Digital Signatures and Certificates

Last Updated : 27 Dec, 2024

Digital signatures and **certificates** are two key technologies that play a crucial role in ensuring the security and authenticity of online activities. They are essential for activities such as online banking, secure email communication, software distribution, and electronic document signing. By providing mechanisms for authentication, integrity, and non-repudiation, these technologies help protect against fraud, data breaches, and unauthorized access.

Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. These are some of the key features of it.

1. **Key Generation Algorithms**: Digital signatures are electronic signatures, which assure that the message was sent by a particular sender. While performing digital transactions authenticity and integrity

should be assured, otherwise, the data can be altered or someone can also act as if he were the sender and expect a reply.

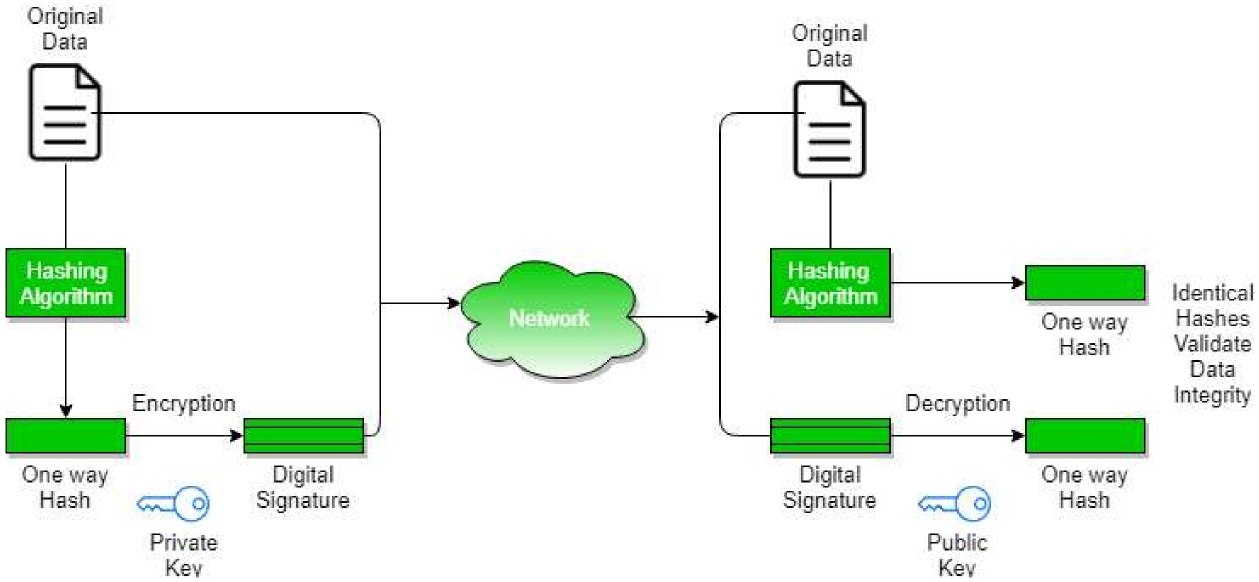
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed-length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and hashing is much faster than signing.
3. **Signature Verification Algorithms**: The Verifier receives a Digital Signature along with the data. It then uses a Verification algorithm to process the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. If they both are equal, then the digital signature is valid else it is invalid.

The steps followed in creating a digital signature are:

1. Message digest is computed by applying the hash function on the message and then message digest is encrypted using the private key of the sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm (message)).
2. A digital signature is then transmitted with the message. (message + digital signature is transmitted)
3. The receiver decrypts the digital signature using the public key of the sender. (This assures authenticity, as only the sender has his private key so only the sender can encrypt using his private key which can thus be decrypted by the sender’s public key).
4. The receiver now has the message digest.

5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



Assurances About Digital Signatures

The definitions and words that follow illustrate the kind of assurances that digital signatures offer.

1. **Authenticity**: The identity of the signer is verified.
2. **Integration:** Since the content was digitally signed, it hasn't been altered or interfered with.
3. **Non-repudiation:** demonstrates the source of the signed content to all parties. The act of a signer denying any affiliation with the signed material is known as repudiation.
4. **Notarization:** Under some conditions, a signature in a Microsoft Word, Microsoft Excel, or Microsoft PowerPoint document that has been time-stamped by a secure time-stamp server is equivalent to a notarization.

Benefits of Digital Signatures

- **Legal documents and contracts:** Digital signatures are legally binding. This makes them ideal for any legal document that requires a signature authenticated by one or more parties and guarantees that the record has not been altered.

- **Sales contracts:** Digital signing of contracts and sales contracts authenticates the identity of the seller and the buyer, and both parties can be sure that the signatures are legally binding and that the terms of the agreement have not been changed.

- **Financial Documents:** Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a attacker trying to trick the buyer into sending payments to a fraudulent account.

- **Health Data:** In the healthcare industry, privacy is paramount for both patient records and research data. Digital signatures ensure that this confidential information was not modified when it was transmitted between the consenting parties.

Drawbacks of Digital Signature

- **Dependency on technology:** Because digital signatures rely on technology, they are susceptible to crimes, including hacking. As a result, businesses that use digital signatures must make sure their systems are safe and have the most recent security patches and upgrades installed.

- **Complexity:** Setting up and using digital signatures can be challenging, especially for those who are unfamiliar with the technology. This may result in blunders and errors that reduce the system's efficacy. The process of issuing digital signatures to senior citizens can occasionally be challenging.

- **Limited acceptance:** Digital signatures take time to replace manual ones since technology is not widely available in India, a developing nation.

Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender. A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. Digital certificate is used to attach public key with a particular individual or an entity.