---|
| Digital signatures use digital certificates to sign a document | Electronic signatures simply apply image signatures to a document |
| Digital Signature complies with standards and enhances security by using cryptographic encryption methods | Electronic signature does not depend on standards and tend to be relatively less secure |
| Digital signature involves certificate-based digital ID authentication method | Authentication method used in the electronic signature is not defined |
| A digital signature can be verified | An electronic signature cannot be verified |
| Digital signatures are highly secured and offer tamper evidence | Electronic signatures are prone to tampering and hence less secure |

Over and above, it has been observed that an electronic signature is basically used to confirm the terms of a particular document and is equivalent to a handwritten signature. On the other hand, digital signature is based on Public key Infrastructure (PKI) technology. Digital signature creates a fingerprint that is unique to both the signer and the content, thus ensuring both signer identity and content integrity.

Though both electronic and digital signatures are legally binding, the latter is preferred because it provides content integrity and signer authenticity. Therefore, the type of signature that can be used is determined by the type of document you want to sign as well as the level of authenticity expected.

## Electronic Signatures and Law

As business over the Internet becomes more accessible and widely used, more countries are allowing electronic signatures to become legally binding.

There are two main pieces of legislation in the United States that form a foundation to recognize electronic signature legal and valid:

- ESIGN - Electronic Signatures in Global and National Commerce Act
- UETA - Uniform Electronic Transactions Act

Electronic signature is legally binding in over 27 countries — including China, India, Russia, Australia, Canada, and those in the European Union.

Some of the criteria that are commonly used in this type of legislation to certify the legality of electronic signature requires are:

- **Intent to sign** - the signer has intended to verify his or her identity
- **Consent to do business electronically** - the signer has agreed to do business electronically
- **Association of signature with the record** - the system used to capture the e-signature can prove the process by which the signature was created
- **Record retention** - the e-signature is archived for the required amount of time so it can be accessed by all interested parties

# Digital Signatures in Docsvault

Docsvault's **Digital Signatures add-on** enables organizations to create high-assurance business processes. Digital signatures in Docsvault are legally binding and are a preferred method of signing documents for compliance with various standards & regulations as they preserve the document's integrity, verify the identity of the signer and provide for non-repudiation of signatures within and beyond your organization. Once a document has been digitally signed, any unauthorized changes to it would make the signature invalid. It is an electronic process which assures the recipient that the contents of signed documents have been created by a known sender and it has not been altered after it was signed.

Digital Signature add-on enables you to sign documents as well as collect signatures from others. It's broadly divided into two main features:

- **Digitally Signing Document within Docsvault**

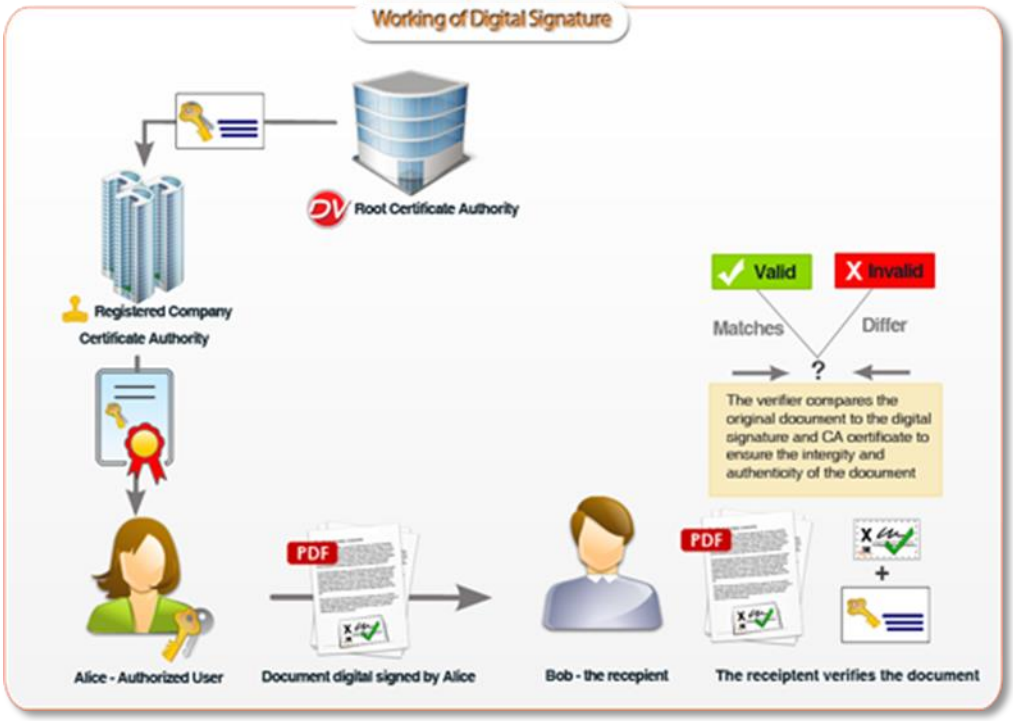
Authorized Docsvault users can digitally sign documents within the Docsvault system on demand, route digitally signed documents in a workflow for multiple approval signatures, auto-sign documents as part of a workflow and verify the validity of all signatures in a digitally signed PDF. A unique digital certificate is issued to individuals for signing documents within Docsvault.

