Digital Signature

Overview

An electronic signature uses a mathematical algorithm commonly used to verify a message's authenticity and integrity. Digital signatures always create a virtual fingerprint unique to identify users and protect the information in statements or digital documents. In emails, the content of the email becomes part of the digital signature. Digital signatures are much more secure than other forms of electronic signature.

The broad category of electronic signatures (eSignatures) includes many types of electronic signatures. The class of signatures includes digital signatures, which are a specific technology implementation of electronic signatures. Both digital signatures and other electronic signature solutions allow you to sign documents and authenticate the signer. However, there are differences in terms of purpose, technical implementation, geographical use, and legal and cultural acceptance of digital signatures compared to other types of electronic signatures.

The use of digital signature technology for electronic signatures differs significantly between countries that follow open and technology-neutral electronic signature laws, including the United States, Great Britain, Canada, and Australia and countries that follow signature models. Tiered electronics prefer locally defined standards based on digital signature technology, including many countries in the European Union, South America, and Asia. Additionally, some industries also support specific measures based on digital signature technology. The digital signature is a procedure that ensures that the content of a message has not been modified during transmission. When you digitally sign a document as a server, you add a one-way (encrypted) hash of the message content with your public and private key pair. Your client can still read it, but the process creates a "signature" that only the server's public key can decrypt. The client can then use the server's public key to verify the sender and the integrity of the message content. Whether it's an email, an online order, or a watermarked photo on eBay, if the transfer arrives but the digital signature doesn't match the public key on the digital certificate, the customer knows the message has been modified.

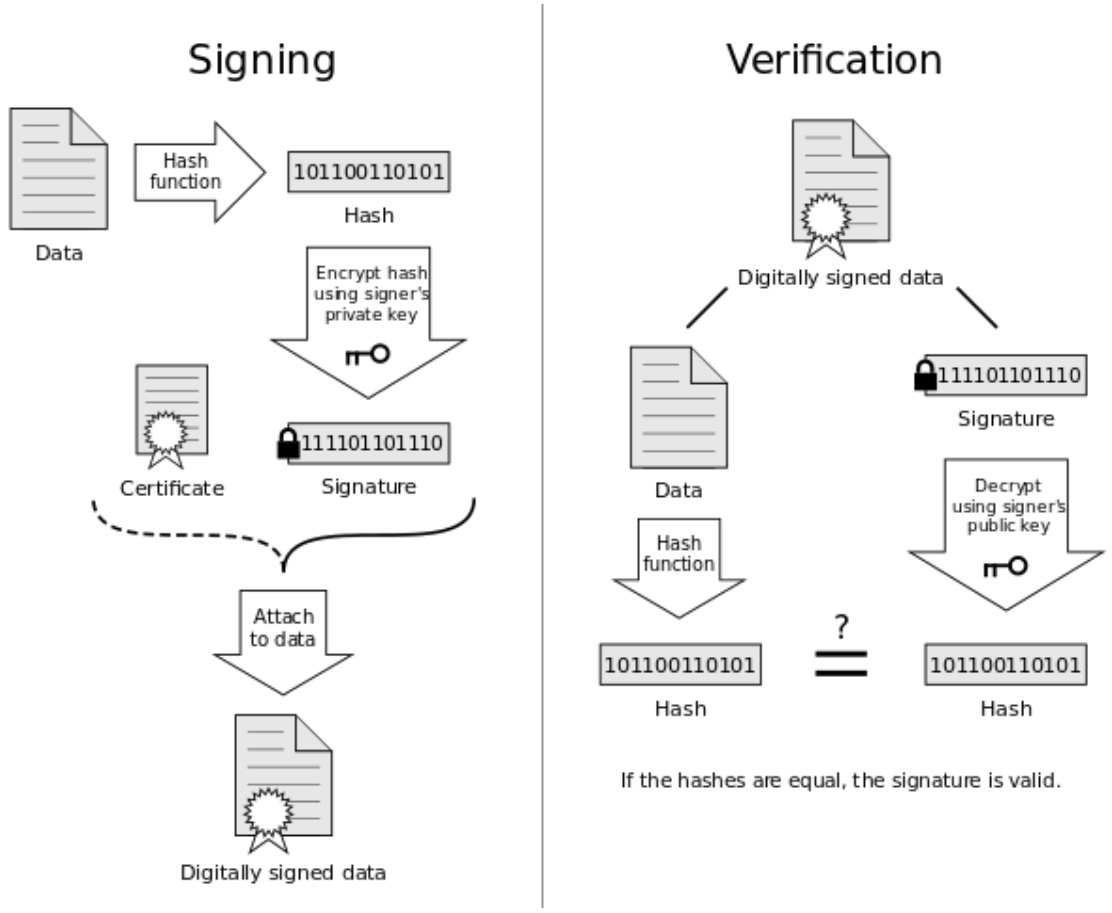

Figure 1: RSA

Working of RSA

Digital signatures are only based on public-key cryptography, also known as asymmetric cryptography. Two keys are generated using a public key algorithm like RSA (RivestShamirAdleman), creating a pair of mathematically linked keys, one private and one public. Digital signatures work through the two mutually authenticating cryptographic keys of public-key cryptography. The person creating the digital signature uses a private key to encrypt the signature-related data, while this can only be decrypted using the signer's public key. If the recipient cannot open the document with the signer's public key, this is an indication that there is some problem with the paper or signature. This is how digital signatures are authenticated. Digital signature technology requires all parties to trust that the person who created the signature kept the private key secret. If someone else has access to the signature's private key, that party could create fraudulent digital signatures on behalf of the personal key holder.

Benefits of Digital Signatures

Security is the main advantage of digital signatures. Security features built into digital signatures ensure that a document is not altered and legitimate signatures. The following security features and methods are used with 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 bad actor 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.
- Federal, state, and local government agencies have stricter policies and regulations than many private sector companies. From approving permits to stamping them on a timesheet, digital signatures can optimize productivity by ensuring the right person is involved with the proper approvals.
- **Shipping Documents:** Helps manufacturers avoid costly shipping errors by ensuring cargo manifests or bills of lading are always correct. However, physical papers are cumbersome, not always easily accessible during transport, and can be lost. By digitally signing shipping documents, the sender and recipient can quickly access a file, check that the signature is up to date, and ensure that no tampering has occurred.