Digital Signature

Digital Signature

- A digital signature is a mathematical technique which validates the authenticity and integrity of a message, software or digital documents.

- It allows us to verify the author name, date and time of signatures, and authenticate the message contents

- The digital signature offers far more inherent security and intended to solve the problem of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.

Application of Digital Signature

- The important reason to implement digital signature to communication is:

- Authentication
- Non-repudiation
- Integrity

Application of Digital Signature

- **Authentication**
  - Authentication is a process which verifies the identity of a user who wants to access the system.
  - In the digital signature, authentication helps to authenticate the sources of messages.

- **Non-repudiation**
  - means assurance of something that cannot be denied.
  - It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or in a file or the sending of a message that they originated.

Application of Digital Signature

- **Integrity**
- Integrity ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.

Algorithms in Digital Signature

- A digital signature consists of three algorithms:
- **Key generation algorithm**
  - selects private key randomly from a set of possible private keys.
  - provides the private key and its corresponding public key.
- **Signing algorithm**
  - A signing algorithm produces a signature for the document.
- **Signature verifying algorithm**
  - A signature verifying algorithm either accepts or rejects the document's authenticity.

How digital signatures work

- created and verified by using public key cryptography, also known as asymmetric cryptography.

- By the use of a public key algorithm, such as RSA, one can generate two keys that are mathematically linked- one is a private key, and another is a public key.

- The user who is creating the digital signature uses their own private key to encrypt the signature-related document

- There is only one way to decrypt that document is with the use of signer's public key.

How digital signatures work

- This technology requires all the parties to trust that the individual who creates the signature has been able to keep their private key secret.

- If someone has access the signer's private key, there is a possibility that they could create fraudulent signatures in the name of the private key holder.

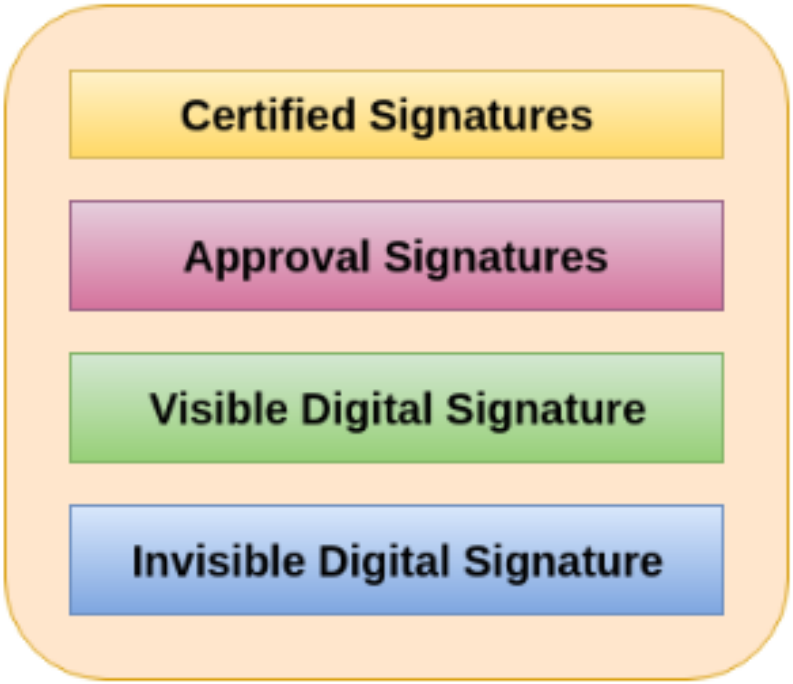
steps in creating a digital signature are:

1. Select a file to be digitally signed.
2. The hash value of the message or file content is calculated. This message or file content is encrypted by using a private key of a sender to form the digital signature.
3. Now, the original message or file content along with the digital signature is transmitted.
4. The receiver decrypts the digital signature by using a public key of a sender.
5. The receiver now has the message or file content and can compute it.
6. Comparing these computed message or file content with the original computed message. The comparison needs to be the same for ensuring integrity.

Types of Digital Signature

- Different document processing platform supports different types of digital signature.

- They are described below:



Certified Signatures

- signature documents display a unique blue ribbon across the top of the document

- The certified signature contains the name of the document signer and the certificate issuer which indicate the authorship and authenticity of the document.

Approval Signatures

- The approval digital signatures on a document can be used in the organization's business workflow
- They help to optimize the organization's approval procedure.
- The procedure involves capturing approvals made by us and other individuals and embedding them within the PDF document.
- The approval signatures to include details such as an image of our physical signature, location, date, and official seal.

Visible Digital Signature

- The visible digital signature allows a user to sign a single document digitally.

- This signature appears on a document in the same way as signatures are signed on a physical document.

Invisible Digital Signature

- The invisible digital signatures carry a visual indication of a blue ribbon within a document in the taskbar

- use invisible digital signatures when we do not have or do not want to display our signature but need to provide the authenticity of the document, its integrity, and its origin.