**How do digital signatures work for authentication?**
Assume you want to send a project contract to your client. You want to give assurance to your client that the contents of the document were not tampered and that the document really is from you.

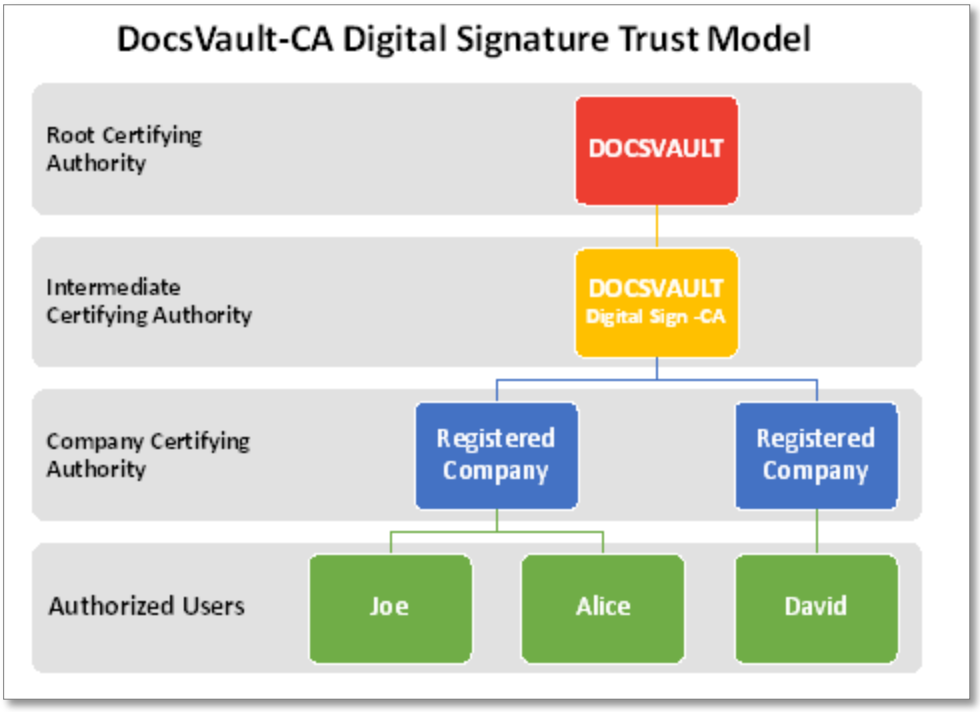
- You draft a project contract
- Using Docsvault's Digital Signature add-on, you sign the document
- When you sign a document, a digital certificate issued to you by Docsvault is embed in the document using your public and private key pair. The keys are used to lock the information in an encrypted mode. (Note that it will be different each time you sign a document)

At the other end, your client receives the document.

- To verify the signature on the document, your client will open the document in say Adobe Acrobat Reader. The application first uses the certificate authority's public key (issued by Docsvault) to check the signature in your digital certificate.
- Successful decryption proves the certificate to be valid
- A valid certificate gives confidence to your client that the document did indeed come from you and has not changed since you signed it. If the document was either altered after it was signed or originated by someone else, Acrobat Reader will indicate that fact.



