Digital signatures are going to play an important role in our lives with the gradual electronization of records and documents.
The IT Act has given legal recognition to digital signature meaning, thereby, that legally it has the same value as handwritten or signed signatures affixed to a document for its verification. The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents.

WHO NEEDS A DIGITAL SIGNATURE CERTIFICATE ?
Under MCA21 Every person who is required to sign manual documents and returns filed with ROC is required to obtain a Digital Signature Certificate (DSC). Accordingly following have to obtain Digital Signature Certificate:
1. Directors
2. Auditors
3. Company Secretary - Whether in practice or in job.
4. Bank Officials - for Registration and Satisfaction of Charges
5. Other Authorized Signatories.

TYPES OF DIGITAL SIGNATURE CERTIFICATE
There are 3 types of Digital Signature Certificates, having different security levels, namely :- Class-1, Class-2 , Class-3.
For filing documents under MCA21, a Class-2 Digital Signature Certificate issued by a Licensed Registration Authority is required. We also offer Class 1 and 3 besides Class 2 certificates.

Why USB e-token?
A Digital Signature certificate (DSC) is kept in internet explorer of computer system (PC) but keeping DSC on your computer system has following draw backs :-
a) It can be misused by anyone who is having access to your computer system.
b) DSC is lost if computer system is formatted or internet explorer is changed.
Accordingly, safe and proper method is to keep DSC on e-token, a small USB port devise, which is password protected. The said e-token is a small hardware device and can be plugged to USB port of any system to digitally sign the documents and when not in use can be kept in safe custody.

Why Digital Signatures?
Ministry of Company Affairs, Government of India (GoI) has initiated MCA21 program, for easy and secure access to its services in a manner that best suits the businesses and citizens. MCA21 is envisioned to provide anytime and anywhere services to businesses. It is a pioneering program being the first mission mode e-governance project being undertaken in the country. This program builds on the GoI vision to introduce a Service Oriented Approach in the design and delivery of Government services, establish a healthy business ecosystem and make the country globally competitive.
The MCA21 application is designed to support Class 2 & 3 Digital Signature Certificates (DSC)

issued by licensed Certifying Authority under Controller of Certifying Authorities, GoI.
Those individuals recommended and forwarded by Superior Authority or those who approach any RA office operating under CA with proper certification from Chartered Accountant/Cost Accountant can avail our certification services for obtaining digital certificate.

What is a Digital Signature Certificate?
Digital signature certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as a 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 your identity, to access information or services on the Internet or to sign certain documents digitally.

Why is Digital Signature Certificate (DSC) required?
Like physical documents are signed manually, electronic documents, for example e-forms are required to be signed digitally through Digital Signature Certificate. As per MCA21 project of ministry of company affairs all the company forms have to be filed electronically.

Who issues the Digital Signature Certificate?
A licensed Certifying Authority (CA) issues the digital signature. Certifying Authority (CA) means a person who has been granted a licence to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000. The list of licensed CAs along with their contact information is available on www.mca.gov.in . You can obtained your DSC from us.

What are the different types of Digital Signature Certificates?
Class 1: These certificates do not hold any legal validity as the validation process is based only on a valid e-mail ID and involves no direct verification.
Class 2: Here, the identity of a person is verified against a trusted, pre-verified database.
Class 3: This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity.

Who can have digital signature certificate?
Any person can apply to the certifying authority for issue of a DSC in the prescribed form and paying prescribed fees. While prescribing, the government can differentiate the fee structure for different classes of applicants. The applicant shall also enclose a certification practice statement and in the absence of such a statement, particulars, as prescribed by regulations, have to be given.