Digital signature

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

Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer.

In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional document signatures.

How digital signatures work

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA, one can generate two keys that are mathematically linked: one private and one public.

Digital signatures work through public key cryptography's two mutually-authenticating cryptographic keys. The individual who is creating the digital signature uses their own private key to encrypt signature-related data; the only way to decrypt that data is with the signer's public key. This is how digital signatures are authenticated.

Digital signature technology requires all the parties to trust that the individual creating the signature has been able to keep their own private key secret. If someone else has access to the signer's private key, that party could create fraudulent digital signatures in the name of the private key holder.

How to create a digital signature

To create a digital signature, signing software -- such as an email program -- creates a one-way hash of the electronic data to be signed. The 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 that 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 validate the integrity of the data by using the signer's public key to decrypt the hash.

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 -- a compromise to its integrity -- 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.

A digital signature can be used with any kind of message -- whether it is encrypted or not -- simply so the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something -- assuming their private key has not been compromised -- as the digital signature is unique to both the document and the signer and it binds them together. This property is called nonrepudiation.

Digital signatures are not to be confused with digital certificates. A digital certificate, an electronic document that contains the digital signature of the issuing certificate authority, binds together a public key with an identity and can be used to verify that a public key belongs to a particular person or entity.

Most modern email programs support the use of digital signatures and digital certificates, making it easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures are also used extensively to provide proof of authenticity, data integrity and nonrepudiation of communications and transactions conducted over the internet.

Classes of digital signatures

There are three different classes of Digital Signature Certificates:

- **Class 1:** Cannot be used for legal business documents as they are validated based only on an email ID and username. Class 1 signatures provide a basic level of security and are used in environments with a low risk of data compromise.
- **Class 2**: Often used for e-filing of tax documents, including income tax returns and Goods and Services Tax (GST) returns. Class 2 digital signatures authenticate a signee's identity against a pre-verified database. Class 2 digital signatures are used in environments where the risks and consequences of data compromise are moderate.
- **Class 3:** The highest level of digital signatures. Class 3 signatures require a person or organization to present in front of a certifying authority to prove their identity before signing. Class 3 digital signatures are used for e-auctions, e-tendering, e-ticketing, court filings and in other environments where threats to data or the consequences of a security failure are high.

Uses of digital signatures

Industries use digital signature technology to streamline processes and improve document integrity. Industries that use digital signatures include:

Government - The U.S. Government Publishing Office publishes electronic versions of budgets, public and private laws and congressional bills with digital signatures. Digital signatures are used by governments worldwide for a variety of uses, including processing tax returns, verifying business-to-government (B2G) transactions, ratifying laws and managing contracts. Most government entities must adhere to strict laws, regulations and standards when using digital signatures.

Cyber Law (IT Law) in India

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software licence is controversial and still evolving in Europe and elsewhere.

According to Ministry of Electronic and Information Technology, Government of India :

Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

Indian Sale of Goods Act 1930

The **Indian Sale of Goods Act, 1930** is a Mercantile Law, which came into existence on 1 July 1930[1][2], during the British Raj, borrowing heavily from the Sale of Goods Act 1893. It provisions for the setting up of contracts where the seller transfers or agrees to transfer the title (ownership) in the goods to the buyer for consideration. It is applicable all over India, except Jammu and Kashmir. Under the act, goods sold from owner to buyer must be sold for a certain price and at a given period of time. The act was amended on 23 September 1963, and was renamed to the *Sale of Goods Act, 1930*. It is still in force in India, after being amended 1963 and in Bangladesh as the Sale of Goods Act, 1930