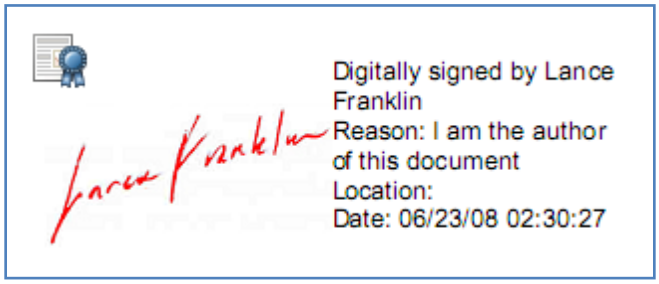
Why is a Digital Signature Necessary?

A digital signature authenticates electronic documents in a similar manner that a handwritten signature authenticates printed documents. This signature cannot be forged and it definitely states that a named person wrote or otherwise agreed to the document to which the signature is attached. The recipient of a digitally-signed message can verify that the message originated from the person whose signature is attached to the document and that the message has not been altered either intentionally or accidentally, since it was signed. Also, the signer of a document cannot later refuse to acknowledge it by claiming that the signature was fake, bogus, artificial etc.

A digital signature is issued by a Certification Authority (CA) and is signed with the CA's private key. A digital signature typically contains: the Owner's public key, the Owner's name, Expiration date of the public key, the Name of the issuer (the CA that issued the Digital ID), Serial number of the digital signature, and the digital signature of the issuer.
Digital signatures deploy the Public Key Infrastructure (PKI) technology.



Examples of Digital Signatures

A person/company which already has the specified Digital Signature for any other application can use the same for filings of the Income tax returns and is not required to obtain a fresh Digital Signature.

The Digital Signature certificates are typically issued with a one-year and two -validity. It includes the cost of medium (a UBS token which is a one-time cost), the cost of issuance of Digital Signature and the renewal cost after the period of validity. The issuance costs in respect of each Certification Agency vary and are market-driven. Digital Signatures are legally admissible in a Court of Law, as provided under the provisions of IT Act, 2000.

A licensed Certifying Authority (CA) issues the digital signature. At present the following organizations are authorized certifying Authorities under CCA, Government of India:

Sr.No	Name of Certifying Authority	Website
1	NIC (For Government Departments/Undertakings only)	http://nicca.nic.in
2	(n) Code Solutions CA(GNFC)	www.ncodesolutions.com
3	Safescript	www.safescrypt.com
4	TCS	www.tcs-ca.tcs.co.in
5	MTNL	www.mtnltrustline.com
6	Customs & Central Exercise	www.icert.gov.in
7	e-Mudhra	www.e-mudhra.com
8	IDRBT	http://idrbtca.org.in/

There are basically 3 types of Digital Signature Certificates: Class-1, Class-2 & Class-3, each with a different level of security.

Class-1

Class -1 Certificates are personal email Certificates that allow you to secure your email messages.

These Certificates can be used to:

- **Digitally sign email**: You can digitally sign your email messages, using Personal Digital Certificate so that the recipient is assured that the email has come from you.
- **Encrypt email:** You can encrypt emails using Personal Digital Certificate to prevent unauthorized people from reading it.
- **Authenticate to Web Servers**: You can authenticate yourself to a Web Server to engage in secure communication with a Web Server using your Personal Digital Certificate.

This protects all information such as credit card details that you send to the Web Server.
Certificates, however, do not facilitate strong authentication of the identity of the Subscriber; hence are not intended for, and shall not be relied upon, for commercial use where proof of identity is required.

Class-2

Class-2 Certificates are issued as Managed Digital Certificates to employees/ partners/ affiliates/ customers of business and government organizations that are ready to assume the responsibility of verifying the accuracy of the information submitted by their employees/ partners/ affiliates/ customers. In the case of a Class-2 Certificate, the verification of details supplied with the request for a Digital Certificate is done by the organization appointed as a Sub-CA/RA under the CA Trust Network.

Class-3

Class-3 Certificates are issued to individuals, companies and government organizations. They can be used both for personal and commercial purposes. They are typically used for electronic commerce applications such as electronic banking, electronic data interchange (EDI), and membership-based on-line services, where security is a major concern. The level of trust created by the Digital Certificate is based on the authentication procedures used by the CA to verify your identity and the service guarantees offered by the CA to back up that authentication. During verification, you will also need to be physically present before a Registration Authority (RA), qualified by a CA due to their neutrality and reliability. These validation procedures provide stronger assurances of an applicant's identity.

In other words, digital signatures enable the "authentication" and “non-repudiation” of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or damage or alteration or misuse of it.