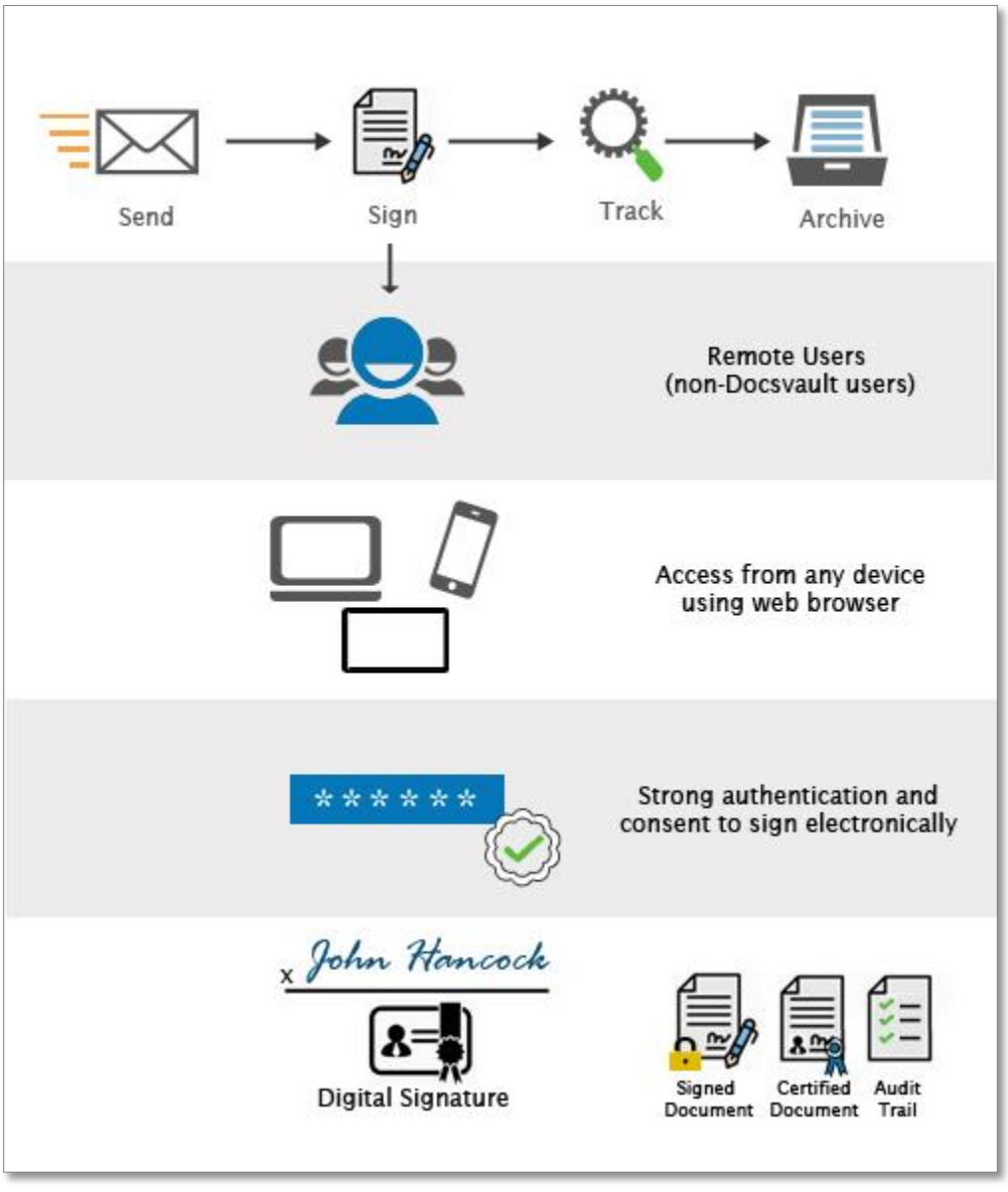

**Below is the structure of Docsvault Digital Signature Trust Model.**



## Getting Signature from Others

Docsvault's Signature Requests feature helps you to get signatures online from anyone outside the organization, i.e. non-Docsvault user, without leaving your Docsvault repository. Authorized Docsvault users can get signatures for contracts, agreements, or any documents from right within Docsvault – No printing, faxing or mail delivery required.

