DIGITAL SIGNATURE

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures which include any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including South Africa, the United States, Algeria, Turkey, India, Brazil, Indonesia, Mexico, Saudi Arabia, Uruguay, Switzerland, Chile and the countries of the European Union, electronic signatures have legal significance.

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. (for more on

Digital signatures work because public key cryptography depends on 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 -- integrity -- or the signature was created with a private key that doesn't correspond to the public key presented by the signer -- 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.

Uses of Digital Signatures

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

1. 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.

2. Healthcare - Digital signatures are used in the healthcare industry to improve the efficiency of treatment and administrative processes, to strengthen data security, for e-prescribing and hospital admissions. The use of digital signatures in healthcare must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

3. Manufacturing - Manufacturing companies use digital signatures to speed up processes, including product design, quality assurance (QA), manufacturing enhancements, marketing and sales. The use of digital signatures in manufacturing is governed by the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) Digital Manufacturing Certificate (DMC).

4. Financial services - The U.S. financial sector uses digital signatures for contracts, paperless banking, loan processing, insurance documentation, mortgages, and more. This heavily regulated sector uses digital signatures with careful attention to the regulations and guidance put forth by the Electronic Signatures in Global and National Commerce Act (E-Sign Act), state UETA regulations, the Consumer Financial Protection Bureau (CFPB) and the Federal Financial Institutions Examination Council (FFIEC).

Digital Signature Certificate

Digital Signature Certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Few Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as proof of identity of an individual for a certain purpose; for example, a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove one’s identity, to access information or services on the Internet or to sign certain documents digitally.

Process of obtaining digital signature certificate

- Digital Signature Certificate (DSC) Applicants can directly approach Certifying Authorities (CAs) with original supporting documents, and self-attested copies will be sufficient in this case.

- DSCs can also be obtained, wherever offered by CA, using Aadhar eKYC based authentication, and supporting documents are not required in this case.

- A letter/certificate issued by a Bank containing the DSC applicant’s information as retained in the Bank database can be accepted. Such letter/certificate should be certified by the Bank Manager

Validity of Digital Signatures

The DSCs are typically issued with one year validity and two year validity. These are renewable on expiry of the period of initial issue.

Costing/ Pricing of Digital Signatures:

It includes the cost of medium (a UBS token which is a one time cost), the cost of issuance of DSC and the renewal cost after the period of validity. The company representatives and professionals required to obtain DSCs are free to procure the same from any one of the approved Certification Agencies as per the MCA portal. The issuance costs in respect of each Agency vary and are market driven.

However, for the guidance of stakeholders, the Ministry has obtained the costs of issuance of DSCs at the consumer end from the Certification Agencies. The costs as intimated by them are as under:

Certifying Authorities for Digital Signature Certificate

The Controller of Certifying Authority for the purpose of issuing digital signatures in India has authorized eMudhra as one of the certifying authority for issuance of Digital Signature Certificate.

Other certifying authorities may include (n) Code Solutions, National Informatics Centre, Safescrypt and Institute for Development and Research in Banking Technology.

Classes of DSC

The type of applicant and the purpose for which the Digital Signature Certificate is obtained defines the kind of DSC one must apply for depending on the need. There are three types of Digital Signature certificates issued by the certifying authorities.

Class 1 Certificates: These are issued to individual/private subscribers and are used to confirm that the user's name and email contact details from the clearly defined subject lie within the database of the certifying authority.

Class 2 Certificates: These are issued to the director/signatory authorities of the companies for the purpose of e-filing with the Registrar of Companies (ROC). Class 2 certificate is mandatory for individuals who have to sign manual documents while filing of returns with the ROC.

Class 3 Certificates: These certificates are used in online participation/bidding in e-auctions and online tenders anywhere in India. The vendors who wish to participate in the online tenders must have a Class 3 digital signature certificate.

Benefits of a digital signature certificate

Digital Signature Certificates are helpful in authenticating the personal information details of the individual holder when conducting business online.

1. Reduced cost and time: Instead of signing the hard copy documents physically and scanning them to send them via e-mail, you can digitally sign the PDF files and send them much more quickly.

The Digital Signature certificate holder does not have to be physically present to conduct or authorize a business

2. Data integrity: Documents that are signed digitally cannot be altered or edited after signing, which makes the data safe and secure.

The government agencies often ask for these certificates to cross-check and verify the business transaction.

3. Authenticity of documents: Digitally signed documents give confidence to the receiver to be assured of the signer's authenticity. They can take action on the basis of such documents without getting worried about the documents being forged.