Below is a general overview of the entities in a remote signing service:



For instance, you want to get signature from your client on a contract. You send a signature request to your client to digitally sign the document.

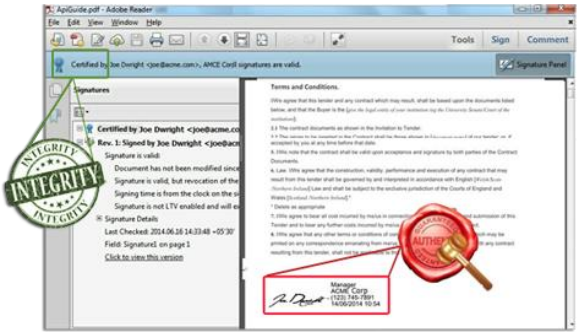
Signature Request is sent directly to the signer's email addresses which ensures that only the designated signers can view and sign documents. Additionally, you can even specify a request specific password and request expiry date to further enhance access security. All transactions and traffic are encrypted so there are no data leaks.

Signer receives an email letting them know that they have a documents to review and sign. They can quickly sign documents from anywhere and on any device using a simple web browser. On clicking the link in the email, they are directed to a welcome page where they are required to consent to the use of electronic signature and might be asked to enter password to authenticate their identity. The signer is then taken to the signing interface where they can view and sign the documents.

Documents are then securely saved to Docsvault repository with digital signature certificate embedded.

**Example of Verified Signature**

Adobe Acrobat Reader (or most modern PDF applications) can validate signatures in documents singed digitally in the Docsvault software. Signature validation data can be viewed either by right-clicking on the signature and choosing 'Show signature properties', from the top "Signature Bar" or through the left "Signature Panel".




If you send a digitally signed PDF to someone outside your company who does not have the Docsvault software installed they will have to go through a onetime process of downloading and running the Docsvault **Sign Validation tool** on their PCs. Once the Docsvault trusted certificates are installed on the client machine, the client can validate all PDFs signed by any Docsvault user in your company.

Download and install the Docsvault Sign Validation tool from here:
https://www.docsvault.com/signature-validation/

## Key benefits of Digital Signatures

- **Save Time and Money:** Eliminate the need to print and sign
- **Multiple Approvals:** Multiple signatures can be applied on any document with each signature having its own purpose.
- **Compliance:** Provides legally binding electronic signatures (AES data encryption), Comprehensive Audit Trail. Anyone can verify each document's authenticity using any standard PDF application.
- **Cross Platform:** Review and sign from any device using web browser
- **Speedy Results:** Signature requests can be delivered instantly and document signers can sign them from anywhere completing the process in no time

## Uses of Digital Signatures

The need to offer legally strong and convenient user approval exists across many different markets and departments. Some of the most common areas where it can be used are:

- Purchase: Sign electronic contracts, purchase order, invoices and notices
- Sales: Sale proposals, contracts with clients
- Admin: Approve periodic maintenance tasks, project budgets, quality checks
- Human Resources: Employee onboarding documents, time sheets
- Legal: Agreements and legal documents
- Healthcare: Patient and consent forms, health records, drug prescriptions, lab reports
- Engineering: Drawings, plans, design, manufacturing instructions, reports

## Conclusion

This white paper demonstrates how Docsvault's Digital Signatures are legally binding, enforceable and easier to manage than traditional paper documents, and are compliant with the U.S. Electronic Signatures in Global and National Commerce Act (E-Sign Act) and many worldwide e-signature legislations.

Docsvault uses PKI technology, where the business establishes their own level of authentication with their clients for the purpose of signing, and provides a clear audit trail of activities performed for signing documents to ensure non-repudiation.

DOCSVAULT

Get in touch

Monday to Friday
10:00 a.m. – 6:00 p.m. (EST)


| | |
|---|---|
| Toll Free USA: | (888) 819 3035 |
| International: | +1 (732) 960 3330 |
| Fax: | (888) 819 5965 |

E-mail us on:
Sales@Docsvault.com




Easy Data Access Sales (at) Docsvault.com 888.819.3035